Волжский университет имени В.Н. Татищева

ВЕСТНИК ПО БЕЗОПАСНОСТИ

№10 декабрь 2017

В НОМЕРЕ:

ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск десятый

Тольятти 2017

ББК 004.00+33.00+34.00+57.00+80/84

Материалы Всероссийской научно-практической конференции по безопасности. Вестник по безопасности. Выпуск десятый. – Тольятти: ВУиТ, 2017. - 153 с.

18-19 декабря 2017 года в Волжском университете имени В.Н. Татищева состоялась Всероссийская научно-практическая конференция по безопасности.

В настоящем издании публикуются материалы участников конференции.

Все материалы представлены в авторской редакции.

Ответственный редактор к. т. н., доцент О.Ю. Федосеева

ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Андреев В.И., студент
Научный руководитель: к. ю. н., доцент Дубовиченко С.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Последние десятилетия XX века и начало XXI века во всем мире и России стали периодом расцвета преступной среды.

Организованная преступность как угроза национальной безопасности Российской Федерации имеет определенные истоки в жизни общества и государства, являясь при этом результатом действий совокупности многочисленных факторов объективного и субъективного, организованного и стихийного характера.

Государство и общество еще не выработали по отношению к организованной преступности подхода, свидетельствующего о полном осознании ее сущности, предпосылок и последствий. Не определены механизмы борьбы с ней, адекватные уровню ее опасности.

Уровень и тенденции распространения организованной преступности в стране поставили ее в один ряд с самыми серьезными проблемами современной действительности нашей страны. Происшествие, свидетельствующее о высокой опасности организованной преступности, стало произошедшее в 2010 году зверское убийство 12 человек в станице Кущевская, где, как выяснилось, на протяжении многих лет действовало хорошо организованное преступное сообщество.

В связи с тем, что организованная преступность представляет собой крайне сложное явление, на протяжении продолжительного периода времени формировалось огромное количество различных подходов к определению понятия организованная преступность. Давались определения в Конгрессе США в 50-е и 60-е годы 20 века, в 1991 году в г. Суздале во время международного семинара посвященного проблеме борьбы с организованной преступностью, в котором участвовали различные международные организации, также давалось определение организованной преступности.

Наиболее точное определение организованной преступности на мой взгляд дано криминологом Александром Ивановичем Гуровым. Согласно формулировке предложенной Гуровым - организованная преступность - «это относительно массовое функционирование устойчивых управляемых сообществ преступников, занимающихся совершением преступлений как промыслом (бизнесом) и создающих с помощью коррупции систему защиты от социального контроля».

Организованная преступность тесно взаимосвязана с коррупционными явлениями и терроризмом. Теоретики и практики отмечают, что, несмотря на то, что терроризм и организованная преступность имеют разные механизмы развития и внешнее проявление, очевидна их внутренняя и внешняя связь. Отмечается, что наркокартели, занимающиеся незаконным оборотом наркотиков, неоднократно прибегают к террору для устрашения правительств и их судебных, полицейских или военных властей для того, чтобы не допустить задержания, преследования и заключения или выдачи своих членов. То есть, цели у террористических организаций и организованных преступных групп разные, а способы достижения целей одинаковые - террор.

Анализируя взаимосвязь организованной преступности с коррупцией, криминолог А.И. Долгова отмечает, что «коррупция для организованных преступников - это средство обеспечения не только их корыстного, но и политического интереса, поскольку у них отмечается двойная мотивация: получить сверхприбыль и власть ради их сохранения и приумножения. В случае коррумпированности государственных служащих, а тем более масштабной коррумпированности, граждане страны фактически теряют свой государственный аппарат, он служит в этом случае не налогоплательщикам, а интересам тех, кто его «перекупил»».

Вопрос относительно истоков зарождения организованной преступности в России является важным и спорным. На наш взгляд 70-е годы 20-го века стали моментом трансформации профессиональной преступности в России в преступность организованную. Наряду с присущими профессиональной преступности свойствами, такими как структурированность и относительно большая численность в период 70-х годов добавляется третий элемент, элемент коррупции. Происходит сращивание профессиональной преступности и представителей властных структур страны. Ключевым этапом в развитии организованной преступности стала перестройка и приватизация, то есть либерализация

собственности. Появление в стране кооперативов дает нелегальным дельцам (так называемым цеховикам) возможность для проникновения в эти структуры для участия в них и отмывания через кооперативы незаконно заработанных денег. Именно на этом этапе организованная преступность получает неограниченные возможности для легализации и дальнейшего проникновения во властные структуры страны.

Важным также является вопрос о противодействии организованной преступности. Противодействие организованной преступности должно являться непротиворечивым фрагментом государственной политики общественного развития. Целесообразно осуществить разработку программного документа (программы, концепции, стратегии) по противодействию организованной преступности.

Борьба с организованной преступностью не сможет быть результативной без серьезной реформы правоохранительных органов. Необходимо воссоздание ранее ликвидированных специальных подразделений по борьбе с организованной преступностью (РУБОПов).

Одновременно с этим следует укрепить законодательную базу. Представляется, что правовые основы борьбы с организованной преступностью должны включать в себя широкий спектр законов, причем не только узкоотраслевых, но и комплексных, приводящих совокупность разнообразных правовых средств воздействия на организованную преступность в единую цельную систему. Это специализированные законы «О борьбе с организованной преступностью», «О борьбе с легализацией незаконных доходов», а также соответствующие положения уголовного, уголовно-процессуального, гражданского, административного кодексов и других законодательных актов.

Борьба с организованной преступностью на международном уровне тоже является значимым элементом. Следует сказать, что уровень международного сотрудничества в борьбе с организованной преступностью, достигнутый между Российской Федерацией и странами СНГ, несомненно, выше, чем между Российской Федерацией и иными государствами, не являющимися членами Содружества Независимых Государств.

Данное обстоятельство успешно применяется членами организованных преступных групп для «ухода» от уголовной ответственности за совершенные ими преступления. Например, будучи осведомленными об отсутствии с тем или иным государством соглашения о выдаче, преступники укрываются на его территории от уголовного преследования государства, где они совершили преступление.

Итак, борьба с организованной преступностью, на сегодняшний день, является важной задачей нашего государства. Последовательная реализация имеющихся мер позволит переломить ход этой борьбы, и будет способствовать постепенному оздоровлению российского общества и государства.

АНТРОПОГЕННАЯ ДЕЯТЕЛЬНОСТЬ ЧЕЛОВЕКА И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

Волкова К., студент
Научный руководитель: к. ю. н., доцент Галеева Г.Р.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Экология – это наука, изучающая условия существования живых организмов, их взаимосвязи между собой и окружающей средой.

Человек в первую очередь существо биологическое и по своей природе стремится к безопасному и комфортному существованию. Именно поэтому в современных условиях среди экологических факторов, влияющих на природную среду, выделяется деятельность человека. Существует специальный раздел экологии, который изучает влияние антропогенных факторов на окружающую среду.

К антропогенным факторам относятся все формы деятельности человеческого общества, приводящие к изменению среды обитания организмов. Антропогенные воздействия на биосферу по их экологическим последствиям подразделяют на положительные и отрицательные (негативные).

К положительным воздействиям можно отнести воспроизводство природных ресурсов, восстановление запасов подземных вод, полезащитное лесоразведение, рекультивацию земель на месте разработок полезных ископаемых и другое[1].

[1] Введение. Теоретическая часть. Антропогенное воздействие. [Электронный ресурс] https://studfiles.net/preview/2789652/ (Дата обращения 20.10.17).

К отрицательным (негативным) воздействиям на биосферу относят все виды воздействий человека ухудшающих состояние природы[1]. Загрязнение природы человеком представляет собой одну из самых актуальных проблем. На протяжении многих веков человек рассматривал окружающую среду лишь как постоянный источник необходимых ему ресурсов. Своими действиями он быстро изменял естественную среду обитания, которая давно не имеет свой первоначальный вид. Быстро разрастаются города и крупные культурные ландшафты. Прогрессивно уменьшаются площади, которые раньше были засажены деревьями. Озера и реки давно превратились в стоки нечистот промышленных отходов, а так же все больше и больше загрязняется атмосфера аэрозолями и газами. В результате все это ведет к заболеванию людей, животных и растений, а часто и к их гибели.

Небывалые по мощности и разнообразию негативные антропогенные воздействия особенно резко стали проявляться во второй половине XX века.

В последнее время угроза для безопасности и благоприятного существования человека по большей части исходит от неблагоприятного состояния окружающей среды. Сейчас совершенно точно известно, что загрязнение окружающей среды способно пагубно влиять на здоровье. Поэтому в интересах каждого человека встать на охрану окружающей среды и стараться собственными усилиями улучшить ее состояние. В глобальном масштабе перед человечеством стоит задача - предотвратить значительные экологические катастрофы и аварии.

С появлением химических производств нарушается природный биогеохимический баланс, изменяется круговорот веществ. Параллельно с развитием промышленности, развивался соответственно и транспорт (водный, железнодорожный, автомобильный), использование которого не только привело за собой усиление загрязнения окружающей среды, но и требует огромного количества природных ресурсов для их реализации и полноценной работы. Природные вещества и соединения всё больше вовлекаются в технологические процессы, что может привести к полному исчерпанию ресурсов. А так же происходит нарушения экологического равновесия, что провоцирует сдвиг наступление времен года – весна начинается несколько раньше, а осень задерживается. Время солнечного сияния на 5 – 15% меньше чем в пригородах[2]. Для того, чтобы восстановить и сохранить баланс природной среды необходимо создать и внедрить принципиально новые безотходные технологические процессы. Производство товаров и услуг, эксплуатация технических систем должны быть максимально безопасными.

Проблемы экологической безопасности и рационального природопользования неразрывно связаны с социально-экономическим развитием общества и обусловлены им. Экологическая безопасность входит в систему государственной безопасности. Её основная цель состоит в обеспечении всестороннего развития государства и общества, но с гарантией сохранения благоприятной среды обитания и комфортных условий для жизнедеятельности и воспроизводства населения, а также обеспечение охраны природных ресурсов и предотвращения техногенных аварий и катастроф.

Для того чтобы решить многие экологические проблемы необходимо:

1. снизить и довести до безопасных уровней техногенную нагрузку на человека и окружающую[3];
2. обеспечить поддержание качество рекреационных объектов, безопасного сбора, перевозки, хранения, переработки и утилизации бытовых и промышленных отходов;
3. поэтапно экологизировать производства и внедрить экологически безопасные технологий;
4. реабилитировать загрязненные территорий города, обеспечить сохранение и восстановление лесов, парков, скверов и зеленых насаждений, их разнообразия;
5. установить полный контроль над добычей полезных ископаемых и их рациональным использованием.

А так же необходимо улучшить единую систему мониторинга окружающей среды и здоровья населения и внедрить многие другие рекреационные процедуры.

Глобально экологической безопасностью занимаются ООН, ЮНЕСКО, ЮНЕП и других международные организации. На этом уровне управления занимаются принятием международных актов по защите окружающей среды в масштабах биосферы, реализацию межгосударственных экологиче-

---

[1] Введение. Теоретическая часть. Антропогенное воздействие. [Электронный ресурс] https://studfiles.net/preview/2789652/ (Дата обращения 20.10.17).

[2] Меры защиты здоровья при нарушении экологического равновесия в городе. [Электронный ресурс] http://www.refbzd.ru/viewreferat-246-1.html (Дата обращения 20.10.17).

[3] Экологическая безопасность [Электронный ресурс] http://diplomba.ru/work/131196 (Дата обращения 21.10.17).

ских программ, создание межправительственных сил по ликвидации экологических катастроф, имеющих природный или антропогенный характер[1].

На глобальном уровне был решен ряд экологических проблем международного масштаба. Большим успехом международного сообщества стало запрещение испытаний ядерного оружия во всех средах, пока кроме подземных испытаний[2].

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ПРИРОДНЫХ РЕСУРСОВ

Воровко К., студент
Научный руководитель: к. ю. н., доцент Галеева Г.Р.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

На начальном этапе 21 века, существования планеты Земля, человечество уже столкнулось с многочисленным рядом экологических проблем. Большое количество происшествий, возникающих в окружающей среде, не подвластны человеку, но и немалое количество среди них возникает, именно, по вине человека.

Развиваясь, человечество достигает невероятных высот в развитии цивилизации. Успешно развивается медицина, технологическая деятельность, наука в целом, и многие другие области деятельности человека. Главной целою всего этого, является усовершенствование жизни, стремление сделать её максимально комфортной.

Средством к достижению этой цели, также служит и использование человеком природных ресурсов, с помощью которых функционируют и развиваются различные сферы жизнедеятельности. Безусловно, не малых успехов человек достиг и в этой области. Люди научились по максимуму использовать природные ресурсы, которые позволяют осуществлять промышленную, экономическую и сельскохозяйственную деятельности. Осуществляется разработка различных технологий, позволяющих извлекать природные ресурсы из недр Земли и на её поверхности, а также перерабатывать их, делая наиболее пригодными к использованию. Но, к сожалению, данная деятельность человека, сугубо действует на состояние экологии, не всегда людям удается осуществлять свои промыслы грамотно и без последствий. Человек научился брать, но не научился отдавать – такова ситуация в мире на данный момент.

Большое количество природных ресурсов уже достигло критических порогов. Несмотря на высокое развитие человечества, люди все же пока не нашли способов возобновления исчерпаемых ресурсов, таких как нефть, газ, минеральные руды, которые наиболее важны для существования человечества, и дефицит и исчезновение которых, способны поставить под угрозу всю жизнедеятельность людей.

Главная задача, которая стоит перед экологическим законодательством, - привести экологический правопорядок в соответствие с состоянием экономических и иных общественных отношений, а также в соответствие с оценками о состоянии природных ресурсов.

Исходя из нынешних показателей состояния экологии, учеными разрабатываются различные концепции, предусматривающие наиболее грамотное использование природных ресурсов. Одним из видов такой деятельности является лимитирование природопользования.

Лимиты на природопользование – это система экологических ограничений по территориям. Они представляют собой ограничения по объёмам предельного изъятия природных ресурсов, которые устанавливаются предприятиям - природопользователям на определённый срок, а также ограничения выбросов или сбросов в окружающую природную среду загрязняющих веществ и размещения отходов производства.

Проекты лимитов разрабатываются предприятиями, учреждениями и организациями - природопользователями и утверждаются Министерством природных ресурсов и экологии Российской Федерации. Руководство работой по определению лимитов природопользования осуществляется на соответствующей территории органами исполнительной власти субъектов РФ, органами местного са-

[1] Экологическая безопасность [Электронный ресурс] http://center-yf.ru/data/Menedzheru/ekologicheskaya-bezopasnost.php (Дата обращения 21.10.17).

[2] Там же.

моуправления совместно со специально уполномоченными органами Российской Федерации в области охраны окружающей природной среды и использования природных ресурсов[1].

В статье КоАП Рф, 8.2 «Несоблюдение экологических и санитарно-эпидемиологических требований при обращении с отходами производства и потребления, веществами, разрушающими озоновый слой, или иными опасными веществами», указывается наказание в виде наложения административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от десяти тысяч до тридцати тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, - от тридцати тысяч до пятидесяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на юридических лиц - от ста тысяч до двухсот пятидесяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток[2].

Лимиты на природопользование включают в себя:

Нормы, касающиеся отвода земель для строительства, деятельности по водопользованию, расчету лесосеки. Также экологическое законодательство устанавливает лимиты на использование объектов животного мира и лимиты на выбросы, и сбросы загрязняющих веществ и микроорганизмов в окружающую сферу[3].

Законодательством предусмотрено два вида лимитов природопользования: объемы предельного использования природных ресурсов (предельно допустимые нормы изъятия природного вещества из окружающей среды) и предельно допустимые нормы загрязнения окружающей среды (выбросов, сбросов загрязняющих веществ, размещения отходов) - (ст. 19 Закона РСФСР «Об охране окружающей природной среды» - в которой устанавливаются требования по лимитам природопользования)[4].

Также, исходя из данного списка, все лимиты можно разделить и на такие группы как, те, которые установлены для контроля в области добычи и использования природных ископаемых, и те, которые предназначены для обеспечения защиты мира фауны.

Деятельность человека по использованию природных ресурсов, наносит немалый вред и животному миру. Множество их видов, так же как и некоторые виды природных ископаемых уже находится на грани исчезновения, такая ситуация однозначно связана с неграмотным осуществлением своих промыслов человеком.

Для того, чтобы замедлить процесс исчезновения тех или иных видов, и привести их показатели в стабильное положение, законодательством также вводятся ограничения. К примеру, устанавливаются запреты на вылов рыбы во время нереста, или запрещается охота на животных, численность которых достигла критических порогов.

Таким образом, в 21 веке сложилась ситуация, что человечество полностью зависит от экологии, а экология от человечества. Все, что позволяет нам жить комфортно и вообще видеть жизнь такой, какой мы привыкли её видеть, напрямую зависит от природных ресурсов. Благодаря взаимодействию человека с окружающей средой, появляется возможность осуществления научной и промышленной деятельностей, которые направлены на усовершенствование условий жизни. Но, к сожалению, возникает и обратная связь, то есть зависимость экологи, а точнее её состояния от деятельности людей.

Однозначно, люди осознают какой вред наносится экологии вследствие их деятельности, но пока, как уже говорилось выше, человечеству не удалось найти способов для возобновления тех ископаемых, количество которых приближается к нулю. Также, не всегда людьми используются определенные концепции и технологии, позволяющие при переработке ископаемых избежать тех или иных экологических катастроф, которые сугубо влияют как на человека, так и на окружающую среду в целом.

В результате этого и устанавливается государственное лимитирование в области природопользования. Возможно, человечеству не в скором времени удастся разработать какие - либо инновации, которые могли бы способствовать скорейшему возобновлению исчерпаемых ресурсов или стать достойной альтернативой им. Таким образом, все силы человека направлены на экономное, грамотное, расчетное пользование природным ресурсами, с цель сохранения их как можно дольше.

---

[1] Инфопедия // [Электронный ресурс] https://infopedia.su/9xc9e8.html (дата обращения:19.10.17)

[2] "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 10.08.2017)

[3] Саркисов О.Р. Любарский Е.Л. Экологическое право: учеб. пособие для студ. учреждений высшего проф. образования . - 5 изд. - Казань: Центр инновационных технологий, 2014. - С. 79.

[4] Закон РСФСР от 19 декабря 1991 г. N 2060-1 "Об охране окружающей природной среды"

ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ – ЗАЛОГ ЖИЗНИ НА ЗЕМЛЕ

Инкина А.Н., студент
Научный руководитель: ст. преподаватель Веретина Ю.А.
ФГБОУ ВО «Оренбургский государственный аграрный университет»
г. Оренбург, Россия

В причинном комплексе экологической преступности взаимодействуют многочисленные и разноплановые обстоятельства. Наиболее общие и постоянно действующие вытекают из противоречий, присущих общественным отношениям, определяющим сущность, характер и процесс взаимодействия человека и природы. Основные из этих противоречий вызваны в последние годы негативными процессами, сопровождающими социальные и экономические преобразования, происходящие в стране. Переориентация с плановой на рыночную экономику наряду с определенными положительными результатами привела к расстыковке экономических и экологических интересов общества, государства и его граждан, ускорила процессы деградации окружающей природной среды, создала условия для развития новых реальных стимулов совершения экологических преступлений. Специфика борьбы с экологической преступностью заключается в необходимости постоянного обеспечения активных и четко скоординированных действий всех природоохранных, контрольных и правоохранительных органов по укреплению экологической законности и правопорядка.

На особом контроле находится вопрос пресечения хищений лесных ресурсов. За первое полугодие 2016 года в стране в результате незаконных рубок уничтожено более 830 000 га лесных насаждений, что выше уровня прошлого года на 67%. В переводе на квадратные километры это составляет 8300 км^2. Экологи отмечают, что фактов незаконной вырубки леса стало больше в связи с ухудшением экономической ситуации в стране.

Острее всего вопрос незаконной вырубки стоит в Сибирском, Северо-Западном и Уральском федеральных округах. При этом государственная инвентаризация лесов в стране завершена только на 30% территории, а на кадастровый учёт поставлено лишь 25,6% земель лесного фонда.

Другой, не менее значимый вопрос – свалки отходов. Их объёмы исчисляются в миллиардах тонн. Например, на Урале их накоплено около 11 млрд. тонн, в Забайкалье – почти 3 млрд. тонн. При этом в регионах Сибири и Дальнего Востока обезвреживается лишь 50% образующихся отходов. Загрязнение природной среды газообразными, жидкими и твердыми веществами и отходами производства, вызывающее деградацию среды обитания и наносящее ущерб здоровью населения, остается наиболее острой экологической проблемой, имеющей приоритетное социальное и экономическое значение.

В регионах, входящих в Арктическую зону РФ, органы прокуратуры за 2015 год – первое полугодие 2016-го выявили более 8000 нарушений законодательства в сфере обращения с отходами. Например, на территориях 7 муниципальных образований вообще нет объектов для размещения твёрдых и жидких бытовых отходов. Отсутствие системы утилизации и переработки отходов приводит к их постоянному накоплению на полигонах, несанкционированных свалках, которые не соответствуют экологическим требованиям.

Арктика имеет уникальные природно-климатические условия, в том числе флору и фауну, а также значительные запасы энергоресурсов, в первую очередь нефти и газа, добыча которых крайне сложна и опасна с экологической точки зрения. Из-за длительного зимнего периода для данных территорий характерны продолжительные распад и разложение вредных веществ, в связи с чем, долгосрочное накопление отходов недопустимо.

По данным МЧС России, на 15% территории Арктической зоны России зафиксирован критический уровень экологического загрязнения, а на Норильскую агломерацию и арктические районы освоения нефтяных и газовых месторождений Западной Сибири приходится 60% суммарного выброса загрязняющих веществ.

В этом году волонтёрский экомарафон «360 минут» прошёл не только на берегах Байкала, но также на территории восточно-сибирских заповедников «Хакасский» и «Столбы». Команды добровольцев собирали мусор у берегов 27 рек, впадающих в Байкал, а жители Иркутска бросили силы к руслу Ангары, берущей своё начало из озера. В заповеднике «Столбы» добровольцы не только собрали мусор, но и очистили более 14 м² скал от надписей, сделанных туристами и жителями Красноярска. В Хакасском заповеднике убрали береговые линии озёр Иткуль и Орловка, а также правый берег реки Абакан в Абазе. Только в одной из точек добровольцы собрали 600 мешков мусора – каж-

дый объёмом в 100 литров. Всего за один день 12 000 волонтёров собрали 27 000 мешков мусора. Чтобы вывезти такой объём на переработку или на полигоны, требуется 114 грузовиков КамАЗ[1].

Проблема ухудшения экологической обстановки рассматривается и требует профилактических мер как на федеральном, так и на региональном уровне, не исключение и Оренбургская область.

Из представленного графика следует, что число зарегистрированных экологических преступлений в 2016 году резко снизилось, и как следствие, наблюдается тенденция восстановления экологической безопасности в регионе[2]. Однако, соотнеся данные государственной статистики по Оренбургской области с данными, свидетельствующими о повышении концентрации экологически опасных деяний в Российской Федерации, необходимо отметить латентность экологических преступлений. В статистике отражается только малая часть совершаемых экологических преступлений (рисунок 1). При этом высока не только скрытая, но и скрываемая часть таких преступлений: общее количество ежегодно возбуждаемых уголовных дел по фактам выявленных преступлений в сфере экологии явно не соответствует числу сообщений о них, известных правоохранительным органам. Некоторые экологические преступления вообще не выявляются и не регистрируются, так из 18 статей УК РФ, предусматривающих уголовную ответственность за экологические преступления, широко применяются в основном только четыре: ст. 256, 258, 260 и 261 УК РФ.

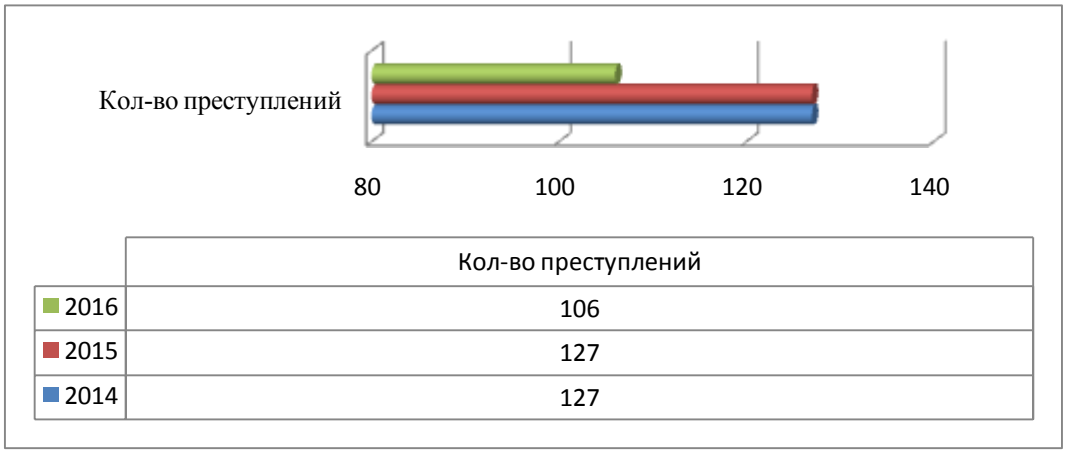

Рисунок 1 – Число экологических преступлений, зарегистрированных в Оренбургской области за 2014-2016 гг.

М.В. Зябликова основными причинами экологической преступности и ее латентности считает: неэффективность практики привлечения к ответственности за экологические правонарушения, преступления, бессистемность и хаотичность преобразований природоохранных органов, отсутствие концептуальной модели государственного управления в данной сфере, низкое кадровое и профессиональное обеспечение природоохранных и правоохранительных органов, наличие коррупции[3].

Еще одним существенным недостатком в борьбе с экологическими преступлениями является тот факт, что разграничение экологических преступлений и экологических правонарушений весьма размыто. Проблемы, связанные с применением административно-правовой и уголовно-правовой ответственности, не раз были в центре внимания ученых и практиков. Инициаторы внесения изменений в законодательство об административной ответственности за земельные правонарушения, в том числе за порчу земель, считают, что необходимо ужесточить административные наказания, установленные законом за эти правонарушения, поскольку они несопоставимы с причиняемым ущербом[4].

С подобными предложениями следует согласиться. В научной литературе также отмечается, что вследствие малозначительности сумм штрафов как главного средства административного воздействия отсутствует стабильность и последовательность в системе административной ответственности[5].

---

[1] http://greenbelarus.info/articles/09-11-2016/massovye-ekologicheskie-prestupleniya-v-rossii-178-tysyach-narusheniy-v-ekosfere

[2] http://www.gks.ru/dbscripts/cbsd/dbinet.cgi

[3] Зябликова М.В. Региональные особенности экологической преступности на Северо-востоке России: Автореф. дис. канд. юрид. наук. М, 2013. 23 с.

[4] Пояснительная записка к законопроекту № 291237-6 Федерального закона «О внесении изменений в статью 8.6 Кодекса Российской Федерации об административных правонарушениях» // СПС «КонсультантПлюс».

[5] Пацев А.А. Анализ правоприменительной практики в сфере использования и охраны земель при осуществлении застройки на территории Москвы // Российская юстиция. 2008. № 6. С. 49 - 54.

Вместе с тем, как справедливо отмечает Е.А. Галиновская, «ужесточение мер ответственности, как за порчу земель, так и за другие правонарушения может возыметь действие в том случае, если и иные механизмы установленного правопорядка – соблюдение требований по охране земель, осуществление государственного земельного надзора и муниципального земельного контроля и др. – выполняются неукоснительно»[1].

Анализируя вышесказанное, следует сделать вывод о важности совершенствования уголовного и административного законодательства в Российской Федерации, а также о необходимости постоянного обеспечения активных и четко скоординированных действий всех природоохранных, контрольных и правоохранительных органов по укреплению экологической законности и правопорядка.

ЖИЗНЬ БЕЗ ОПАСНОСТИ

Карлов В.П., к. ю. н., доцент
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

ПРАВОМЕРНОЕ ПОВЕДЕНИЕ, ПРАВОНАРУШЕНИЯ И ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ

Томас Карлейль

Станьте честным человеком, и тогда вы сможете быть уверены, что одним плутом стало меньше на свете.

Понятие и признаки правомерного поведения

С раннего детства люди начинают постигать окружающий мир, усваивать правила поведения, приобретать навыки общения друг с другом, учатся бережно относиться к чужим интересам, к окружающей среде, научаются взаимопомощи и поддержке, а также привыкают контролировать свое поведение, познают основы и тонкости разрешения конфликтов и противоречий, возникающих между людьми.

В этом им помогают законы, т.е. специальные правила, которые в интересах всех людей устанавливает государство.

Все эти правила называются правом.

Право призвано влиять на человеческое поведение, предупреждать и пресекать преступления и иные правонарушения.

Поведение людей, упорядоченное правилами законов, становится значимым для закона, т.е. имеющим юридическое значение (юридический, законный, правовой — в общем смысле синонимы).

Оно при этом может быть правомерным, то есть соответствующим закону, или противоправным, то есть нарушающим закон.

Правомерное поведение - это поведение, соответствующее праву, т.е. юридическим правам и обязанностям.

Правомерное поведение способствует положительному, бесконфликтному взаимодействию между людьми, совершенствованию общественных отношений, успешному решению стоящих перед государством и обществом задач.

Поэтому само государство заинтересовано в правомерном поведении граждан и иных лиц, обладающих правами и обязанностями (предприятия, учреждения, организации, должностные лица, органы власти, само государство).

Это достигается с помощью различных мер воздействия.

Ни одно государство не может констатировать полное отсутствие правонарушений среди своих граждан.

В действительности следует говорить о сокращении преступности до определенного уровня.

Жизнь показывает, что причиной правонарушений являются различные общественные противоречия, правонарушения совершают представители всех слоев населения.

Нередко в неблагополучных семьях вырастают прекрасные дети. Бывают и обратные примеры.

[1] Галиновская Е.А. Институт юридической ответственности как составляющая земельного правопорядка // СПС «КонсультантПлюс».

Одно из главных правил права гласит, что неприкасаемых перед законом быть не должно, наказание обязательно должно быть неотвратимым.

Так, ежегодно в Российской Федерации возбуждаются уголовные дела в отношении различных представителей власти, совершивших преступления.

При этом общий уровень преступности в Российской Федерации продолжает оставаться высоким и составляет около 230 человек на 100 тысяч населения. В европейских государствах он колеблется от 60 (скандинавские государства, Дания) до 90 человек (Испания, Англия) на 100 тысяч населения.

В 2008 году правоохранительными органами России было зарегистрировано 3209862 преступления. Состав совершенных преступлений имел следующий вид: тяжких и особо тяжких - 851392; причинивших значительный ущерб, совершенных в крупном либо сопряженных с извлечением дохода в особо крупном размере - 312093; а природоохранной сфере - 44883; террористического характера - 642; экстремистской направленности - 460; убийств и покушений на убийство - 20056; умышленных причинений тяжкого вреда здоровью - 45436; изнасилований и покушений на изнасилование - 6208; разбоев - 35366; грабежей - 243957; краж - 1326342; мошенничеств - 192490; присвоений и растрат - 72142; вымогательств - 9953.

Правонарушение

Абеляр Пьер

Никто не познает точно добродетели,
если не имеет понятия о пороке,
в особенности когда некоторые пороки
до такой степени близки к
добродетели,
что легко обманывают своим подобием.

Каждый день мы совершаем множество поступков, наиболее важные из них, те, которые вызывают какие-либо заметные последствия, совершаются на основе правил, установленных законом.

Например, когда приятели договорились пойти на рыбалку, купили снасти, но потом один из них пойти не смог, это не вызовет никаких последствий, т.к. действия и бездействие совершены на основе дружеских чувств, к проявлению которых нельзя принудить нормой права.

Однако например, покупка в магазине требует от покупателя равнозначного стоимости товара денежного возмещения, без этого она не может быть совершена.

Таким образом, закон в этом случае требует взаимного действия продавца и покупателя — один передает товар, другой его оплачивает, таким образом между продавцом и покупателем происходит обмен.

Или уголовный закон запрещает брать и обращать в личную собственность чужую вещь, деньги, устанавливая за это наказание.

Таким образом, закон в этом случае требует воздержания от действия, запрещённого законом.

Нарушение таких требований, установленных законом, называется правонарушением.

Под правонарушением, т.е. нарушением правила, установленного законом, принято понимать виновное, противоправное деяние вменяемого (т.е. осознающего свои действия и управляющего своими действиями) лица, причиняющего вред другим лицам и обществу, либо создающее угрозу причинения вреда и влекущее юридическую ответственность, т.е. меры воздействия, предусмотренные законом.

Правонарушение характеризуется строго определенными признаками (т.е. чертами), отличающими его от нарушений не правовых правил (норма, - синоним правил) (т.е. правил морали, обычаев, правил общественных организаций, которыми пользуются люди в своем общении, часть из которых являются не писанными, т.е. воспринимаются из личной практики общения с другими людьми, а часть писанными, но имеющими значение для жизни отдельных коллективов).

Из чего же складывается правонарушение, как нам разобраться, правильно мы поступаем или нет?

1. Правонарушение является ***действием или бездействием*** человека.

Не является правонарушением событие, то есть то, происходит помимо воли человека и исходит не от человека. Событие не контролируется сознанием человека и не зависит от его деятельности (землетрясение, наводнение, эпидемия и т.п.).

Действие противоправно, если оно противоречит указанному в норме закона или иного акта обязательному правилу поведения.

Бездействие противоправно, если закон предписывает, как необходимо действовать в соответствующих случаях (положениях, ситуациях), но действие не совершается.

Правонарушение может состоять только из акта поведения (действия или бездействия), внешне выраженного правонарушителем.

Нельзя считать правонарушением ***не проявленные*** через поступки (действия и бездействие) мысли, чувства.

2. ***Противоправность*** действий (бездействия) выражается в противоречии предписаниям права.

Правонарушение — это нарушение закона, его норм, содержащих юридические обязанности и запреты.

Противоправность индивидуальна, поскольку применима лишь к сознательным волевым поступкам человека, т. е. поступкам, совершенным под влиянием осознаваемого желания, намерения, побуждения.

Правовая система(то есть все упорядоченные правила поведения, выраженные в различных законах) учитывает значение руководящего начала (принципа) права:

нет правонарушения, если оно не предусмотрено законом (согласно древнему принципу римского права - разрешено все, что не запрещено законом или нет преступления без указания о том в законе).

3. ***Наличие вреда,*** это совокупность отрицательных последствий; степень общественной опасности (причиненного вреда и угрозы причинения вреда).

Правонарушение причиняет вред общественным и личным интересам, установленному правопорядку, т.е. порядку пользования своими правами и правилам защиты своих прав.

Вред выражается в отрицательных последствиях правонарушения, представляющих собой нарушение правопорядка, разлад общественных отношений и одновременно, зачастую, умаление, уничтожение благ, ценностей, права, принадлежащего лицу, ограничения возможностей пользования ими, стеснение свободы поведения других лиц вопреки закону.

Вред или угроза его причинения - непременный признак каждого правонарушения.

Он может носить ***материальный*** (вещественный) или ***моральный*** (невещественный, в виде физических или нравственных страданий) характер, быть измеримым или несоизмеримым, восстановимым или невосстановимым, более или менее значительным, ощущаемым отдельными гражданами, коллективами или обществом в целом.

Та или иная характеристика вреда зависит от видов нарушенных интересов, конкретных прав, отношений, связей между участниками общественных отношений.

4. ***Вина*** является обязательным признаком правонарушения, ее называют субъективной частью правонарушения, т.е. индивидуальным внутренним(субъективным, личным) отношением лица к совершаемому правонарушению.

Вина — это индивидуальное внутреннее (т.е. психическое, происходит от слова Психея - душа) отношение правонарушителя к своему противоправному поведению. Различают две формы(способа выражения) вины: умысел и неосторожность.

Умысел (умышленная вина) имеет место тогда, когда лицо, совершающее правонарушение, понимает, предвидит и желает наступления общественно вредных последствий своего поведения и своей волей совершает преступные действия (бездействие).

Умысел бывает двух видов: прямой и косвенный.

Прямой умысел состоит в осознании правонарушителем общественно вредного характера совершаемого им деяния, предвидении возможности или неизбежности наступления противоправного результата, причинной связи между ними и желания их наступления.

Косвенный умысел устанавливается в том случае, если правонарушитель осознавал противоправность своего деяния, предвидел противоправный результат, но не желал его наступления, хотя сознательно допускал или относился безразлично к его наступлению.

Неосторожность, как и умысел, также бывает двух видов:

преступление признается совершенным **по легкомыслию**, если лицо предвидело возможность наступления общественно опасных последствий своих действий (бездействия), но без достаточных к тому оснований самонадеянно рассчитывало на предотвращение этих последствий.

Преступление признается совершенным **по небрежности**, если лицо не предвидело возможности наступления общественно опасных последствий своих действий (бездействия), хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия.

Правонарушителями не являются малолетние и душевнобольные люди.

В Российской Федерации законодательно определены следующие требования к возрасту граждан, подлежащих юридической ответственности:

за административные правонарушения - с 16 лет;

за уголовные преступления - с 16 лет (умышленные преступления),

за часть наиболее распространенных или тяжких преступлений с 14 лет.

В то же время ни государство, ни общество не могут оставлять безнаказанными общественно опасные преступные деяния, совершенные малолетними (до 14 лет) гражданами.

Например, законодательством Российской Федерации предусматривается возможность направления малолетних правонарушителей или детей с отклоняющимся от нормального поведением в специальные школы открытого и закрытого типов, несовершеннолетних правонарушителей для воздействие на их поведение могут поместить на срок до одного месяца в специальные центры.

5. Обязательно между правонарушением и действием должна быть причинная связь.

Причинная связь означает, что вред наступил именно вследствие противоправных и виновных действий правонарушителя.

Противоправное деяние предшествует во времени последствию и является главной и непосредственной причиной, ***неизбежно*** вызывающей данное последствие.

Таким образом, по уголовному законодательству России правонарушение имеет место в том случае, если присутствуют все следующие пять его составных частей:

это действие или бездействие;

противоправный характер деяния;

наличие вреда или угрозы причинения вреда;

наличие вины;

наличие причинной связи.

ОБСТОЯТЕЛЬСТВА, ИСКЛЮЧАЮЩИЕ ПРЕСТУПНОСТЬ ДЕЯНИЯ

Государство поощряет правомерное поведение.

Для обеспечения правопорядка у государства существуют правоохранительные органы, к обеспечению правопорядка государство привлекает и граждан, создавая дружины для охраны общественного порядка.

Однако подавляющее большинство отношений между людьми возникает без прямого участия государства, представители которого не имеют возможности присутствовать лично повсюду и контролировать поведение каждого лица, однако до сведения всех участников общественных отношений общедоступным способом доводится информация о том, что за противоправные действия законом установлены различные виды ответственности.

И в отдельных случаях государство гарантирует возможность защиты прав и интересов самими гражданами при соблюдении ими соответствующих правил.

В уголовном законе такие действия граждан и других лиц называются обстоятельствами, исключающими преступность деяния и, соответственно, исключающих уголовную ответственность за такие действия, совершенные с общественно полезной целью — целью защиты лично принадлежащих лицу прав и интересов и прав и интересов других лиц, общества и государства.

Таким образом, обстоятельства, исключающие преступность деяния, - это условия, при которых деяние, внешне напоминающее преступление, в действительности таковым не является. Более того, в двух случаях причинение вреда при соблюдении определенных условий признается ***общественно полезным*** (необходимая оборона и задержание лица, совершившего преступление).

Необходимая оборона

Распространенная ситуация, когда совершается, например, нападение на человека, на учреждение, магазин с целью завладения имуществом, противоправные действия совершаются с хулиганской целью с применением насилия, по мотивам национальной, расовой, религиозной ненависти, ненависти к лицам, имеющим отличные от убеждений нападающего взгляды по различным вопросам, деяния, подрывающие безопасность государства.

В этом случае закон случае закон предоставляет право самостоятельно обороняться от нападения и не считает такие действия преступлением.

Оборона — это синоним слова защита.

Причем это защита, связанная, как правило, с применением силы.

Понятие необходимой обороны определено в ст. 37 УК Российской Федерации, согласно которой не является преступлением причинение вреда посягающему лицу в состоянии необходимой обороны, т.е. **при защите личности и прав обороняющегося или других лиц, охраняемых законом интересов общества или государства от общественно опасного посягательства, если это посягательство было сопряжено с насилием, опасным для жизни обороняющегося или другого лица, либо с непосредственной угрозой применения такого насилия (ч. 1).**

В ч. 2 приведенной статьи, помимо этого, указывается, что защита от посягательства, не сопряженного с насилием, опасным для жизни обороняющегося или другого лица, либо с непосредственной угрозой применения такого насилия, является правомерной, если при этом не было допущено превышения пределов необходимой обороны, т.е. умышленных действий, явно не соответствующих характеру и опасности посягательства.

На основании приведенных законодательных положений **необходимую оборону можно определить как правомерную защиту личности, общества и государства от общественно опасного посягательства путем причинения вреда посягающему лицу**.

Насилие — это ничем не ограниченное, не предусмотренное законом применение силы(физической и угроз) в противоправных и аморальных целях, с целью причинить боль, страдания, добиться выполнения противоправных действий, подавить сопротивление, достичь преступного и иного незаконного результата.

Необходимая оборона является субъективным (т.е. личным) правом, а не обязанностью лица, подвергшегося посягательству, поскольку связана с определенным риском для него.

Правом на необходимую оборону могут воспользоваться в равной степени все лица независимо от их профессиональной или иной специальной подготовки и служебного положения.

Для некоторых должностных лиц пресечение общественно опасных посягательств, в том числе преступлений, ***является профессиональной обязанностью.*** К таким лицам относятся сотрудники полиции, органов государственной безопасности, сотрудники таможенных и налоговых органов и др.

Право на необходимую оборону (то есть возможность обороняться) существует ***независимо*** от имеющейся возможности избежать общественно опасного посягательства, например путем бегства или уклонения от посягательства, либо возможности обратиться за помощью к другим лицам или органам власти (ч. 3 ст. 37 УК), т. е. каждый человек решает этот вопрос самостоятельно исходя их своих возможностей и конкретных жизненных обстоятельств, в которых он оказался, исходя из своих взглядов и убеждений, личных физических и моральных качеств.

Необходимая оборона называется необходимой потому, что она имеет вынужденный характер.

Обороняющийся поставлен в необходимость защищать свои права или права других лиц, интересы общества или государства самостоятельно - в отсутствие защиты со стороны государственных органов.

Условия правомерности и общественной полезности необходимой обороны делятся на две группы:

относящиеся к посягательству и относящиеся к защите.

Условия, относящиеся к посягательству.

А) Посягательство должно иметь характер **действительно (объективно) общественно опасного.**

Объективный(действительный) характер опасности посягательства означает ее оценку без учета иных обстоятельств.

Так, правомерна защита от действий явно невменяемых или малолетних лиц, совершающих общественно опасное посягательство, несмотря на то что их действия преступлениями не считаются и такие лица не могут быть привлечены к уголовной ответственности.

Уголовный закон **не допускает причинение вреда** при защите от малозначительного деяния, не обладающего общественной опасностью. Поэтому, допустим, убийство лица, совершающего малозначительную кражу (на ничтожную сумму при направленности умысла на хищение имущества именно на эту сумму), нельзя считать убийством, совершенным при превышении пределов необходимой обороны. Это простое убийство, и ответственность за него наступает на общих основаниях.

Не допускается также защита от правомерных действий, например от действий сотрудника полиции, осуществляющего обоснованное задержание преступника, или от акта необходимой обороны, если при этом не превышаются ее пределы.

В то же время защита от превышения пределов необходимой обороны и от превышения мер, необходимых для задержания лица, совершившего преступление, возможна, поскольку такое превышение общественно опасно.

Также возможна защита от неосторожного преступления.

Допустим, какой-либо гражданин наблюдает, как рабочий вот-вот сбросит строительный мусор с верхнего этажа строящегося дома вниз, где играют дети. Местоположение гражданина позволяет ему видеть и детей, и рабочего. Рабочий же детей не видит и самонадеянно рассчитывает на то, что его действиями вред никому причинен не будет. Если при попытке сбросить мусор гражданин причинит рабочему вред, бросив камень, сильно толкнув, ударив, - налицо необходимая оборона от неосторожного преступления.

Таким образом, защитное действие возможно при реальной угрозе неосторожного посягательства и может быть только умышленным.

Общественно опасное посягательство, дающее основание для использования права на необходимую оборону, делится на два вида:

опасное для жизни и **неопасное для жизни.**

К **опасному** для жизни вреду, создающему непосредственную угрозу для жизни человека, относятся, например:

проникающие в полость черепа ранения головы, в том числе без повреждения головного мозга;

перелом свода или основания черепа;

ушиб головного мозга тяжелой степени;

ранения в шею, проникающие в просвет глотки или гортани;

проникающие ранения в брюшную полость;

переломы крупных трубчатых костей;

повреждения позвоночника;

ожоги большой площади тела;

острая кровопотеря и др.

К **неопасному** для жизни вреду относятся все иные виды вреда здоровью человека, включая тяжкий вред здоровью, неопасный для жизни в момент причинения (например, потеря какого-либо органа, утрата органом функций, неизгладимое обезображивание лица и пр.), а также средней тяжести и легкий вред здоровью.

Б) Общественно опасное посягательство должно быть **наличным (то есть быть *налицо, быть очевидным*).**

Наличность посягательства означает его определенные временные рамки: посягательство уже началось, либо существует реальная угроза того, что оно вот-вот начнется, либо оно еще не завершилось.

Разумеется, ждать "первого удара" не следует, однако упреждающая защита неправомерна.

Если опасность угрожает лишь ***в более или менее отдаленном*** будущем, можно прибегнуть к иным способам защиты, обратившись, например, в правоохранительные органы, поменяв дверь в квартире или дверной замок и т.д., - в зависимости от ситуации.

Наличность посягательства отсутствует в случаях предупредительного причинения вреда, когда, например, в дачно-садовых домиках устанавливают самострелы, капканы, оставляют яд в холодильнике с целью обезопасить себя и свое имущество от похитителей.

В некоторых случаях момент окончания посягательства не ясен для обороняющегося, поскольку посягающий, например, продолжает высказывать угрозы или совершать какие-либо иные действия (пробует встать, размахивает руками, не выпускает из рук орудие), не будучи в действительности способным причинить сколько-нибудь серьезный вред.

В этом случае подвергшийся посягательству считается действующим в состоянии необходимой обороны.

Состояние необходимой обороны может иметь место и тогда, когда защита последовала непосредственно за актом хотя бы и оконченного посягательства, но по обстоятельствам дела для оборонявшегося не был ясен момент его окончания.

Переход оружия или других предметов, использованных при нападении, от посягавшего к оборонявшемуся сам по себе не может свидетельствовать об окончании посягательства" (п. 5).

В) Еще один признак посягательства - его **действительность.** Это значит, что посягательство не должно существовать лишь в воображении обороняющегося, когда он домысливает ситуацию и решает, что подвергся нападению, в то время как никаких реальных оснований для таких домыслов нет(например, у прохожего спросили время или попросили сигарету, а в его воображении разыгра-

лась сцена нападения на него, не существующая в действительности, сену такую он видел когда-то в кинофильме, знает из прессы, в данном случае под влиянием страха он ее домыслил).

В этом случае говорят о так называемой «мнимой обороне», которая не освобождает от уголовной ответственности.

Условия правомерности необходимой обороны, относящиеся к защите:

А) Допускается защита **не только собственных интересов, но и интересов других лиц, общества и государства.**

Объектами необходимой обороны могут выступать жизнь и здоровье, половая свобода и половая неприкосновенность, имущество, общественный порядок и общественная безопасность и др.

Б) Защита может выражаться лишь в **активном поведении** - действиях, причиняющих определенный вред посягающему лицу.

Пресечение общественно опасного посягательства посредством бездействия невозможно.

Защитные действия могут заключаться либо в парировании удара, либо в контрнападении.

В) Причинение вреда только **посягающему, а не третьим лицам.**

Это условие вытекает из самого содержания необходимой обороны - защиты от общественно опасного посягательства.

Уголовный закон допускает причинение вреда лишь человеку, являющемуся источником опасности для обороняющегося или других лиц, а также для интересов общества или государства.

Вред, причиняемый посягающему, может быть как физическим (причинение вреда здоровью различной тяжести или смерти), так и каким-либо иным (ограничение свободы передвижения, связывание, повреждение имущества и т.д.).

Главное, чтобы адресатом (получателем) вреда, причиняемого в ходе необходимой обороны, был непосредственно посягающий.

Причинение вреда третьим лицам влечет уголовную ответственность на общих основаниях, если его нельзя оценить по правилам крайней необходимости.

В случае, когда владелец собаки натравливает ее на прохожего, сделавшего замечание о недопустимости выгула собаки бойцовой породы без намордника и поводка, возможно причинение смерти собаке, которая с правовой точки зрения является имуществом посягающего.

В этой ситуации физический вред мог быть причинен и непосредственно хозяину собаки, если при этом не будет нарушено условие соразмерности защитных действий и тяжести посягательства.

Г) **Соответствие защиты тяжести посягательства.**

Право на необходимую оборону предоставлено всем, но использование этого права возможно с соблюдением установленных уголовным законом пределов.

Превышение пределов необходимой обороны само обладает общественной опасностью и также влечет уголовную ответственность.

Под **превышением пределов** необходимой обороны понимаются умышленные действия, явно не соответствующие характеру (например, наносятся удары человеку) и опасности (куда наносятся куда, с какой силой, их количество) посягательства.

При оценке соразмерности защиты тяжести посягательства необходимо учитывать обстоятельства, в которых осуществлялась необходимая оборона, в частности количество посягающих, их возраст и пол, физическое состояние, наличие оружия или предметов, используемых в качестве оружия, время суток, обстановку и т.д.

В случае группового посягательства обороняющийся вправе применить к любому члену группы такие меры, которые определяются опасностью и характером действий всей группы.

Если один из членов группы, совершающей, например, вооруженный разбой, угрожает применением насилия, опасного для жизни, то смерть для защиты жизни потерпевшего может быть причинена любому участнику группы.

Следует учитывать, что при необходимой обороне причиненный вред может быть несколько большим, чем тот вред, который мог быть причинен в результате общественно опасного посягательства.

Главное, чтобы причиненный вред не был чрезмерным, явно, т.е. очевидно для обороняющегося, не обусловленным тяжестью посягательства.

Превышение пределов необходимой обороны - всегда умышленное действие, что следует из его законодательного определения.

Неосторожное причинение ***в процессе необходимой обороны*** несоразмерного вреда уголовной ответственности не влечет.

Своими правами, т. е. и правом на необходимую оборону, могут злоупотреблять.

Такие случаи называются провокацией необходимой обороны и предлогом необходимой обороны.

Провокация — это обманные действия лица, направленные на вызов ответных действий другого лица с целью создать повод для нападения.

Провокация необходимой обороны имеет место в том случае, когда лицо с целью расправы провоцирует посягательство, а затем прибегает якобы к необходимой обороне.

Предлог — это недобросовестное использование своих прав, замаскированное под законные действия.

Предлог необходимой обороны - это ситуация, при которой лицо действительно подверглось посягательству, но использует это обстоятельство для сведения счетов, маскируя причинение вреда под необходимую оборону.

В этих случаях умысел "обороняющегося" приобретает иную направленность.

При необходимой обороне главная цель - пресечение посягательства, поэтому и провокация, и предлог необходимой обороны в действительности необходимой обороной не являются.

Общественно опасное посягательство, как правило, является неожиданным для обороняющегося, осуществляется в условиях, когда решение об оборонительных действиях должно быть принято быстро, иначе пресечь посягательство будет затруднительно.

Не всегда лицо, подвергшееся нападению или иному посягательству, способно адекватно и быстро оценить характер и степень опасности посягательства.

Поэтому в УК Российской Федерации включено положение, согласно которому превышением не считаются действия обороняющегося лица, если это лицо вследствие неожиданности посягательства не могло объективно оценить степень и характер опасности нападения (ч. 2.1 ст. 37).

В случае превышения пределов необходимой обороны уголовная ответственность оборонявшегося лица наступает по специальным нормам об ответственности за эти не тяжкие преступления.

Так, в УК существуют составы причинения смерти и тяжкого вреда здоровью человека при превышении пределов необходимой обороны (соответственно ч. 1 ст. 108 и ст. 114 УК).

Согласно гражданскому законодательству вред, причиненный в состоянии необходимой обороны, не возмещается (ст. 1066 ГК), т. е. денежная и иная компенсация за причиненный вред не взыскивается с причинителя вреда.

Причинение вреда при задержании лица, совершившего преступление

Причинение вреда лицу, совершившему преступление, при его задержании для доставления органам власти и пресечения возможности совершения им новых преступлений также не рассматривается как преступление при условии, что иными средствами задержать такое лицо не представлялось возможным и при этом не было допущено превышения необходимых для задержания мер (ч. 1 ст. 38 УК).

Задержание лиц, совершивших преступление, является одним из элементов (составных частей) борьбы с преступностью.

Правом задержания указанных лиц, как и правом необходимой обороны, обладает любой гражданин.

Для некоторых должностных лиц задержание лиц, совершивших преступление, как и пресечение общественно опасных посягательств, является служебной обязанностью (сотрудники полиции, федеральной службы безопасности, вневедомственной охраны и др.).

Содержание этой обязанности определяется специальными законами.

Условия правомерности причинения вреда при задержании делятся на две группы:

1) условия, относящиеся к факту совершения преступления,

2) условия, относящиеся к осуществлению задержания.

Первая группа условий характеризует преимущественно **основания задержания.**

Бесспорным основанием задержания является побег из мест лишения свободы, где лицо отбывает уголовное наказание.

Отбывание наказания свидетельствует об осуждении за ранее совершенное преступление, и, кроме того, сам побег - преступление средней тяжести (ч. ч. 1 и 2 ст. 313 УК) или тяжкое (ч. 3 ст. 313 УК).

В случаях, когда лицо еще не осуждено, основаниями для задержания служат предусмотренные в ст. 91 УПК (Уголовно-процессуального кодекса РФ) обстоятельства, при которых допустимо задержание подозреваемого лица:

1) лицо застигнуто на месте совершения преступления или непосредственно после его совершения;

2) очевидцы, в том числе потерпевшие, прямо укажут на данное лицо как на совершившего преступление;

3) на подозреваемом или на его одежде, при нем или в его жилище будут обнаружены явные следы преступления.

Основанием для задержания может служить совершение как оконченного, так и неоконченного преступления (напр., в случае, когда лицо стреляет в потерпевшего из ружья, но промахивается).

Неоконченное преступление, хотя и не влечет указанных в статье УК РФ последствий, а только создает угрозу причинения вреда, обладает общественной опасностью и дает основание для привлечения лица к уголовной ответственности.

Однако следует иметь в виду, что приготовление и покушение суть прерванные по независящим от виновного лица обстоятельствам деяния;

если же посягательство еще не прервано, а продолжается, задержание невозможно, а возможна необходимая оборона.

Условия, относящиеся к осуществлению задержания:

а) **наличие двух целей:**

1) доставление органам власти и

2)пресечение возможности совершения задерживаемым новых преступлений.

Причинение вреда при задержании в отличие от причинения вреда при необходимой обороне осуществляется не с целью пресечения общественно опасного посягательства, а главным образом **для доставления лица,** уже совершившего оконченное или неоконченное преступление, в правоохранительные органы или другие органы государственной власти.

В связи с этим ответ на вопрос о возможности причинения смерти задерживаемому лицу в процессе задержания может быть только отрицательным.

Если ставится цель доставления лица органам власти, то причинять ему смерть нельзя.

При задержании вред не может причиняться из мести, допустим, за оказанное сопротивление, совершенное тяжкое преступление или по иным каким-либо мотивам.

Второй целью причинения вреда при задержании является пресечение возможности совершения задерживаемым лицом новых преступлений.

Если осуществляется задержание особо опасного преступника, совершившего тяжкое или особо тяжкое преступление, в особенности насильственное, причинение существенного вреда задерживаемому лицу допускается, например, при его попытке скрыться.

Здесь опять-таки возникает вопрос о возможности причинения смерти такому опасному преступнику.

Вспомним финальный эпизод фильма "Место встречи изменить нельзя", в котором Глеб Жеглов стреляет в одного из членов банды, предпринявшего попытку бегством избежать задержания, и причиняет ему смерть.

Подобные ситуации отличает невозможность или крайняя затруднительность задержания.

На первое место в этом случае выдвигается цель предупреждения новых преступлений, которые предположительно могло бы совершить данное лицо. Вместе с тем в случае причинения смерти, пусть и с целью предупреждения новых преступлений, о задержании говорить нельзя.

Причинение смерти лицу не есть его задержание.

В подобных случаях необходимо говорить о другом обстоятельстве, исключающем преступность деяния, - крайней необходимости;

б) задержание лица **возможно лишь после того, как преступление стало оконченным либо было прервано по независящим от виновного лица обстоятельствам.**

До этого момента можно воспользоваться правом на необходимую оборону. Задержание осуществляется в определенных временных границах: начиная с момента окончания или прерывания преступления по независящим от виновного лица причинам;

в) **адресатом (получателем) причинения вреда** может быть только лицо, совершившее оконченное или какой-либо из видов неоконченного преступления (приготовление или покушение).

г) **причинение вреда при задержании лица, совершившего преступление, - крайнее средство**, прибегать к которому можно только тогда, когда иначе задержать преступника невозможно.

В этом сходство данного обстоятельства с крайней необходимостью. Если лицо, совершившее преступление, не уклоняется от уголовной ответственности и наказания, известны его личность и место жительства, оно в данный момент не представляет опасности для окружающих, если имеются не

связанные с причинением вреда способы задержания, причинение вреда в процессе задержания недопустимо.

Характер вреда, причиняемого задерживаемому лицу, может быть различным: ограничение или лишение свободы, связывание, надевание наручников, причинение боли или другого физического вреда различной степени тяжести, повреждение или изъятие имущества, принадлежащего задерживаемому лицу, и др.;

д) **непревышение мер, необходимых для задержания.**

В процессе задержания лица, совершившего преступление, допустимо причинение ему большего вреда, нежели тот, что причинен преступлением, за исключением превышения мер, необходимых для задержания.

Таким превышением признается **явное несоответствие** указанных мер характеру и степени общественной опасности совершенного задерживаемым лицом преступления и обстоятельствам задержания, когда лицу без необходимости причиняется явно чрезмерный, не вызываемый обстановкой вред (ч. 2 ст. 38 УК).

Другими словами, **меры задержания должны соответствовать тяжести преступления и обстановке задержания.**

Вид и сила мер задержания определяются с учетом того, на что посягает преступник, и с учетом способа совершенного посягательства, использованных орудий и средств, характера и размера причиненных общественно опасных последствий, формы и степени вины и др.

Например, при задержании лица, совершившего карманную кражу, являющуюся ***ненасильственным*** преступлением против собственности, недопустимо причинение тяжкого вреда здоровью.

Если же лицо совершило разбойное нападение и убийство потерпевшего, причинение тяжкого вреда здоровью задерживаемого правомерно.

Чем тяжелее совершенное преступление, чем опаснее личность преступника, тем больший вред ему может быть причинен при задержании.

Так, если задерживается преступник, неоднократно судимый за совершение преступлений, то ему может быть причинен более тяжелый вред, чем лицу, совершившему преступление впервые.

Следует учитывать и такие обстоятельства, как пол, возраст, состояние здоровья и другие физические данные задерживаемого лица.

Необходимо также учитывать обстановку, в которой происходит задержание.

В процессе задержания преступник может оказывать активное сопротивление, создавать своими действиями опасность для окружающих лиц, нарушать общественный порядок, препятствовать работе транспорта и т.п.

Таким образом, меры задержания определяются с учетом не только уже совершенного преступления, но и обстоятельств, в которых такое задержание осуществляется.

Например, К., совершившего карманную кражу, преследовала группа граждан и потерпевший Б.

Спасаясь от преследователей, К. забежал в подъезд дома и стал подниматься по лестнице.

В это время Б. выстрелил в него из пистолета в спину, тяжело ранив.

В такой ситуации не было необходимости в применении огнестрельного оружия, поскольку ни преступление, совершенное К., ни обстановка задержания не давали оснований для этого.

К. совершил не тяжкое преступление, посягающее на имущественные отношения, а не на личность, к тому же был безоружным.

С учетом обстановки избежать задержания ему бы не удалось.

Следовательно, вместо задержания преступника был осуществлен самосуд.

Суд, рассматривавший уголовное дело, обоснованно осудил Б. за умышленное причинение тяжкого вреда здоровью К.

Причинение смерти задерживаемому лицу в ходе задержания недопустимо, поскольку, как уже отмечалось, основная цель задержания - предать преступника правосудию.

Однако, если в процессе задержания преступник совершает общественно опасное посягательство на лиц, осуществляющих задержание, или иных лиц, возникает ситуация необходимой обороны, при которой причинение смерти возможно - при условии непревышения пределов такой обороны.

Превышение мер задержания влечет уголовную ответственность только при умышленном причинении вреда задерживаемому лицу, неосторожное превышение указанных мер непреступно.

Крайняя необходимость

Бывают случаи, когда в результате сложившейся ситуации, для предотвращения крупного и непоправимого вреда, требуется причинение вреда лицу, лицу, совершающему какие-либо опасные действия, или имуществу, способному причинить вред человеку, окружающей среде в результате утраты управления им (напр., у автомобиля отказывают тормоза и чтобы его остановить, предотвратить наезд на людей, другой автомобиль встает на пути и при столкновении причиняет вред такому автомобилю).

Таким образом, при крайней необходимости имеет место правомерное причинение вреда охраняемым уголовным законом интересам при условии, что это связано с устранением опасности, непосредственно угрожающей личности и правам данного лица или иных лиц, охраняемым законом интересам общества и государства, если эта опасность не могла быть устранена иными средствами и при этом не было допущено превышения пределов крайней необходимости (ст. 39 УК).

Но действия в состоянии крайней необходимости требуют соблюдения нескольких условий.

При крайней необходимости возникает ситуация, при которой опасность угрожает охраняемому законом благу или интересу.

Предотвратить эту опасность можно лишь путем причинения вреда другому, тоже охраняемому благу или интересу.

Если лицо в такой ситуации причиняет ***меньший вред*** по сравнению с предотвращенным, то имеет место акт крайней необходимости.

Условия правомерности причинения вреда в ситуации крайней необходимости, **относящиеся к самой опасности**:

а) **источник опасности** может быть любым: действия или бездействие людей, биологические процессы, происходящие в организме человека, поведение животных, действие стихийных сил природы, неисправности механизмов и источников повышенной опасности, столкновение (взаимное наложение) нескольких правовых обязанностей(для лиц определенных профессий, напр., врачей) и др.

Опасность может возникать в результате общественно опасного поведения человека, например при нарушении им правил дорожного движения, выразившемся в превышении скорости и повлекшем причинение тяжкого вреда здоровью человека.

Если для спасения пострадавшего в результате ДТП из близлежащего аптечного киоска изымаются перевязочные средства или лекарства, налицо акт крайней необходимости, т.к. это делается для спасения жизни человека и сохранения его здоровья, поскольку нет ничего дороже человеческой жизни.

Состояние крайней необходимости может быть вызвано биологическими процессами, происходящими в организме человека. Это голод, жажда, болезни, роды и др.

Например, заблудившийся в лесу человек использует часть продуктов, предназначенных для геологической группы;

для доставления в роддом женщины, у которой начались роды, отбирается автомобиль у его владельца;

для спасения человека осуществляется пересадка донорского(чужого, полученного на законном основании) органа или ткани.

Ситуация крайней необходимости может сложиться в результате опасного поведения животного.

Так, при съемках фильма "Невероятные приключения итальянцев в России" произошел трагический случай.

Дрессированный лев, участвовавший в съемках, был помещен на время съемок в спортзал одной из школ г. Москвы, пустовавшей в период летних каникул.

По недосмотру охраны лев смог выбраться из здания школы и стал "прогуливаться" по скверу.

В это же время с собакой вышел на прогулку мужчина. Лев повел себя агрессивно и напал на гражданина, повалив его на землю.

Дежуривший поблизости участковый сотрудник милиции (в настоящее время полиции), увидев происходящее, применил табельное оружие и застрелил льва.

В данном случае причинение смерти ценному животному было актом крайней необходимости.

Стихийные силы природы - землетрясение, извержение вулкана, цунами, наводнение, оползень, лесной пожар, вызванный молнией, разлив реки - могут создавать опасность для жизни и здоровья людей, животного и растительного мира, материальных ценностей.

Неисправности машин и механизмов, различные аварии также могут быть источником опасности, а следовательно, и основанием для причинения вреда в условиях крайней необходимости.

К примеру, радиоактивное заражение местности в результате аварии на атомной электростанции требует немедленной эвакуации людей, для чего принудительно изымается личный автотранспорт.

При отсутствии другой возможности спасения людей это следует признать правомерным причинением вреда в ситуации крайней необходимости.

Состояние необходимости может возникнуть в результате столкновения двух правовых обязанностей.

Например, врача вызвали одновременно к двум пациентам, каждому из которых он обязан оказать медицинскую помощь.

Не имея возможности оказать помощь обоим сразу, врач едет к тому, кто болен тяжелее.

В подобных случаях неоказание помощи второму больному осуществляется в условиях крайней необходимости.

При крайней необходимости в большинстве случаев угрожающая опасность устраняется путем действий.

Однако в отличие от необходимой обороны и задержания лица, совершившего преступление, которые всегда осуществляются путем действий, акт крайней необходимости может быть осуществлен и путем бездействия.

Это возможно в случаях столкновения двух правовых обязанностей: лицо предотвращает причинение большего вреда посредством неисполнения другой обязанности.

В приведенном выше примере врач, оказывая помощь одному больному, бездействует в отношении другого.

Состояние крайней необходимости может возникнуть в результате действия сразу нескольких причин в совокупности.

б) **опасность должна быть наличной**, что означает либо уже существующую опасность, либо непосредственную угрозу правоохраняемым ценностям. Это условие отсутствует, когда опасность возможна лишь в будущем. Для предотвращения будущего вреда необходимо предпринять предупредительные меры, не связанные с причинением вреда правоохраняемым интересам. Например, при возможности землетрясения заблаговременно вывезти людей и ценное имущество, при опасности пожара сделать запасы воды и песка, приобрести огнетушитель, при возможности химического отравления надеть защитный костюм или маску и т.д.

Не является основанием причинения вреда и миновавшая опасность, когда вред правоохраняемому благу уже причинен и применением акта крайней необходимости спасти такое благо невозможно. В подобных случаях возможны лишь ликвидация или минимизация последствий причинения вреда.

К **условиям, характеризующим устранение опасности, относятся следующие**:

а) **целью** причинения вреда при крайней необходимости является устранение опасности **любого вреда**: личности, имущественным отношениям, государственным и общественным интересам;

б) **неустранимость возникшей опасности иным способом** - одно из важнейших условий правомерности причинения вреда в ситуации крайней необходимости. Это означает, что при сложившихся обстоятельствах правоохраняемое благо может быть спасено только путем причинения вреда другому правоохраняемому благу, никакой другой возможности нет. Если же существуют иные способы избежать опасности, не связанные с причинением вреда, лицо должно ими воспользоваться. В противном случае не исключено наступление уголовной ответственности;

в) **адресатом** причинения вреда являются, как правило, третьи лица. Именно этим лицам может причиняться физический, экономический и другой вред. Вместе с тем необходимо учитывать, что в ряде случаев вред может причиняться и лицу, правовой интерес которого защищается актом крайней необходимости.

Так, во время свадебного торжества в доме В. начался пожар, вызванный неисправной электропроводкой. Один из гостей, действуя в состоянии крайней необходимости, сорвал со стены ковер и потушил им пламя. Путем причинения незначительного имущественного ущерба В. спас все имущество;

г) **причиненный вред должен быть меньше вреда предотвращенного. Превышением** пределов крайней необходимости признается причинение вреда, явно не соответствующего характеру и степени угрожавшей опасности и обстоятельствам, при которых опасность устранялась,

когда указанным интересам был причинен **вред равный или более значительный**, чем предотвращенный (ч. 2 ст. 39).

В отличие от необходимой обороны и задержания лица, совершившего преступление, при крайней необходимости превышением пределов признается уже причинение ***равного вреда.***

Это связано с тем, что актом крайней необходимости вред причиняется правоохраняемым интересам третьих лиц, не причастных к созданию опасности, не совершающих общественно опасного посягательства и не совершивших преступление.

Причинение равного вреда делало бы бессмысленным акт крайней необходимости, поскольку одно благо спасалось бы путем уничтожения такого же по ценности блага.

Не следует забывать и о других условиях правомерности причинения вреда в состоянии крайней необходимости, в частности о неустранимости опасности другим способом.

Может возникнуть ситуация, при которой придется сопоставлять, например, интересы личности и государства: когда, допустим, под угрозой причинения смерти требуют выдать сведения, составляющие государственную тайну. Думается, что ничто не может быть противопоставлено жизни человека, даже интересы государства, поэтому рассматриваемая ситуация должна быть разрешена в пользу интересов личности.

В соответствии с нормами морали человек не может жертвовать жизнью другого лица для спасения собственной жизни, а лишение жизни человека может быть признано актом крайней необходимости лишь в исключительных случаях, когда только таким путем можно предотвратить смерть нескольких людей.

Широко известно английское дело, насчитывающее более 120 лет.

В 1884 г. англичане Дадли, Стифенс, Брукс и юнга 17 - 18 лет оказались единственными выжившими после крушения яхты "Миньонетт" в открытом море в 1600 милях от мыса Доброй Надежды.

Оказавшись в шлюпке практически без запасов воды и еды, они стали дрейфовать.

На восемнадцатый день, когда они были седьмой день без еды и пятый - без воды, Дадли и Стифенс предложили Бруксу, намекая на юнгу, пожертвовать одним из них. Брукс отказался.

На следующий день Дадли предложил бросить жребий, однако Брукс вновь отказался.

Тогда Дадли сказал, что, если судно не появится на следующее утро, юнга должен быть убит.

Утром судно не появилось, и Дадли с согласия Стифенса, прочитав молитву, зарезал юнгу, лежавшего в крайне истощенном состоянии на дне лодки, но находившегося в сознании.

В течение последующих дней все трое питались мясом и кровью убитого.

На четвертый день после убийства они были спасены проходившим мимо судном.

Дадли и Стифенс предстали перед судом, их обвинили в тяжком убийстве, но присяжные не признали их виновными, указав, что, если бы обвиняемые не съели юнгу, они, вероятнее всего, не выжили бы; что юноша, находившийся в еще более ослабленном состоянии, скорее всего, умер бы раньше всех; что во время совершения убийства не было ни единого шанса выжить.

Впоследствии дело рассматривалось в Суде королевской скамьи, который вынес обвиняемым смертный приговор.

Однако, принимая во внимание общественное мнение, королева Виктория помиловала Дадли и Стифенса, заменив смертную казнь шестимесячным тюремным заключением.

Противоречивость судебных решений по данному делу подтверждает морально-правовую зыбкость возможности спасения своей жизни за счет жизни другого человека, хотя в приведенном деле причиненный вред меньше вреда предотвращенного: ценой жизни одного человека спасены три жизни, следовательно, акт крайней необходимости по-видимости имеет место.

В связи с большими успехами медицинских наук актуален вопрос о возможности спасения жизни многих людей путем причинения вреда одному человеку-донору.

Ученые подсчитали, что ценой жизни только одного донора можно спасти свыше 400 человек, каждый из которых находится в непосредственной опасности смерти, устраняемой лишь трансплантацией органов или тканей.

Значит ли это, что можно схватить на улице подходящего человека, расчленить его на органы и ткани и таким образом спасти несколько сот больных людей?

С зрения правил крайней необходимости вред правомерен: опасность наличная и не устранимая иным путем, вред причиненный меньше вреда предотвращенного.

Думается, что в такого рода случаях "арифметический" подсчет неуместен.

Жизнь каждого человека важна, и ее нельзя сопоставить по значимости с жизнями других людей.

В то же время, думается, что наказание человека, спасшего в состоянии крайней необходимости свою жизнь за счет жизни другого, нецелесообразно, в частности, из-за невозможности воздействовать на инстинкты человека средствами уголовного права, поскольку инстинкт самосохранения у человека чаще всего сильнее правовых предписаний.

Превышение пределов крайней необходимости влечет уголовную ответственность **только при умышленном причинении вреда**, неосторожное причинение вреда не наказывается.

Лицо может ошибочно полагать, что предотвращает более значительный вред, нежели тот, что он причиняет, на самом же деле это не так.

В этом случае действия лица вне зависимости от воли и сознания лица общественно опасны и не могут признаваться актом крайней необходимости.

Вместе с тем, если лицо не предвидело и не могло предвидеть, что причиняет вред равный или более значительный, нежели предотвращенный вред, в силу сильного душевного волнения или других причин, оно не может быть привлечено к уголовной ответственности из-за отсутствия вины.

В ситуации крайней необходимости может существовать несколько способов устранения опасности, каждый из которых сопряжен с причинением вреда правоохраняемым интересам, однако один из них более "щадящий", а другой - менее.

Лицо, устраняющее опасность, не обязано из всех способов выбирать тот, что связан с наименьшим вредом.

Самое главное, чтобы вред причиненный был меньше вреда предотвращенного.

Например, во время сильного наводнения для спасения людей разбирается деревянный дом, из которого изготавливаются плоты.

Это должно быть признано актом крайней необходимости, несмотря на то что имелась возможность сломать менее ценный дом.

В подобных случаях необходимо учитывать то, что в ситуации крайней необходимости, как правило, нет возможности выбирать наилучший способ устранения опасности, а тем более осуществлять расчет наиболее выгодного решения.

У лиц, устраняющих опасность, может не хватать соответствующих знаний, опыта и навыков.

Единственное требование, которое предъявляет законодатель к акту крайней необходимости, - это то, чтобы вред причиненный был меньше вреда предотвращенного.

Крайнюю необходимость необходимо отграничивать от необходимой обороны. Эти различия проводятся по: 1) по источнику опасности, 2) по адресату причинения вреда, 3) в зависимости от того, можно ли устранить опасность другим способом, 4) по понятию превышения пределов, 5) по социальной значимости отношений, 6) по юридическим последствиям (возможности привлечения к ответственности).

При необходимой обороне источником опасности является только общественно опасное поведение человека, при крайней необходимости источник опасности может быть любым: действия или бездействие человека, стихийные силы, столкновение обязанностей и пр.

При необходимой обороне вред причиняется только посягающему лицу, при крайней необходимости - как правило, третьим лицам. Необходимая оборона признается правомерной даже в случаях, когда у обороняющегося имелась возможность уклониться от посягательства путем бегства или обращения за помощью к другим лицам.

Крайняя же необходимость предполагает причинение вреда единственным способом устранения опасности.

При необходимой обороне вред, причиненный лицу, осуществляющему общественно опасное посягательство, может быть больше угрожающего вреда, за исключением явно чрезмерного вреда.

Крайняя необходимость правомерна только при причинении меньшего вреда: не только больший, но и равный вред недопустим.

Социальная значимость необходимой обороны состоит в том, что она по сути общественно полезна, а крайняя необходимость лишь исключает преступность деяния, поскольку при крайней необходимости вред причиняется правоохраняемым интересам.

Вред, причиненный в процессе необходимой обороны, согласно ст. 1066 ГК возмещению не подлежит, если не были превышены ее пределы.

Вред же, причиненный в состоянии крайней необходимости, по общему правилу должен быть возмещен лицом, причинившим вред (ч. 1 ст. 1067 ГК).

В некоторых случаях, учитывая обстоятельства, при которых был причинен такой вред, суд может возложить обязанность его возмещения на третье лицо, в интересах которого действовал

причинивший вред, либо освободить от возмещения вреда полностью или частично как это третье лицо, так и причинившего вред (ч. 2 ст. 1067 ГК).

Физическое или психическое принуждение

Иногда человек совершает преступление не своей волей, а в результате примененного к нему принуждения в виде насилия. И здесь требуется выяснить, мог ли человек противодействовать такому принуждению. Если он такой возможности не имел, то это является основанием, исключающим уголовную ответственность за совершенное деяние. Но для решения вопроса об этом должны существовать необходимые условия.

Так, не является преступлением причинение вреда охраняемым уголовным законом интересам в результате физического принуждения, если вследствие такого принуждения лицо не могло руководить своими действиями (бездействием).

Вопрос об уголовной ответственности за причинение вреда охраняемым уголовным законом интересам в результате психического принуждения, а также в результате физического принуждения, вследствие которого лицо сохранило возможность руководить своими действиями, решается с учетом положений ст. 39 УК (ст. 40 УК).

Причинение вреда под влиянием физического или психического принуждения предполагает ***вынужденность поступка, исключительную обстановку, в которой принуждаемый лишается возможности действовать по своему усмотрению.***

Физическое (телесное) принуждение по своему характеру и последствиям может быть различным и представляет собой непосредственное контактное воздействие на организм человека (побои, истязание, связывание или другие способы лишения возможности производить телодвижения или действия, болевая демонстрация намерений причинить смерть, порезы жизненно важных органов и тканей, имитация(создание видимости) удушения и пр.

Непреодолимое физическое принуждение, т.е. такое, при котором принуждаемый лишен возможности руководить своими действиями, поступать по своему усмотрению, исключает уголовную ответственность за причиненный принуждаемым вред (ч. 1 ст. 40 УК).

Так, во время нападения на Сбербанк один из преступников был ранен. Его приятели, сумевшие скрыться от задержания, отвезли раненого на квартиру, а затем, ворвавшись внезапно в больницу, принудили врача-хирурга прервать операцию и поехать с ними.

Выбора варианта поведения у врача не было, так как его насильно вывели из больницы и посадили в машину.

В результате прерванной операции больной умер.

В ч. 2 ст. 40 УК говорится о таком физическом принуждении, которое не исключает возможности принуждаемого руководить своими действиями.

Если при непреодолимом физическом принуждении принуждаемый лишается в определенных условиях возможности действовать самостоятельно, то при преодолимом физическом принуждении лицо сохраняет возможность действовать по своему усмотрению, т.е. руководить своими действиями, и тогда встает вопрос об уголовной ответственности за причиненный принуждаемым вред. Согласно ч. 2 ст. 40 УК этот вопрос решается по правилам крайней необходимости, т.е. по ст. 39 УК.

Помимо физического принуждения в ч. 2 ст. 40 УК говорится и о **психическом принуждении** (психическом насилии), которое в отличие от физического заключается в воздействии не на организм человека, а на психику(душу, разум) лица, его волевую сферу и осуществляется путем угроз, унижения, понуждения к выполнению или невыполнению каких-то действий и пр.

Физическое и психическое принуждение является обстоятельством, наиболее отличным от иных обстоятельств, исключающих преступность деяния.

Формальное сходство между ними сводится к отсутствию ***общественной опасности лица*** и освобождению за причиненный правоохраняемым интересам вред при невозможности руководить своими действиями в случае физического принуждения.

Различаются же эти обстоятельства весьма существенно по основаниям причинения вреда, по целям его причинения, по субъекту причинения вреда и по оценке действий принуждаемого.

Основанием ненаступления ответственности причинителя вреда при физическом и психическом принуждении является противоправное поведение другого лица, использующего методы физического или психического насилия для принуждения первого к причинению вреда.

У принуждаемого отсутствует желание не только причинения вреда, но и совершения действий, к которым он принуждается.

Принуждаемый используется при такой ситуации как орудие чужой злой воли.

Что касается психического и физического принуждения в случаях, когда принуждаемый сохраняет возможность руководить своими действиями, то такие случаи полностью подпадают под признаки ст. 39 УК и рассматриваются с позиции соразмерности причиняемого принуждаемым вреда и вреда, которым ему угрожают.

Обоснованный риск

Технический прогресс порождает ситуации, когда в различных сферах и видах человеческой деятельности требуется принятие решений, которые могут вызывать неблагоприятные последствия.

Сама такая ситуация принятия решения при не очевидности получения благоприятного результата исполнения решения называется риском.

Но иногда без риска в общественно полезной деятельности не обойтись, он сам по себе является стимул к техническому и социальному прогрессу, совершенствованию общественных отношений.

Наука уголовного права выработало понятие обоснованного риска, которое закреплено в Уголовном законе.

Обоснованный риск - это совершенные с общественно полезной целью действия, причинившие вред правоохраняемым интересам, если поставленная цель не могла быть достигнута другими, не связанными с риском действиями (бездействием), а лицо, допустившее риск, приняло достаточные меры для предотвращения вреда.

В соответствии со ст. 41 УК **основными признаками**, позволяющими отнести обоснованный риск к числу обстоятельств, исключающих преступность деяния , являются:

1) направленность действий (бездействия) на достижение общественно полезной цели (ч. 1 ст. 41);

2) невозможность достижения поставленной общественно полезной цели другими, не связанными с риском действиями (бездействием) - ч. 2 ст. 41;

3) использование достаточных и возможных мер для предотвращения вреда правоохраняемым интересам (ч. 2 ст. 41);

4) отсутствие при совершении рискованных действий угрозы для жизни многих людей, а равно угрозы экологической катастрофы или общественного бедствия (ч. 3 ст. 41).

1. **Достижение общественно полезной цели** означает такой результат рискованных действий, который одобряется моралью и правом.

Это могут быть: спасение людей, научные открытия, значительная прибыль предприятия, обеспечение безопасности общества и т.п.

Говоря об общественно полезной цели, закон имеет в виду такую цель, достижение которой имеет общественное, социальное значение, значимо для общества, хотя закон не исключает также достижение полезной цели, значимой для одного лица при соблюдении остальных условий, регламентирующих обоснованный риск.

2. Обязательным признаком обоснованного риска является **невозможность достижения общественно полезной цели иными, не связанными с риском действиями (бездействием).** Учитывая, что при совершении рискованных действий может иметь место причинение вреда правоохраняемым интересам, такие действия допустимы лишь в случаях, когда достичь поставленной общественно полезной цели иным образом невозможно. Причинение вреда при совершении рискованных действий при наличии иной возможности достижения цели означает отсутствие этого необходимого для обоснованного риска признака.

3. **Принятие достаточных мер** для предотвращения вреда означает, что приняты все необходимые, по мнению рискующего, меры, способные в конкретной обстановке предотвратить наступление вреда. Понятия "достаточность" и "недостаточность" принятых мер относятся к числу оценочных категорий, передаваемых на усмотрение правоприменителя. При этом во внимание принимаются все обстоятельства: научно-технические достижения на момент совершения рискованных действий (бездействия), уровень профессиональных знаний рискующего, его навыки и опыт, возможность правильно оценить обстановку, например, в экстремальных условиях. В ст. 41 УК говорится именно о достаточных мерах, что означает необходимость учета как объективных факторов, так и возможностей рискующего.

4. Наличие при совершении рискованных действий **угрозы для жизни многих людей, а равно угрозы экологической катастрофы или общественного бедствия** служит безусловным основанием признания рискованных действий необоснованными.

Угроза для жизни многих людей имеет место в случаях, когда в результате совершения рискованных действий возникает угроза причинения смерти значительному числу людей. Вопрос о том, какое число людей, оказавшихся в опасном для жизни состоянии, можно считать значительным, решается правоприменителем.

Угроза экологической катастрофы представляет собой создание такого состояния экологического неблагополучия, при котором страдают люди вследствие значительных отравлений атмосферы и водных источников, гибнут животные и растительность, большие территории становятся зонами экологического бедствия и чрезвычайной экологической ситуации .

Зонами экологического бедствия и чрезвычайной экологической ситуации признаются территории, на которых происходят глубокие и устойчивые неблагоприятные изменения окружающей среды, угрожающие жизни и здоровью людей, состоянию естественных природных образований.

Угроза общественного бедствия заключается в появлении опасности нарушения состояния защищенности жизненно важных интересов общества. Так, об общественных бедствиях есть основания говорить при возникновении наводнений, обвалов, возгорании лесных массивов на значительных территориях и т.п.

Можно выделить следующие признаки обоснованного риска:

1) причинение вреда интересам, охраняемым уголовным законом;

2) совершенное действие (бездействие) прямо не запрещено законом;

3) возможные вредные последствия должны быть осознаны

В зависимости от цели, к достижению которой стремится лицо, совершающее рискованные действия, можно выделить:

риск из предотвращения вреда, т.е. риск с целью предотвращения грозящей опасности, и **инициативный риск**, т.е. риск с целью достижения наибольшего профессионального эффекта, не связанного с наличием какой-либо угрозы.

Риск из предотвращения вреда может иметь место в случаях грозящей опасности в результате стихийных бедствий, техногенных катастроф и аварий и пр.

Инициативный(деятельный) риск - это риск при проведении различного рода экспериментов, усовершенствования действующих систем, постановке опытов для подтверждения сделанных открытий и пр.

Различаются несколько видов обоснованного риска в зависимости от сферы совершения рискованных действий.

Например, производственный риск, т.е. стремление достичь общественно полезной цели или предотвратить вредный результат путем поставления в опасность правоохраняемые интересы;

хозяйственный риск, т.е. стремление получить экономическую выгоду;

научно-технический риск, т.е. стремление внедрить в практику новые методики, разработки, исследования, в том числе медицинский риск.

При этом сфера обоснованного риска охватывает любую профессиональную деятельность, в том числе правоохранительную.

Обоснованный риск чаще имеет место в профессиональной сфере. Но случаи обоснованного риска могут иметь место и в бытовых условиях, в частности риск из предотвращения вреда.

Наличие изложенных ранее условий правомерности обоснованного риска исключает ответственность за причинение вреда.

Отсутствие хотя бы одного из этих условий выдвигает на первый план вопрос об ответственности за причиненный вред, при этом большое значение имеет вопрос о степени предвидения причинения вреда при совершении рискованных действий.

Крайняя необходимость и **обоснованный риск**, хотя и имеют определенное сходство, являясь обстоятельствами, исключающими преступность деяния, но это разные отношения, характеризующиеся индивидуально-определенными признаками.

1. При крайней необходимости причиненный вред является необходимым и неизбежным для предотвращения опасности, тогда как при обоснованном риске он лишь возможен.

2. При крайней необходимости больший вред должен быть предотвращен за счет меньшего вреда, тогда как при обоснованном риске такого требования не выдвигается.

3. Превышение пределов крайней необходимости влечет за собой уголовную ответственность лишь в случаях причинения вреда умышленно, тогда как при обоснованном риске возможно привлечение к ответственности за неосторожное преступление (чаще всего это имеет место при инициативном риске).

Исполнение приказа или распоряжения

Существование государства предполагает создание различных учреждений, выполняющих государственные задачи в различных сферах деятельности — обороне, борьбе с преступностью, борьбе с чрезвычайными ситуациями и т.п.

Для успешной деятельности эти государственные учреждения и их должностные лица, руководители, наделены правом требовать соответствующего поведения от других лиц, начальники от подчиненных, государственные служащие от граждан и т.п.

Эти требования выражаются в виде приказов и распоряжений, которые могут быть в устной или письменной форме и должны соответствовать закону.

Однако в сфере государственной распорядительной деятельности также могут допускаться злоупотребления, в результате чего могут быть отданы приказы и распоряжения, не соответствующие закону, противоречащие ему.

Не всегда исполнитель приказа может оценить его правомерность.

Для защиты интересов и прав личности, обществ и государства в этом случае Уголовным законом предусмотрены специальные правила.

Так, согласно ч. 1 ст. 42 УК **не является преступлением причинение вреда охраняемым уголовным законом интересам лицом, действующим во исполнение обязательных для него приказа или распоряжения. Уголовную ответственность за причинение такого вреда несет лицо, отдавшее незаконные приказ или распоряжение.**

Уголовно-правовые принципы(основные правила) правового воздействия(регулирования) на причинение вреда вследствие исполнения приказа были сформулированы в международном уголовном праве в связи с учреждением Международного военного трибунала в Нюрнберге, созданного после окончания Второй мировой войны.

Нацистские военные преступники, будучи привлеченными к ответственности, ссылались на то, что они были простым орудием незаконных приказов своих руководителей.

Вопрос об ответственности исполнителей преступных приказов был предметом специального рассмотрения трибуналом, в Уставе которого сказано: "Тот факт, что подсудимый действовал по распоряжению правительства или по приказу начальника, не освобождает его от ответственности, но может рассматриваться как повод для смягчения наказания, если Трибунал признает, что этого требуют интересы правосудия".

По такому пути пошло уголовное законодательство как ряда зарубежных стран, так и России.

Ответственность за вред, причиненный охраняемым законом правам и интересам в результате выполнения незаконного приказа (распоряжения), возлагается на лицо, отдавшее такой приказ (распоряжение), при условии что исполнитель не сознавал его незаконности.

Иная ситуация предусмотрена ч. 2 ст. 42 УК, согласно которой лицо, совершившее умышленное преступление во исполнение заведомо незаконного приказа или распоряжения, несет уголовную ответственность на общих основаниях. Неисполнение же такого приказа или распоряжения уголовную ответственность исключает.

Явно незаконное или преступное свойство приказа или распоряжения определяется не только по формальным признакам, но и по содержанию, очевидному противопоставлению приказа или распоряжения правоохраняемым интересам (например, распоряжение руководителя коммунального предприятия отключить от системы жизнеобеспечения многоквартирный дом по причине на него жалоб жильцов). Ответственность за повиновение явно преступному предписанию наступает на общих основаниях, т.е. зависит от реально наступивших последствий.

Если приказ (распоряжение) был отдан компетентным лицом с соблюдением предписанной законом формы, его исполнение не исключает ответственности, если очевиден его незаконный или даже преступный характер.

В случаях исполнения преступного приказа (распоряжения) к ответственности за вред, причиненный правоохраняемым интересам, должны быть привлечены как исполнитель приказа (распоряжения), так и лицо, отдавшее его.

Последнее является подстрекателем(возбуждением желания) к преступлению, совершенному исполнителем, естественно, при наличии умышленной вины.

Незаконность приказа (распоряжения) должны осознавать оба.

Об этом свидетельствует указание закона на признак заведомости (осведомленности заранее).

Условиями правомерности, относящимися к приказу или распоряжению, являются: 1) приказ или распоряжение отданы в установленном законом порядке, уполномоченным лицом, в пределах его полномочий;

2) приказ (распоряжение) является незаконным, так как его исполнение повлечет за собой причинение вреда правоохраняемым интересам.

Условиями правомерности, относящимися к исполнителю незаконного приказа (распоряжения), являются:

1. исполнитель не имел права (возможности) отказаться от выполнения обязательного для него приказа (распоряжения) и

2. исполнитель не осознавал незаконность отданного ему приказа, а следовательно, и того, что в результате исполнения такого приказа будет причинен вред охраняемым законом интересам.

При наличии перечисленных условий лицо, исполнившее незаконный приказ (распоряжение), в результате чего правоохраняемым интересам был причинен вред, от ответственности освобождается.

К ответственности в этих случаях привлекается, как уже отмечалось, лицо, отдавшее незаконный приказ (распоряжение).

Исполнение же незаконного приказа (распоряжения) при осознанности его незаконности рассматривается как совершение умышленного преступления.

Подводя итог, следует подчеркнуть, что основным ориентиром для правомерности совершаемых действий является признание в отношениях между людьми главными ценностями - человеческой жизни, свободы, прав и интересов человека, общества и государства, а право помогает человеку правильно выбирать то поведение, которое способствует их сохранению, сохранению мира в обществе, процветанию государства.

Материал подготовлен в рамках выполнения НИР на тему «Проблемы квалификации преступлений в уголовном праве» (науч. рук. – д. ю. н., профессор Якушин В.А.).

ПРАВОВЫЕ ОСНОВЫ ЛИЧНОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ РЕАЛИЯХ

Кузнецова А.Д., студент
Научный руководитель: д-р пед. наук, доцент Ронжина Н.В.
Российский государственный профессионально-педагогический университет
г. Екатеринбург, Россия

Эмма Ротшильд говорила: «Безопасность – это условие, благодаря которому становится возможным все остальное». Другими словами, личная безопасность представляется собой состояние защищенности таких интересов общества, которые обеспечивают стабильное развитие государства, то есть возможность выявления и предотвращения угроз национальным интересам.

Действительно, благодаря безопасности возможно развитие государства и благоприятная жизнь его граждан. Именно поэтому основной составляющей национальной политики государства является личная безопасность.

Уверенно говорить о способности гражданина защитить как самого себя, так и своих близких и окружающих в настоящее время невозможно, поскольку радикализм, религиозная, этническая нетерпимость приводят сегодня к конфликтам, правонарушениям и даже преступлениям.

Особое место в современных реалиях занимает один из разновидностей террористической деятельности – религиозный терроризм. Данный феномен имеет ярко выраженную особенность – основанием противоправной деятельности религиозных экстремистов являются религиозные нормы. Религиозный терроризм имеет специфические идеологические основы, социальную базу, организацию и т.п.

Таким образом, деяния приверженцев религиозного экстремизма становятся наиболее кровавыми. Уничтожение врагов для религиозных фанатиков превращается в священный долг, в осуществление божественной воли. Религия, таким образом, легитимирует террор. И чем больше жертв приносится во имя бога, тем лучше, по мнению идеологов терроризма, выполняется миссия «борцов за веру». [3, с. 13].

В целом религиозный терроризм имеет признаки общественно-опасного социально-политического явления.

Но понятие «религиозный терроризм» имеет достаточно условный характер, поскольку основные религии мира в их традиционном каноническом содержании не совершают террористических актов, не призывают к нему, провозглашая, наоборот, целый ряд высоконравственных постулатов [9, с. 158-159].

Официального термина «религиозный терроризм» не существует, что создает проблему изучения взаимообратной связи терроризма и религии. Во многих литературных источниках можно обнаружить различные формулировки данного феномена: «исламский терроризм», «христианский терроризм» и т.д. Но невозможно с уверенностью утверждать, что данные формулировки являются правильными, так как в основе любой религии (в том числе в исламе и христианстве) лежит

гуманизм, что вследствие по определению не дает возможности объединения понятий «религия» и «терроризм».

М.П. Требин считает возможным говорить о квазирелигиозной составляющей терроризма. Он объясняет свою позицию следующим образом: «В основе любой религии лежит вера в Бога, который един для всего сущего, но имен у него много, так как человек всегда стремится узурпировать право на истину, в том числе и в вопросах духовной жизни. Но в любом случае дух всякой религии основан на уважении, любви и терпимости ко всему живому [4, с. 98].

Исходя из всего вышесказанного, считаем, что формулировку феномена «религиозный терроризм» стоит заменить на «терроризм религиозных экстремистов». Так, в основе террористической деятельности лежат религиозные экстремистские учения антигуманного направления, использующие религиозные положения в качестве инструмента легализации терроризма.

Наличие противоречий в каноническом содержании, в том числе неточность формулировок религиозных обязанностей и требований, а также не единообразное толкование и применение религиозных догм способствует прикрытию экстремистской деятельности за счет религии.

Также стоит отметить такое явление как религиозный фанатизм.

Религиозный фанатизм понимается как неявный метод религиозной практики, основанный на состоянии полной поглощенности (тотальной суженности) религиозного сознания идеей Спасения и нацеленный на максимальную эффективность религиозной деятельности в процессе достижения Спасения [2, с. 48].

Социальной опасностью такого явления как религиозный фанатизм является полная трансформация создания, возможность манипулирования личностью, а также высокая социальная мобильность религиозных фанатиков.

Таким образом, можно сделать вывод, что такие явления как терроризм религиозных экстремистов и религиозный фанатизм бесспорно представляют опасность современному обществу и требуют разработки путей предупреждения и ликвидации негативных последствий терроризма религиозных экстремистов и религиозного фанатизма.

По нашему мнению, одним из таких путей может быть усиленное культурно-религиозное просвещение в общеобразовательных учреждениях и в средствах массовой информации, наравне с пропагандой развития здорового образа жизни, культуры и экологии. Суть должна заключаться в донесении до населения различного возраста информации о различных религиях, делая акцент на опасности таких учений, которые поддерживают и легитимируют терроризм.

В связи с тем, что существует возможность интерпретации религиозных норм с разных точек зрения, что является проблемой в условиях усиливающегося терроризма, имеет смысл решить данный вопрос с позиции права, так как согласно п. 43 Стратегии национальной безопасности, утвержденной Указом президента Российской Федерации от 31 декабря 2015 г. № 683, основными угрозами государственной и общественной безопасности являются: деятельность радикальных общественных объединений и группировок, использующих <…> религиозно-экстремистскую идеологию, иностранных и международных неправительственных организаций <…>, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, включая инспирирование «цветных революций», разрушение традиционных российских духовно-нравственных ценностей [6].

Поскольку целями экстремистов, прикрывающих свою деятельность под религиозными нормами могут быть как защита конфессии, реорганизация общественной мысли, создание религиозного государства, так и осуществление целей политического терроризма: завладение государственной властью либо изменение внешней и внутренней политики государства, необходимо государственное вмешательство.

Согласно ст. 28 Конституции РФ [1] каждому гарантируется свобода совести, свобода вероисповедания, включая право исповедовать индивидуально или совместно с другими любую религию или не исповедовать никакой, свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними.

Но п. 3 ст. 55 Конституции РФ гласит о том, что права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Таким образом, есть основание для регулирования государством такого социального института как религия.

Так, с точки зрения права, существуют нормы, способствующие реализации безопасного существования человека в современном обществе. В РФ правовая безопасность личности от внешних посягательств закреплена в таких нормативных правовых актах как:

- Конституция РФ;

- Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». В четвертой главе Указа отражены стратегические национальные приоритеты государства, в том числе в п. 44 указано, что главными направлениями обеспечения государственной и общественной безопасности являются совершенствование правового регулирования предупреждения преступности, коррупции, терроризма и экстремизма.

- Федеральный закон «О противодействии терроризму», который устанавливает основные принципы противодействия терроризму, правовые и организационные основы профилактики терроризма и борьбы с ним, минимизации и ликвидации последствий проявлений терроризма, а также правовые и организационные основы применения Вооруженных Сил РФ в борьбе с терроризмом [7].

-Уголовный кодекс РФ, в 24 главе которого закреплена ответственность за преступления против общественной опасности [5].

- Федеральный закон «О свободе совести и о религиозных объединениях» от 26.09.1997 №125-ФЗ (далее ФЗ №125) регулирует правоотношения в области прав человека и гражданина на свободу совести и свободу вероисповедания, а также правовое положение религиозных объединений, в том числе особенности их гражданско-правового положения [8].

В главе 3 Закона говорится о запрете осуществления миссионерской деятельности, цели и действия которой направлены на:

-нарушение общественной безопасности и общественного порядка;

-осуществление экстремистской деятельности;

-посягательство на личность, права и свободы граждан;

-нанесение установленного в соответствии с законом ущерба нравственности, здоровью граждан, в том числе использованием в связи с их религиозной деятельностью наркотических и психотропных средств, гипноза, совершением развратных и иных противоправных действий;

-склонение к самоубийству или к отказу по религиозным мотивам от оказания медицинской помощи лицам, находящимся в опасном для жизни и здоровья состоянии;

-воспрепятствование угрозой причинения вреда жизни, здоровью, имуществу, если есть опасность реального ее исполнения, или применения насильственного воздействия, другими противоправными действиями выходу гражданина из религиозного объединения;

-побуждение граждан к отказу от исполнения установленных законом гражданских обязанностей и к совершению иных противоправных действий и некоторых других.

Согласно ФЗ №125 надзор за исполнением законодательства РФ о свободе совести, свободе вероисповедания и о религиозных объединениях осуществляют органы прокуратуры РФ.

Считаем, что необходимо создавать условия для установления связи между федеральным органом государственной регистрации, органами прокуратуры РФ и учредителем (представителем) религиозной организации для усиления осуществления контроля за соблюдением религиозной организацией законодательства РФ о свободе совести, свободе вероисповедания и о религиозных объединениях, а также целей и порядка деятельности, предусмотренных ее уставом, при осуществлении федерального государственного надзора за деятельностью религиозных организаций. Усиление контроля позволит выявить и предотвратить еще на ранних стадиях развитие террористических (экстремистских) организаций, скрывающихся под религиозным объединением.

Таким образом, можно сделать вывод, что проблема терроризма религиозных экстремистов и религиозного фанатизма является актуальной и ставят под угрозу безопасность гражданина.

Но российское государство контролирует сферу предупреждения преступности, терроризма и экстремизма, гарантированные стратегией национальной безопасности и осуществляет попытки обеспечения личной безопасности граждан через совершенствование нормативной правовой базы Российской Федерации.

Библиографический список

1. Конституция Российской Федерации от 12.12.1993г. (в ред. от 21.07.2014 г.) // Российская газета. 1993. 25 декабря.

2. Кузнецова, М.Н. Религиозный фанатизм: понятие, сущность и пути преодоления дис. … канд. филос. наук. Омск, 2003. 171 с.

3. Пушков, А.К. Россия, безопасность, терроризм: Круглый стол // Свободная мысль – XXI в. 2001. № 12. С.13.

4. Требин, М.П. Терроризм в XXI. Минск: Харвест, 2004. 816 с.

5. Уголовный кодекс Российской Федерации от 13.06.1996 г. №63 -ФЗ (в ред. от 19.12.2016 г.) // Российская газета. 1996. 25 июня.

6. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 1 (часть II). Ст. 212.

7. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 06.07.2016) «О противодействии терроризму» (с изм. и доп., вступ. в силу с 01.01.2017) // Российская газета. 2006. 10 марта.

8. Федеральный закон от 26.09.1997 № 125-ФЗ (ред. от 06.07.2016) «О свободе совести и о религиозных объединениях» // Российская газета. 1997. 01 октября.

9. Юргенсмайер, М. Понимание нового терроризма // Текущая история. Терроризм. 2000. № 636. С.158-159.

ПРИОРИТЕТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ РОССИИ

Рыжакова Д.Г., Каракаев Д.Г., студенты
Научный руководитель: к. п. н., доцент Исакова Т.Б.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Актуальность темы исследования обусловлена тем, что в последние годы в современной России часто поднимается вопрос о приоритетах национальной безопасности.

Цель исследования: рассмотреть национальную безопасность как условие устойчивого развития и существования (жизнедеятельности) личности, общества и государства, сохранения духовных и материальных ценностей и раскрытие механизма обеспечения безопасности.

Базовым документом стратегического планирования, определяющим национальные интересы и национальные приоритеты РФ, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности РФ и обеспечение устойчивого развития страны на долгосрочную перспективу является Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»[1].

В данном документе отмечается, что обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:

– оборона страны;
– государственная и общественная безопасность;
– повышение качества жизни российских граждан;
– экономический рост;
– наука, технологии и образование;
– здравоохранение;
– культура;
– экология живых систем и рационального природопользование;
– стратегическая стабильность и равноправное стратегическое партнерство.

Укрепление национальной безопасности обороны страны обеспечивает физическое существование государства, его защиту от внутренних и внешних угроз.

Повышение качества жизни, укрепление здоровья населения обеспечивает стабильное развитие страны, общества, личности.

Сохранение и развитие культуры обеспечивает сохранение традиционных российских духовно-нравственных ценностей.

Повышение конкурентоспособности национальной экономики способствует закреплению за Россией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях мира.

[1] Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»

Проведенный анализ позволил констатировать, что реализация приоритетных направлений национальной безопасности является условием устойчивого развития и существования личности, общества и государства.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ПРАВОВОЙ ЗАЩИТЫ ЧУВСТВ ВЕРУЮЩИХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Седнин Д.А., студент
Научный руководитель: д-р пед. наук, доцент Ронжина Н.В.
Российский государственный профессионально-педагогический университет
г. Екатеринбург, Россия

Проблемы безопасности государства, общества, разных социальных групп, наконец, личности – это вопрос правовых гарантий, закрепленных в законодательстве страны по отношению к каждому из названных субъектов. Особенно остро сегодня встает вопрос о правовом регулировании безопасности личности в зависимости от таких факторов, как вероисповедание (христианство – ислам), цвет кожи (белый – темный), вид деятельности (умственный – физический), материальный доход (богатые и бедные), уровень образования и др. Следует признать, что толерантность сегодня присуща далеко не всем людям, и многие конфликты возникают именно на этой почве. Одной из серьезных причин такой опасности, как в России, так и в Европе в целом, являются миграционные процессы. Столкновение разных цивилизаций, культур, религий, нравов и обычаев порождают в настоящее время ряд сложнейших противоречий, способом разрешения которых должно быть разумное правовое регулирование, а также формирование нового мировоззрения в поликультурном, поликонфессиональном обществе.

Множество народов при миграции оказываются в других странах с другим законодательством и, главное, культурой, создавая свои коалиции, национальные диаспоры. Но если государство добровольно осуществляет миграционную политику, то его заботой должно являться и обеспечение этих мигрантов всем тем, в чем у них есть духовная потребность, в частности, обеспечение доступа к религиозным священным местам, возможность отправлять религиозный культ. И поэтому недопустимо унижение, игнорирование религиозных взглядов представителей других религий и мировоззрения (в т ом числе научного, атеистического). Главное, чтобы деятельность мигрантов не противоречила законодательству той страны, в которой они проживают. Второй стороной выступает безопасность граждан страны, принимающей мигрантов – также со своей культурой, религией, традициями и т.д. Проблема равновесности взаимоотношений коренного населения и мигрантов – важнейшая проблема для европейских стран и России сегодня.

В связи с обозначенной проблемой хотелось бы остановиться на правовом регулировании, с одной стороны, конституционного права граждан на свободу совести и вероисповеданий и, с другой стороны, зашиты чувств верующих. В Российской Федерации в ряде нормативно-правовых актов имеется урегулирование данного вопроса, в частности, Ст. 29 Конституция РФ провозглашает свободу вероисповедания, Ст.148 УК РФ говорит о воспрепятствовании осуществлению права на свободу совести и вероисповеданий; в Ст. 282 УК РФ речь идет об ответственности в связи с возбуждением ненависти либо вражды, а равно унижении человеческого достоинства; КоАП РФ в Ст. 5.26 регулирует нарушения законодательства о свободе совести, свободе вероисповедания и о религиозных объединениях. Таким образом, существует правовое регулирование представленной проблемы. Однако, появилась необходимость в изменении Ст.148 УК РФ в плане уточнения ответственности за оскорбление чувств верующих.

Исследователи данной проблемы в связи с этим обращают внимание на ряд противоречий: нет четкого определения понятий «кощунство», «оскорбление религиозных чувств», «вандализм» и др. Сложно привлечь к ответственности лиц, использующих социальные сети. Вот ряд судебных дел, которые говорят о сложности названной проблемы.

Решение по делу 5-1052/2016 (16.11.2016, Судебный участок №109 Осинского муниципального района). Гражданин Х., используя страницу в социальной сети Интернет «В контакте», разместил публично в свободном доступе карикатуры на Пресвятую Богородицу, на икону «Знамения», а также на Распятие Спасителя Иисуса Христа, оскверняющие предметы религиозной и мировоззренческой атрибутики Русской Православной церкви.

В судебном заседании лицо, в отношении которого ведется дело об административном правонарушении, пояснил, что негативно относится к РПЦ, так как священнослужители не выполняют

свои обязанности, прихожане ничего не знают о своей вере. В целях развлечения и общения он размещал на своей странице «В контакте» карикатуры, не считая их оскорбительными. Данные карикатуры брал из сети Интернет, которые размещены в свободном доступе, он лишь переместил их на свою страницу пользователя «В контакте». Копию протокола об административном правонарушении не получал.

Потерпевший Y. пояснил, что является настоятелем Троицкого собора в г. Оса. К нему обратились десятки людей, прихожан церкви, несовершеннолетние ученики воскресной школы с сообщением о размещении в сети Интернет в свободном доступе карикатур на святыни православной церкви. Изображения комментировались нецензурными выражениями. Такие карикатуры оскорбляют чувства верующих, являются глумлением над памятью предков. В связи с этим гражданин Y. обратился в правоохранительные органы для защиты религиозных святынь и чувств верующих.

Руководствуясь ст. 29.9, 29.10 КоАП РФ, суд постановил признать гражданина X. виновным в совершении административного правонарушения, предусмотренного ч. 2 ст. 5.26 КоАП РФ, и назначить административное наказание в виде административного штрафа в размере 50 000 (Пятьдесят тысяч) рублей.

По Делу № 1-37/2017 гражданин Сафиуллин М.Ф. подозревается в незаконном воспрепятствовании деятельности религиозных организаций или проведению богослужений, других религиозных обрядов и церемоний.

Судом было установлено, что 26 февраля 2017 года Сафиуллин М.Ф. публично, явно проявляя неуважение к обществу ,зашел в православный храм Андрея Блаженного Симбирского Чудотворца, где стал громко кричать и привлекать к себе внимание, чем сорвал проходящее там в это время богослужение. В действиях Сафиуллина М.Ф. усматриваются признаки преступления, предусмотренного ч. 3 ст. 148 УК РФ – незаконное воспрепятствование деятельности религиозных организаций или проведению богослужений, других религиозных обрядов и церемоний.

На основании изложенного, руководствуясь ст.76.2 УК РФ, ст.ст. 25.1, 446.3 УПК РФ, суд постановил: назначить Сафиуллину М.Ф.1 меру уголовно-правового характера в виде судебного штрафа в размере 10 000 (десять тысяч) рублей.

Весьма показательным является дело в отношении к блогеру В. Краснову в феврале 2016 года, проживающему в г. Ставрополе. Виктор Краснов в споре в социальной сети «В Контакте» написал, что «Бога нет», а Библию назвал «сборником еврейских сказок». Экспертиза признала Краснова вменяемым. В феврале 2017 года дело было закрыто в связи с истечением срока давности.

В апреле 2016 г. Кировский районный суд Екатеринбурга направил местного жителя Антона Симакова на принудительное лечение в психиатрическую клинику. В октябре 2014 г. Симаков в своем офисе провел «обряд» с использованием куклы вуду, крови жертвенного животного, а также предметов христианского культа. Симаков вышел из больницы в январе 2017 года.

В апреле 2016 г. Оренбургский суд оштрафовал на 35 тыс. руб. преподавателя Оренбургского медицинского университета Сергея Лазарова. В 2013 г. в статье «Злой Христос», опубликованной на сайте Лазарова, в отношении Христа были приведены негативные эпитеты – «убийца» и «тиран» и др.

В июле 2016 года Кировский областной суд признал виновными по ст. 148 УК РФ Константина Казанцева и Рустема Шайдуллина. По версии следствия, они повесили самодельное чучело с оскорбительной надписью на поклонный крест в деревне Старая Малиновка. Каждый получил по 230 часов исправительных работ.

В июле 2016 года Элистинский городской суд приговорил к двум годам условно спортсмена из Дагестана Саида Османова. Османов в буддийском храме ударил статую Будды и помочился на нее, а после выложил видео в интернет.

В августе 2016 года Соколовский выложил ролик, в котором играет в игру Pokemon Go в Храме-на-Крови в Екатеринбурге. Поводом для этого послужил сюжет телеканала «Россия 24», где утверждалось, что «ловлю покемонов» в церквях можно трактовать как оскорбление чувств верующих. Соколовский решил это опровергнуть, и после публикации ролика на него завели уголовное дело. 3 сентября 2016 года Соколовского отправили в СИЗО, позже меру пресечения изменили на домашний арест.

11 мая Верх-Исетский районный суд Екатеринбурга приговорил блогера Руслана Соколовского к трем с половиной годам лишения свободы условно с испытательным сроком в три года, а также к обязательным работам. Судья Екатерина Шепоняк признала Соколовского виновным в возбуждении ненависти (часть 1 статьи 282 УК РФ), оскорблении религиозных чувств верующих (часть 1 статьи 148 УК РФ) и незаконном обороте технических средств негласного получения информации (статья

138.1 УК РФ). Государственный обвинитель Екатерина Калинина просила для блогера три с половиной года колонии общего режима [ ].

Основанием для обвинительного приговора стало, в том числе, отрицание Соколовским существования Иисуса Христа и вообще бога.

Обобщая материалы судебной практики, можно сказать, что Статья 148 УК РФ носит довольно размытый характер. Представляется весьма непростым делом определить, задеты ли чувства верующего человека или задеты ли они вообще, или же это просто проявление свободы слова. Сейчас всё чаще реализуется такая политика государства, что при любом негативном высказывании в сторону религии, даже без цели кого-либо обидеть, задеть или возбудить вражду, человека можно привлечь к ответственности, в том числе и уголовной, просто потому, что он так выражает свое мнение, реализуя свободу слова и печати. Естественно, нельзя допускать, чтобы одни люди публично оскорбляли то, что свято другим, но и лишать свободы за выражения своего мнения тоже нельзя. Полагаем, что необходимо конкретизировать статью 148 УК РФ, как, например, предложил депутат Госдумы Олег Смолин, а именно: внести изменения в Уголовный кодекс по ч. 1, ст. 148 «Нарушение права на свободу совести и вероисповеданий», а именно конкретизировать место и обстоятельства, при которых могут быть нарушены права верующих. Поэтому законопроектом предлагается четко определить, как и каким образом могут быть затронуты чувства верующих. Политик отмечает, что из контекста УК РФ и Конституции следует, что публичные действия неуважительного характера могут оскорблять религиозные чувства, только если они мешают или препятствуют богослужениям или другим церемониям. По этим доводам депутат предлагает дополнить закон формулировкой, которая будет уточнять, что чувства верующих могут быть нарушены только при проведении религиозных мероприятий.

После принятия данного законопроекта будет, наконец, понятно, что значит оскорбить чувства верующих, когда, где и каким образом это можно сделать. Осознание этого позволит более чётко понимать и применять статью 148 УК РФ и, вследствие этого, не нарушать её.

Библиографический список

1. Материалы судебной практики: [Электронный ресурс] – Режим доступа: https://rospravosudie. com/law.

РЕАЛИЗАЦИЯ НОРМ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ В ОБЛАСТИ ИСПОЛЬЗОВАНИЯ ЗЕМЕЛЬ В РФ

Пулукчу У.А., студент
Научный руководитель: к. ю. н., доцент Галеева Г.Р.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Земля как основа жизни и деятельности народов составляет фундамент национального благосостояния Российской Федерации. Конституция РФ относит вопросы владения, пользования и распоряжения землей к совместному ведению России и её субъектов, соответственно возлагая на государство обязанность по охране земли[1]. Тем более, что в современных непростых условиях, в том числе внешних санкций целью Российской Федерации является не только рационализировать сферу землепользования, но и защитить экономические интересы будущих поколений россиян.

Для достижения поставленной цели необходимо совершенствование правового регулирования ответственности за правонарушения в области использования и охраны земель. В целом правовые нормы, определяющие обязанности собственников земельных участков, установлены ЗК РФ и другими федеральными законами и соотнесены с требованиями норм юридической ответственности за неисполнение данных обязанностей[2]. Привлекая к ответственности за правонарушения в области использования и охраны земель, законодатель стимулирует исполнение обязанностей по их

[1] См.: Конституция РФ, ст.72. ч.1, ст.9. ч.1 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[2] См.: Земельный Кодекс РФ. ст.ст. 44–47, 74–76 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017); Кодекс РФ об административных правонарушениях. ст.ст. 7.1., 7.2., 8.6., 8.8. [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017); Гражданский Кодекс РФ. ст.ст. 285–287 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017); Уголовный Кодекс РФ. ст. 254 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

рациональному использованию и охране. При этом предполагается не только предупредить действия, противоречащие требованиям установленного землепорядка, но и способствовать осуществлению законной деятельности по использованию земель и их охране. Таким образом, нормы о юридической ответственности направлены, в первую очередь, на восстановление земель.

Однако, реализация норм юридической ответственности по приведению земельного участка в надлежащее состояние может быть затруднена уже при определении правонарушения и виновных лиц. Препятствия касаются как недостаточной эффективности выполнения органами государственной власти и органами местного самоуправления своих функций по контролю и надзору, так и несовершенства самого правопорядка в области землепользования. Так, право собственности и иные права на землю принудительно прекращаются в случае нецелевого использования земельного участка[1]. Также земельный участок можно изъять у собственника, если участок предназначен для ведения сельского хозяйства либо жилищного или иного строительства и не используется по целевому назначению в течение трех лет, если более длительный срок не установлен законом[2]. Известно, что использование земельных участков не по целевому назначению, невыполнение обязанностей по приведению земель в состояние, пригодное для использования по целевому назначению законодатель определяет как административное правонарушение[3]. При этом, если по каким — либо причинам категория земли документально не подтверждена, то и привлечение к ответственности за ее нецелевое использование не представляется возможным.

Случаи ошибок и нарушений оформления категории земель при кадастровом учете[4] и в правоустанавливающих документах обращают внимание на противоречие законодательства о целевом использовании земель и законодательства о кадастре недвижимости. Так, законодатель относит к дополнительным сведения о категории земель и разрешенном их использовании[5]. При этом, на практике данные сведения в кадастровые документы могут быть и не внесены. Таким образом, фактически допускается образование и использование земельного участка без четко установленного его целевого назначения при сохранении норм, позволяющих привлечь к ответственности за несоблюдение установленной категории земель.

Подобные трудности возникают при привлечении к юридической ответственности за несоблюдение положений законодательства о разрешенном использовании земельных участков. Порядок установления вида разрешенного использования земельного участка законодательно закреплен[6]. Однако, не определены виды разрешенного использования для значительного числа земельных участков (например, для земель сельскохозяйственного назначения, земель особо охраняемых природных территорий, земель лесного фонда). Также при кадастровом учете есть случаи установления разрешенного использования земельного участка по его фактическому использованию. Вследствие чего о юридической ответственности за несоблюдение порядка такого «разрешенного использования» речь идти уже не может.

Состав правонарушения «неиспользование земель по целевому назначению» предполагает отслеживание качественного состояния земли как природного ресурса и природного объекта. Сложности возникают при определении факта неосуществления законодательно закрепленной хозяйственной деятельности на земельном участке. Правительство РФ лишь отчасти обеспечивает

---

[1] См.: Гражданский Кодекс РФ. ст. 285 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017); Земельный Кодекс РФ. ст.ст. 46, 454 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[2] Гражданский Кодекс РФ. ст. 284 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[3] Кодекс РФ об административных правонарушениях. ст. 8.8. [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[4] См.: Федеральный закон от 24.07.2007 № 221-ФЗ «О кадастровой деятельности» [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[5] Федеральный закон от 13.07.2015 № 228—ФЗ «О государственной регистрации недвижимости» Ст.8, п.5 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017

[6] См.: Градостроительный кодекс Российской Федерации. ст. 37 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

Постановление Правительства РФ от 23 апреля 2012 г. N 369 "О признаках неиспользования земельных участков с учетом особенностей ведения сельскохозяйственного производства или осуществления иной связанной с сельскохозяйственным производством деятельности в субъектах Российской Федерации" [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

контролирующие органы критериями нецелевого использования сельскохозяйственных земель[1]. Также осложнено привлечение к юридической ответственности за использование земельного участка способами, существенно снижающими плодородие сельскохозяйственных земель или значительно ухудшающими экологическую обстановку[2], за использование земельного участка с грубым нарушением законодательно установленных правил рационального использования земли[3]. Во всех случаях, чтобы определить правонарушение необходимо оценить состояние земельного участка и окружающей среды. Однако правил рационального использования земель законодательство РФ не содержит. При отсутствии единых правил не представляется возможным определить и критерии их грубого нарушения. Власти субъектов РФ пытаются урегулировать вопрос о критериях самостоятельно[4].

Таким образом, эффективность системы регулирования юридической ответственности в области использования земель как части механизма правового воздействия на земельные отношения в целом должна быть обеспечена, в том числе дальнейшим совершенствованием земельного правопорядка в РФ.

[1] Постановление Правительства РФ от 23 апреля 2012 г. N 369 "О признаках неиспользования земельных участков с учетом особенностей ведения сельскохозяйственного производства или осуществления иной связанной с сельскохозяйственным производством деятельности в субъектах Российской Федерации" [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[2] Земельный Кодекс РФ. ст.ст. 45, 46 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[3] См.: Гражданский Кодекс РФ. ст. 285 [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

[4] См.: Закон Самарской области от 11.03.2005 № 94 «О земле» и др. [Электронный ресурс] // СПС КонсультантПлюс (Дата обращения 23.10.2017)

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УДАЛЕННОГО ДОСТУПА

Абрюков А.А., студент
Научный руководитель: преподаватель Васильева С.Н.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

«Информационные надомники» или, по-другому, удаленные пользователи информационных систем – явление в современности вполне привычное. С каждым годом число таких пользователей значительно увеличивается. Это проявилось и оставило свой след даже в языке - в обиходе технического английского закрепились слова telecommuter и teleworker.

Информационные ресурсы и коммуникация на основе удаленного доступа ныне общедоступны. Раньше «надомник» пользовался только модемом на коммутируемой линии (являющийся до сих пор бюджетным и общедоступным предметом), а на сегодняшний день чаще всего встречаются GPRS, xDSL, стремительно увеличивается доступность мобильных сервисов 3G, являющиеся относительно дешевыми, высокоскоростными и надежными.

Если ныне проблемы коммуникаций фактически являются решенными, становятся значимыми задачи организации информационной защиты пользователя, работающего на расстоянии.

В связи с этими задачами возникают следующие вопросы: какие существуют особенности использования удаленного доступа относительно обеспечения безопасности информации? Как все-таки обеспечить защиту удаленному пользователю и в чем ее отличия от защиты пользователя офисной сети?

Удаленное рабочее место сопровождается тремя сверхштатными рисками и угрозами:

1. Деятельность удаленного пользователя физически не контролируется и не регулируется организацией. Пользователю приходится для получения доступа к узкогрупповому источнику доказывать, что он не является злоумышленником.

2. Информация об отдаленном пользователе рассеиваются по каналам, находящимся за пределами зоны управления организацией. Они рискуют быть перехваченными и модифицированными без ведома пользователя.

3. Организации становится непосильна задача обеспечения физической защиты места работы пользователя на расстоянии. Присутствует все тот же риск похищения данных, к тому же, такое рабочее может не соответствовать конфигурации, которую требует организация.

Из вышеперечисленного вытекает вопрос, – как же можно уменьшить, либо совсем предотвратить, влияние негативных факторов?

По моему мнению, сегодняшние способы защиты информации могут гарантировать вполне достойную защиту удаленного рабочего места. В данной статье и излагаются воззрения на разрешения подобной задачи.

Нахождение основных методов защиты удаленного доступа

На сегодняшний день наблюдается конкуренция между технологиями надежности сетевого и транспортного уровня (IPsec и SSL/TLS соответственно).

Для понимания того, чем же различаются эти технологические решения, водится определенная классификация: SSL или TLS; SSL (TLS) VPN.

Первоначально заметим, что три этих архитектуры эксплуатируют схожий по постоянности комплект криптографических алгоритмов. Следовательно, решения допустимо считать практически идентичными по критерию криптографической стойкости.

Отметим, что решение IPsec как достаточно гибко, так и весьма сложно в применении и реализации, касаемо коммуникационного протокола. В основе этого решения трафик приложений отправляется на сетевую ступень в виде пакетов. Они собираются, зашифровываются и подписываются.

Протокол Internet Key Exchange служит для регулирования ключей и координации политики безопасности.

SSL/TLS VPN менее желателен, по сравнению с IPsec VPN согласно отчету компании, The Burton grou.

SSL/TLS в классической схеме нельзя отождествить с VPN.

По информации одного из новейших словарей IETF, VPN - это «способ использования открытых или частных сетей таким образом, чтобы пользователи VPN были отделены от других пользователей и могли взаимодействовать между собой, как если бы они находились в единой закрытой сети».

SSL/TLS – образцовое решение и не подходит под это определение. Оно гарантирует засекреченность и общность единичного транспортного соединения.

Другие приложения дают проход к «незакодированным» портам и посылают публичный, неконтролируемый трафик.

В системах защиты глобального удаленного доступа существует крупная проблема, когда нельзя установить каждому посетителю частный VPN-клиент и замены браузеру, использующему SSL или TLS соединения, нет. Поэтому, все приватные сети, такие как электронная коммерция, банковские клиентские сети используют SSL/TLS соединения в браузере.

IPsec же наоборот, представляет архитектуру, полностью компенсирующую функции VPN. Весь трафик в нем сообщается сквозь специализированные транспортные порты в виде подписанных зашифрованных IP-пакетов, которые туннелируются через не доверенные сети. Из-за этого доступ к сети получает узкий круг обладателей ключей, сеть становится взломать практически нельзя.

Технологии SSL/TLS VPN распространились не так давно, примерно пять лет назад. VPN продукты создавались для удешевления и упрощения использования VPN решений. Но не всегда все в данной ситуации оказывается гладко, возникаю нюансы, например, то, что VPN разделился на так называемый «псевдо» и «честный», сильно отличающиеся по свойствам друг от друга.

БЕЗОПАСНОСТЬ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 7

Букша Я.О., студент
Научный руководитель: к. т. н., доцент Куралесова Н.О.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Большинство пользователей WindowsXP, в своё время не поторопившейся сменит ОС на Windows-Vista, возможно, приняли верное решение. В интервью, представитель Microsoft Стив Баллмер выразил свои мысли по этому поводу «Если люди хотят подождать, они, безусловно, могут это сделать». Достоинства новой ОС Windows7, стоят того, чтобы перескочить WindowsVista, тем более, на тот момент ждать осталось совсем не долго.

В офисах разработки ПО обещанные сроки обычно трудно соблюдать, но обстоятельства того, что срок действия бета-версии Windows 7 (build 7000), предоставленной для массового тестирования в первых числах января, подходит к концу первого августа, по всей вероятности это свидетельствует о скором появлении полноценной ОС после конечной даты

Наша гипотеза также подтверждается обращением главы Compal Рея Чена о том, что Microsoft может начать старт продаж своей новой ОС Windows 7 уже в конце июля 2009 г. Сама организация Microsoft не подтвердила и не опровергла эти высказывание. По официальной информации предоставленной Билом Вехте, Microsoft ранее рассчитывала закончить операционную системуWindows7 в начале 2010года, но в скором времени последовало несколько сообщений о том, что новая операционная система может появиться на несколько месяцев раньше изначально запланированного срока.

Одна из главных задач, стоявших перед разработчиками Windows7, состояла в сокращении размеров и снижении требований к оборудованию по сравнению с её младшей версией. Предполагается, что новая ОС сможет без проблем запускаться на нетбуках, и, наконец, заменит WindowsXP. Эффективность и возможность использовать для подвижных работников более дешёвые устройства являются главным достоинствами новой ОС, но далеко не последним.

Немалую работу компания Microsoft выполнила для повышения уровня безопасности систем, которые будут строиться на базе Windows 7. Рассмотрим основные новые и переработанные прежние возможности этой операционной системы.

UAC

Вызывавшая немало нареканий технология UserAccessControl в новой версии ОС переработана. Основным её неудобством было то, что необходимость лично подтверждать все потенциально опасные действия программ в среде Vista даже при установке вполне легитимного программного продукта сопровождалось многократными запросами пользователю на подтверждения действий.

Чтобы сделать Windows 7 более дружественной к пользователям, разработчики Microsoft решили ввести 4 уровня контроля, в том числе «не оповещать никогда», «оповещать при заведомо

опасных действиях», «оповещать, только когда программа пытается внести изменения в систему» и самый строгий уровень «оповещать всегда». По умолчанию в финальной версии Windows 7 будет установлен «оповещать, только когда программа пытается внести изменения в систему». По мнению некоторых специалистов, такое значение по умолчанию, являющееся более слабым по сравнению с прошлой версией, отрицательно скажется на безопасности, однако не стоит забывать, что в WindowsVista пользователи, устав от постоянных нажатий на кнопку подтверждения, нередко полностью отключали механизм UAC, оставляя свою систему незащищенной.

DirectAccess

Использование виртуальных частных сетей (VPN – VirtualPrivateNetwork) стало стандартом для организации безопасного доступа удалённых пользователей к корпоративным ресурсам. Новая технология DirectAccess позволяет отказаться от традиционных решений по построению VPN, которые нередко вызывали нарекания со стороны конечных пользователей из-за своей ненадёжности и нестабильности. С использованием DirectAccess доступ к предоставленным в совместный сетевой доступ файлам в локальной сети и корпоративным приложениям становится возможным сразу, как только компьютер подключается к сети Интернет. При интернет-трафик пользователя автоматически перенаправляется на внешние адреса и «не смешивается» с трафиком, предназначенным для корпоративных ресурсов.

DirectAccess работает и в обратном направлении: администраторы имеют возможность удалённо управлять компьютером с Windows 7. В частности, обновлять настройки групповых политик и устанавливать обновления программного обеспечения каждый раз, когда пользователь соединяется с Интернет, даже если работа при этом осуществляется под локальной учётной записью. Такое решение, по мнению Microsoft, позволит более эффективно управлять компьютерами, которые редко подсоединяются непосредственно к корпоративной сети. DirectAccess для Windows 7 работает только совместно с DirectAccessserver, в роли которого выступает WindowsServer 2008 R2.

AppLocker

С использованием данной технологии администраторам гораздо проще, чем это было раньше запрещать и разрешать использование приложений на рабочих местах под управлением Windows 7. Тонкие настройки, в том числе с привязкой к конкретной версии ПО, позволяют снизить риски от потенциально опасных программ, запускаемых пользователями без ведома администратора.

BitLocker

Решение по шифрованию дисков, появившееся ещё в WindowsVista получило дальнейшее развитие в новой операционной системе. В частности, упростился интерфейс — зашифровать целиком весь жёсткий диск можно просто нажав на его имени правой кнопкой мыши и выбрав нужный пункт меню. Важнейшим нововведением стало появление BitLockerToGo, с помощью которого теперь можно зашифровать внешние устройства, такие как USB-диски, USB-флэш и другие. Windows 7 может быть настроена таким образом, что будет запрещать копирование на незашифрованные внешние устройства.

Разновидности

Данные новшества будут доступны не во всех вариантах новой операционной системе, а лишь в некоторых. Детали приведены в таблице 1:

Таблица 1 - Новшества новой операционной системы

	Starter, Home Basic, Home Premium	Professional	Enterprise	Ultimate
Подключение к домену	-	+	+	+
Remote Desktop	-	+	+	+
BitLocker	-	-	+	+
AppLocker	-	-	+	+

Главное отличие Windows7-Enterprise и Ultimate состоит в версиях приобретения (Windows7-Enterprise нельзя будет приобрести в розницу) и лицензирования (для Windows7-Ultimate не предусмотрена возможность объемного лицензирования). Для пользователя стремящегося иметь весь перечень функций, без необходимости подписания полного контракта как раз и посвящена Ultimate-версия — своего рода Enterprise-версия, предназначенная для владельцев домашнего ПК.

Вывод

Любые новоявленные намерения, помимо этапа разработки подразумевают тщательное тестирование и их реализации, именно поэтому Microsoft постоянно выкладывает во всеобщий доступ бета-версии своих товаров. Согласно результатам промежуточных тестирований бета-версии Windows7

тестеры нашли более двух тысяч неисправностей и недоработок в операционной системе, которые Microsoft обязалась исправить к моменту выхода финальной версии. Вместе с тем, новая операционная система довольно стабильна и, в отличие от WindowsVista, на нескольких миллионах ПК, примененных для тестирования во всём мире, на 75% аппаратахWindows7 с первого старта начала стабильно работать и только для оставшихся ПК, надо было загрузить драйвера через WindowsUpdate или с сайта разработчика. Такое отменное свойства продукта дает возможность рассчитывать на высококачественную реализацию продукта и рассмотренных методик.

Библиографический список

1. Дейтел, Х.М. Операционные системы. Ч. 2: Распределенные системы, сети, безопасность / Х.М. Дейтел, П.Дж. Дей - тел, Д.Р. Чофнес. – М.: Бином, 2006.

2. Дейтел, Х.М. Операционные системы. Ч. 1: Основы и принципы / Х.М. Дейтел, П.Дж. Дейтел, Д.Р. Чофнес. – М.: Би-ном, 2006.

3. Гордеев, А.В. Операционные системы: учебник для вузов / А.В. Гордеев. – СПб.: Питер, 2004. – 416 с.

4. Олифер, В.Г. Сетевые операционные системы / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2001. – 544 с.

5. Танненбаум, Э. Современные операционные системы. 2-е изд. / Э. Танненбаум. – СПб.: Питер, 2002. – 1040 с.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ДВИЖЕНИЯ, РЕАЛИЗОВАННОЕ С ПОМОЩЬЮ STEP7 И КОТРОЛЛЕРА SIEMENS S7-300

Васильев А.С., Сандров С.В., студенты
Научный руководитель: ст. преподаватель Плюснина Е.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Программируемый логический контроллер (PLC – Programmable Logic Controller) - устройство, используемое для автоматизации технологических процессов. В отличие от встроенных систем и микроконтроллеров, PLC производится как самостоятельный продукт, отдельно от управляемого им оборудования. В системах управления технологическими процессами PLC взаимодействуют с различными компонентами систем человеко-машинного интерфейса (например, панели оператора) или рабочими местами операторов ПК. Датчики и приводы подключаются напрямую к большинству PLC или к дополнительным модулям входов/выходов.

В настоящей статье основное внимание уделяется информационной безопасности промышленных контроллеров. Интерес исследователей к различным уязвимостям в этих устройствах растут с каждым днем. И вот почему: эта категория информационно-управляющих систем находятся как можно ближе к «грубому оборудованию» - машинам, технологическому оборудованию, исполнительным механизмам электростанций, системам транспортировки нефти и газа, проще говоря, к устройствам, нестандартная работа (или просто блокировка) которых, может привести к последствиям, сопоставимым с результатами саботажа.

На сегодняшний день существующие подходы к элементам информационной безопасности APCS (Automated Process Control System) недостаточны из-за особенностей архитектуры и свойств, программных и аппаратных элементов, это предоставляет злоумышленнику множество векторов влияния на технологические автоматизированные системы.

В элементах APCS, его составной программно-аппаратной базе, были обнаружены множественные уязвимости, что может привести к нарушению правильной работы технологического процесса и внедрение угроз несанкционированного доступа к информации, обработанной в:

−системах контроля и сбора данных (SCADA);

−элементах телеметрических подсистем и телемеханики;

−программных приложениях для анализа производственных и технологических данных;

−системах управления производством.

Чтобы заниматься защитой APCS, нужны высококвалифицированные специалисты, которые понимают архитектуру этих систем и их функциональность, способные анализировать конкретное ПО, строить сценарии развития событий в случае нарушений и информировать владельцев технологических процессов о информационной безопасности в понятых терминах. Необходим

тщательный анализ лучших практик в соответствии с западными стандартами безопасности для контроля процесса, грамотного перевода и адаптации уже существующих стандартов безопасности.

Информационная безопасность - это непрерывный процесс. Изменение бизнес-процессов, появление новых угроз и открытие новых уязвимостей, именно поэтому, по крайней мере, один раз в год необходимо проводить анализ рисков, аудит и анализ существующих систем безопасности с целью их дальнейшего совершенствования.

Программируемые контроллеры Siemens SIMATIC S7 широко используются в системах автоматизации во всех отраслях современного промышленного производства. Удобство и надежность конструкции, простота монтажа и эксплуатации, высокая производительность, мощные коммуникационные возможности, способность поддерживать обмен данными через Интернет, PROFIBUS, Industrial Ethernet и MPI делают технические устройства данной серии незаменимыми при решении задач автоматизации разных уровней сложности. А большой выбор модулей контроллеров Siemens SIMATIC S7 позволяет максимально адаптировать любую аппаратуру для решения любой производственной задачи (рисунок 1).

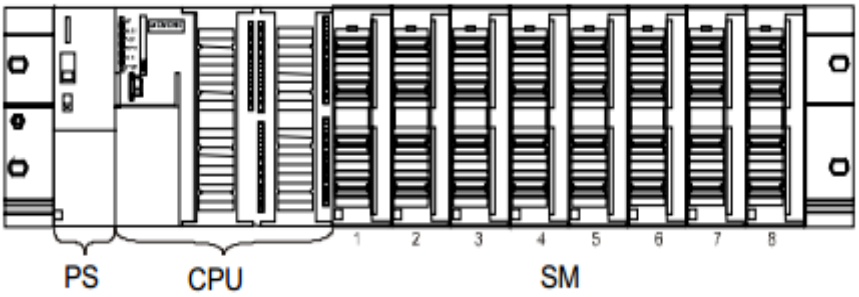

Рисунок 1 - Контроллер SIMATIC S7-300

Siemens SIMATIC S7-300

Модульный контроллер стандартного исполнения для работы в нормальных промышленных условиях. Используется для создания систем автоматизации средней степени сложности. Системы на основе этого типа контролера могут обслуживать от 16 до 65536 дискретных входов/выходов.

Экспериментальная часть

Поставленной задачей является использование контроллера SIEMENS S7-300 для управления светофорами на перекрестке.

Задача заключается в создании периода работы светофора. В каждом направлении (1 и 2) перехода есть два больших светофора и два маленьких светофора. Большой светофор для транспортных средств состоит из трех светов: красного (БК), желтого (БЖ), зеленного (БЗ).

Маленький светофор для пешеходов состоит из двух светов: красного (МК), зеленного (МЗ). В одном периоде работы светофоров большая зеленная лампа 1 горит в течение 10с, в то время маленький светофор 1 находится в красном состоянии. Потом большой светофор 1 переходит на желтое состояние в течение 2с для предупреждения водителям об остановке. После того большая красная 1 горит на 12с, чтобы остановить транспортные средства. А в то время маленькая зеленная лампа 1 горит на 8с для разрешения пешеходов. Эта лампа не сразу горит после большой красной лампы, так как надо запасное время для безопасности. Период работы светофоров продлится 24с. Для направления 2 очередь горений ламп совсем наоборот (рисунок 2).

Десять ламп светофоров D1, D2...D10 подключат к выходам контроллера. Лампы D1, D2, D3, D6, D7, D8 соответствуют зеленным, желтым, красным лампам больших светофоров в направлениях 1 и 2. Лампы D4, D5, D9, D10 соответствуют зеленным, красным маленьких светофоров в направлениях 1 и 2.

Используя пакет STEP 7, мы пишем программу для управления системой светофора на перекрестке.

STEP7 - это программное обеспечение для программирования S7-300/400. Для организации работы по конфигурированию, программированию и тестированию программной части системы автоматического управления процессами служит утилита SIMATIC Manager. SIMATIC Manager – это приложение, работающее под управлением Windows и содержащее все функции, необходимые для создания проекта. При необходимости SIMATIC Manager инициирует запуск других утилит, например, для конфигурирования станций, для инициализации модулей или для написания и тестирования программ.

Сначала мы создадим сигнал с частотой 1 Гц с помощью блока Timer T1 и T2. Сигнал с частотой 1 Гц входит в блок счетчика C0, который считает время периода работы системы светофоров. Значение выхода счетчика (MW2) входит в блок сравнения, которые сравняет с распределенными временами для каждого лампы. Выходы блока сравнения идут в вход сигнала лампы.

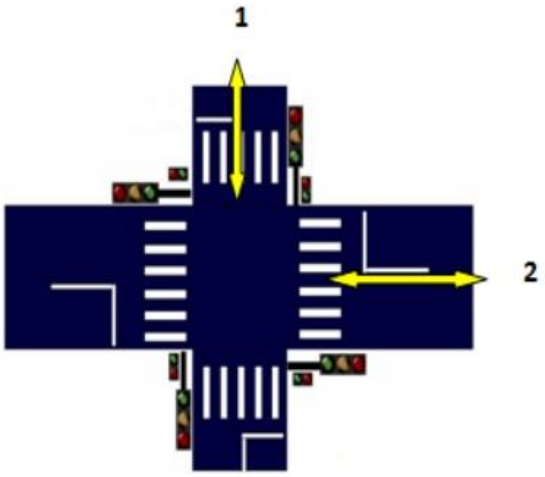

Рисунок 2 - Схема распределения времени для светофоров

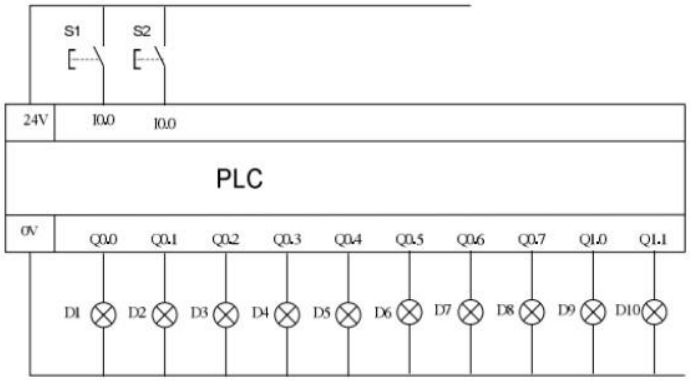

Рисунок 3 - Схема подключения входов-выходов контроллера

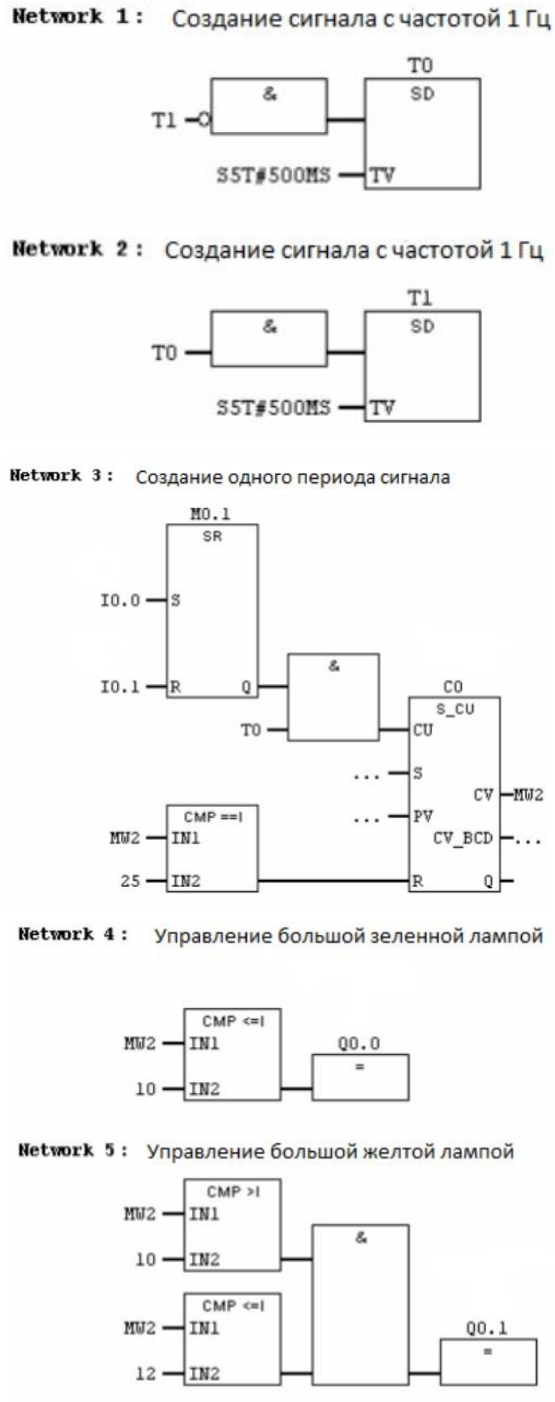

Рисунок 4 - Блочная программа

Заключение

При использовании контроллера S7-300 и пакета STEP 7 управление системой светофоров на перекрестке облегчиться и станет более точным. Перспективой этого проекта является создание единого центра управления транспортом. Диспетчеры центра будут следить за транспортной ситуацией во всем городе в метро на автомобильных и железных дорогах, а также на вокзалах и транспортно-пересадочных узлах.

Библиографический список

1. Бергер, Г. Автоматизация с помощью Программ STEP7 LAD и FBD. Siemens AG, 2001. – 605 с.

2. Программирование с помощью STEP7 V5.3.–Siemens AG, 2004.–682 с.

ФУНКЦИОНАЛ И БЕЗОПАСНОСТЬ WINDOWS SERVER 2012

Городецких Л.П., студент
Научный руководитель: к. т. н., доцент Трубачева С.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

К решению фундаментальных задач, которые современный бизнес ставит перед ИТ, в первую очередь требуется последовательный и комплексный подход. Конечной задачей организации является возможность эффективно использовать все преимущества современных бизнес-приложений независимо от их размещения — на собственной инфраструктуре, в частном или публичном облаке, или любой их комбинации.

Функционал и безопасность Windows Server 2012

Windows Server 2012 воплотила в себе опыт компании Microsoft в области создания глобальных центров обработки данных, которые включают сотни тысяч серверов и предоставляют более чем 200 облачных сервисов.

Она содержит в себе весь необходимый стек новейших технологий для создания легко масштабируемой, простой и экономически эффективной серверной платформы, и в первую очередь обеспечит необходимую гибкость выбора стратегии использования и развития ИТ-инфраструктуры.

Современная платформа виртуализации. Windows Server 2012 предлагает динамичную платформу с разделяемой архитектурой, которая позволяет выйти за пределы традиционной виртуализации и обеспечивает свободу выбора в построении серверной инфраструктуры, будь то собственный ЦОД, частное облако, в том числе и для оказания услуг, или организация взаимодействия с публичными облачными сервисами.

У***ниверсальная, масштабируемая платформа для WEB и приложений***. Windows Server 2012 — универсальная, масштабируемая платформа для WEB и приложений. Позволяет легко, удобно и безопасно обеспечить пользователей доступом к привычной рабочей среде независимо от используемого устройства и местоположения.

Удобство и эффективность управления. Windows Server 2012 упрощает задачи управления с помощью применения политик распределения ресурсов, что позволяет ИТ-подразделению быстрее реагировать на изменяющиеся потребности. Windows Server 2012 демонстрирует значительные улучшения в масштабируемости и производительности за счет новых возможностей Hyper-V и вывода ряда процессов на аппаратный уровень, что помогает ИТ-подразделениям и сервис-провайдерам, при неизменных физических ресурсах, повышать их эффективность и поддерживать больше рабочих нагрузок. Повышая производительность, масштабируемость и надежность виртуализованных сред.

Инновационные решения на базе облачной модели, повышенный уровень безопасности. Windows Server 2012 помогает организациям использовать инновационные решения на базе облачной модели. Windows Server 2012 обеспечивает повышенную безопасность и надежность взаимодействия между географически удаленными сетями и публичным облачным сервисам, расширяя единую систему идентификации, управления и обеспечивая повышенную защиту информации. Функции расширенного подключения, включают в себя:

федерация систем идентификации Active Directory Federation Services, позволяющая распространить единую идентификацию Active Directory на географически удаленные сети, в том числе и публичные облачные сервисы. Пользователю достаточно один раз пройти идентификацию, чтобы получить доступ к локальным и облачным ресурсам и сервисам;

компоненты ОС, функционал которых обеспечивает взаимодействие между географически удаленными сетями, являются частью возможностей удаленного доступа, встроенных в Windows Server 2012, обеспечивают повышенную безопасность соединений, в том числе и с публичными облачными сервисами;

компоненты ОС, функционал которых, обеспечивая подключение к облачным сервисам, расширяет возможности использования приложений, расположенных локально.

Выводы

Windows Server 2012 помогает организациям выйти за пределы базовых технологий и функций виртуализации и создать комплексную платформу для построения частного облака, предоставляя высокоэффективные сервисы своим заказчикам, внутренним или внешним.

Windows Server 2012 представляет собой открытую web-платформу, предоставляющую ИТ-специалистам гибкость при построении многопользовательских приложений для локального разме-

щения или на базе публичных облачных сервисов. С помощью функций, сервисов и инструментов ОС, хостинг-провайдеры и крупные организации могут повысить плотность, упростить управление и достичь большей масштабируемости при создании разделяемой среды, повысить безопасность используемой системы.

Библиографический список

1. Моримото, Рэнд. Полное справочное руководство Windows Server 2012.
2. Minasy, Mark Windows Server 2012 R2. Изд. Sybex. -2014.
3. Tomas, Shinder Windows Server 2012 Security from End to Edge and Beyond. Изд. Syngress. -2013.

ЗАЩИТА ДАННЫХ 1С: ПРЕДПРИЯТИЯ

Иванов А.В., студент
Научный руководитель: к. п. н., доцент Горбачевская Е.Н.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Информационная безопасность 1С.

Исторически сложилось так, что продукт 1С: Предприятие стал самым распространенным на территории стран бывшего СССР. Каждая вторая организация использует продукты 1С для ведения учета и управления предприятием. А как обстоят дела с безопасностью 1С? Откровенно говоря, в версии 7.7 внимание безопасности не уделялось вообще. С выходом 8.2 версии платформы отношение разработчиков к защите информации улучшилось незначительно. Существует две основных реализации работы программы: файловый вариант и клиент-серверный. Каждый из них имеет массу уязвимостей, как общих, так и особенных.

Рассмотрим файловая вариант работы программы.

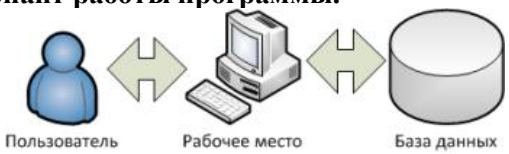

Рисунок 1 – Файловый вариант работы программы

Работа и хранение базы данных организованы на одном рабочем месте. При такой реализации говорить о безопасности 1С вообще не приходится. Конфигурация и база данных хранятся на локальном диске, который доступен для записи и чтения информации любому пользователю операционной системы. Это дает неограниченные возможности по обходу системы защиты самой 1С. База программы может находиться и на сетевом диске, что только усложняет вопрос обеспечения ее безопасности. При всем этом сохранность и целостность данных организации обеспечивается только средствами программы 1С.

Рассмотрим вариант клиент – серверный работы программы.

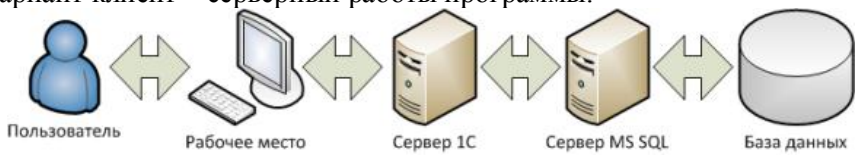

Рисунок 2 – Клиент – серверный вариант работы программы

Из схемы работы сетевого варианта отчетливо видно большое количество звеньев системы. На каждом таком этапе обработки и пересылки информации существуют свои угрозы, которые могут способствовать хищению коммерческих данных, их повреждению, или вероятности выхода из строя как отдельных, так и некоторых звеньев:

1. простые пароли пользователей (хранение паролей на листочках, приклеенных на рабочем месте);
2. доступ пользователей к административным действиям конфигуратора;
3. уязвимости операционной системы и СУБД;
4. отсутствие разграничений прав доступа в 1С;

5. возможность доступа к данным сервера СУБД;
6. вирусы, шпионские программы;
7. перехват информации;

В платформе 1С: Предприятие есть встроенный язык программирования, посредством которого выполняется разработка конфигурации, ее доработка или модернизация под нужды предприятия. В этом языке есть готовые объекты и классы для работы с протоколами HTTP, FTP, SMTP и POP3, файловой системой, реестром Windows, медиафайлами и онлайн медиапотоками, системными процессами, базами данных и XML, ресурсами локальной сети и другим.

Данный факт дает широкие возможности потенциальным злоумышленникам: от написания безобидных модулей для просмотра фильмов в самой 1С или интернет-серфинга, до отправки коммерческой информации через электронную почту или протокол FTP прямо из программы 1С. Также, платформа активно использует компоненты интернет-обозревателя Internet Explorer, о уязвимостях которого не говорил лишь ленивый.

На рисунке 3 показан принцип взаимодействия данных с программой 1С:Предприятие на сервере.

Рисунок 3 – Принцип взаимодействия данных с программой 1С: Предприятие

Так, например, были случаи, когда «нечестный» рекламный баннер внедрял в Internet Explorer свой модуль. Все бы ничего, но при запуске 1С загружался этот модуль и передавал информацию своему владельцу.

Другой пример. Множество компаний сейчас предлагают удаленное использование 1С через интернет из любой точки мира. Подключение происходит в терминальном режиме, где запрещено все, кроме 1С. Защита, казалось бы, идеальная. Только достаточно воспользоваться типами встроенного языка 1С для работы с файлами и реестром — ограничения сняты. Мы получаем доступ к файловой системе, сетевому обмену, базам данных, в том числе к чужим базам, которые через протокол SMTP можем отправить себе на почту.

Корпоративным облаком является облачный сервер для 1С, но и возможность вывести на новый уровень ИТ-инфраструктуру вашего предприятия.

Ключевым аспектом данной услуги является индивидуальный подход к каждому клиенту и это подтверждается фактически - личный ИТ-инженер обеспечит стабильную поддержку вашей системы.

Компании невыгодна утечка данных клиента, чего не скажешь о рядовых сотрудниках, для которых отсутствие безупречной репутации не является крахом карьеры.

Поэтому существует ряд мероприятий, позволяющих минимизировать эти риски:

1. Сотрудники, обслуживающие клиентов, находятся региональных филиалах, тем самым создан барьер для «личного» общения на предмет подкупа человека. Человек не будет доверять сомнительному предложению из почты или скайпа - вдруг это провокация.

2. В компании создана партнерская схема оплаты, когда доход сотрудника прямо пропорционален количеству клиентов и качеству работы с ними. Доход сотрудника должен на 20-30% превышать среднерыночный, также создана прозрачная схема повышения категории (и как

следствие дохода), основанная на сдаче сертификатов Cisco и Microsoft. Все это делает сотрудника гораздо более лояльным к компании и клиентам.

3. В компании создан департамент экономической безопасности, в задачи которого входит выборочный аудит деятельности персонала. С каждым сотрудником заключен договор о конфеденциальности, который в частности разрешает осуществлять слежение за действиями человека, а в случае выявления факта утечки информации позволяет привлечь сотрудника к уголовной ответственности. Внедрена система записи телефонных переговоров, почтовых сообщений и Skype.

Защита данных от несанкционированного доступа:

1. Резервное копирование с уведомлением клиента. Компания в своих решениях применяет технологию двойной авторизации при удаленном подключении к серверу: по паролю и USB-ключу. Такой тип авторизации актуален для сотрудников, которые подключаются вне офиса. Если при работе из офиса в большинстве случаев будет достаточно только пароля, то устройство, которое покидает пределы офиса, оказывается в зоне риска. Оно может быть потеряно, украдено, или к нему может быть получен несанкционированный доступ. Наконец сотрудник может настроить удаленное подключение со своего личного устройства, и тогда при увольнении у него доступ может остаться. Чтобы избежать этих рисков и применяется аппаратный USB-ключ, на котором записан сертификат для подключения. Без этого устройства наличие пароля доступа бесполезно, так что даже если он будет сохранен на ПК (а многие пользователи это к сожалению делают) подключиться к серверу будет невозможно. Данная услуга включена в базовую стоимость, поэтому вам придется купить лишь сами аппаратные ключи e-Tolken, при этом любые, удовлетворяющие этому формату.

В связи с этим, многие клиенты задают вопрос о гарантии возвращения их данных в случае разрыва договора. К сожалению, на нашем рынке встречают недобросовестные хостинг - провайдеры которые начинают шантажировать клиента невозвратом их данных, если он не заплатит какую-нибудь задолженность. Да, можно с такой компанией начать судиться и суд выиграть, но время, затраченное на этот процесс, будет весьма значительным, а данные нужны сейчас, а не через несколько месяцев.

Клиент застрахован не только юридическим, но и технологическим путем: мы автоматически делаем резервные копии данных клиента на его носитель с уведомлением (по электронной почте или СМС) о каждой резервной копии для контроля. В качестве носителя обычно используется NAS или арендованный клиентом FTP сервер. Если вдруг что-то случится, то у клиента будет выгрузка его данных. А значит и отношения между нами будут более доверительными и спокойными. Периодичность этих выгрузок зависит от объема и критичности данных, например, для баз данных это можно делать каждую ночь, а для файлов частота резервирования обычно больше и составляет один раз в неделю.

2. Отказоустойчивая инфраструктура 24/7. Облачный сервис оказывает полный комплекс услуг по созданию ИТ-инфраструктуры предприятия, важным критерием которой является отказоустойчивость. Отказоустойчивая система сохраняет свою работоспособность при выходе из строя минимум одного узла. Мы используем кластерные технологии и профессиональные системы хранения данных для создания такой системы, функционирующей 24 часа в сутки 7 дней в неделю.

К преимуществам отказоустойчивой системы можно отнести следующее:

1. Непрерывность рабочих процессов.
2. Экономическая эффективность.
3. Защита целостности данных.
4. Альтернативное использование резервных мощностей.

Заключение. Все вышеописанное красноречиво свидетельствует о необходимости комплексного подхода к защите продуктов на базе «1С: Предприятие». Как определить конкретные угрозы и выработать меры защиты?

Ответ прост: провести аудит информационной безопасности. Специалисты фирмы «1С» со статусом «Центр компетенции по производству», имеют огромный опыт автоматизации, системной интеграции и защиты предприятий.

Библиографический список

1. [Электронный ресурс]: https://users.v8.1c.ru/.
2. [Электронный ресурс]: https://its.1c.ru/
3. [Электронный ресурс]: https://www.diadoc.ru/
4. [Электронный ресурс]: https://portal.1c.ru/applications/2#description

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Калинин М.С., Першин М.В., Мамзин А.С., студенты
Научный руководитель: к. п. н., доцент Горбачевская Е.Н.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

На сегодняшний день в базах данных (database) по всему миру хранится информация, которая затрагивает, большинство отраслей промышленности, каждую разновидность бизнеса и область нашей повседневной жизни.

Компании хранят в базах данных, включенных в их информационные системы, данные о клиентах и поставщиках, ресурсах предприятия, сотрудниках, информацию бухгалтерии, данные о внутренних операциях предприятия и многое другое. Базы данных применяются в информационных системах банков и государственных учреждений, кроме того, сегодня, в эпоху распространенного, доступного и быстрого Интернет-соединения, многие программы и приложения создаются с учетом возможности практически бесперебойного доступа к сети – данные для клиента поступают с сервера разработчика или издателя.

Базы данных - это критически важный элемент любой информационной системы. Обеспечение их безопасности является необходимым шагом для защиты информации. Но чтобы обезопасить этот критический элемент системы, необходимо ответить на вопросы: «как можно взломать базу данных?» и «кто может взломать базу данных?».

Источники угрозы

Как уже было сказано, в базах данных хранится огромное количество разнообразной и важной информации. По этой причине похищение, изменение или уничтожение этой информации может быть крайне привлекательной задачей для злоумышленника - одна атака может позволить похитить или уничтожить информацию, собиравшуюся годами, тем самым нанести, возможно, непоправимый ущерб организации или переманить, таким бесчестным и незаконным путем, клиентов этой организации к себе.

Но не все угрозы безопасности баз данных являются умышленными, направленными действиями лица или группы лиц, что занимаются промышленным шпионажем. Нет, вирусы и прочие деструктивные программы, которые могут привести к повреждению или похищению информации, могут попасть на сервер случайно, из-за некомпетентности сотрудника или недостаточной защиты аппаратной части. Полное или частичное уничтожение информации в базах данных также может произойти из-за сбоя или отказа аппаратуры – комплектующие ЭВМ могут выходить из строя под действием внешних факторов.

Источники угроз безопасности баз данных принято делить на внешние и внутренние.

К внешним угрозам относят умышленные, деструктивные действия хакеров, искажения в каналах передачи данных, сбои и отказы оборудования, вирусы и им подобные программы, а также не сертифицированные изменения аппаратной части информационной системы.

К внутренним угрозам принято относить системные и программные ошибки, ошибки проектирования и реализации информационных систем и баз данных, ошибочные и несанкционированные действия пользователей, а также недостаточная эффективность методов и средств обеспечения безопасности.

Теперь, зная источники угроз, можно определить, как именно они могут навредить базам данных.

Типы угроз

Существует три основных типа угроз для базы данных и информации, содержащейся в ней - изменение информации, уничтожение информации и похищение информации.

Похищение информации – это несанкционированный доступ к информации с ее незаконным копированием, но нередко вместе с незаконным перехватом информации, при возможности, уничтожают или повреждают оригинал. Существуют множество способов похищения информации, как изнутри, так и извне. Перехват информации по проводным или беспроводным каналам связи, программные закладки на серверах и компьютерах, незаметно копирующие информацию по мере её поступления и передающие её злоумышленнику. Возможным также является похищение базы данных путем её копирования прямо с сервера или кражей серверных ПЗУ, на которых эти базы данных находятся.

Уничтожение информации также может быть произведено злоумышленником как снаружи, так

и изнутри. Несанкционированный доступ с последующим удалением баз данных или таблиц, умышленное или неумышленное повреждение оборудования, на которых эта информация находится. Вирусы, удаляющие данные, а также недочеты в проектировании баз данных. Нередки случаи, когда при разработке БД, разработчики забывали производить изоляцию их кода - базы данных в таком состоянии работоспособны, вот только поддаются изменению со стороны. Зная команду и названия таблиц, злоумышленники в состоянии, удалять таблицы, из которых состоит база данных, просто прописав соответствующий запрос в поле для ввода.

К типу угроз также принято относить и изменение информации, содержащейся в базах данных, ведь, как известно из школьного курса информатики «неверная, ошибочная информация - это бесполезная информация». Сюда относят изменение информации на бессмысленный набор символов путем несанкционированного доступа или вирусной атаки, внесение ложной информации в базу данных или, один из наиболее экзотичных вариантов - шифрование базы данных по определенному алгоритму, известному только злоумышленнику с целью вымогания чего-либо за ключ, по которому проводилось шифрование.

Понимание того, как именно базе данных могут повредить, является необходимым для того, чтобы разработать методы противодействия и защиты.

Особенности защиты базы данных

Хранилища данных состоят из двух элементов: хранимые данные (БД) и программы управления (СУБД). Обеспечение безопасности хранимых данных, в целом, невозможно без обеспечения безопасного управления данными. Таким образом можно условно разделить уязвимости и вопросы безопасности на две группы: зависящие и не зависящие от данных.

Независящие от данных уязвимости являются типичными и для всех прочих разновидностей программного обеспечения. Причиной их возникновения могут быть: Отсутствие своевременного обновления ПО, низкая квалификация администратора ПО или присутствие неиспользуемых функций.

Большая часть аспектов безопасности СУБД остаётся зависящей от данных. Однако, немалая доля уязвимостей являются косвенно зависимой от данных. Большая часть СУБД поддерживает определенный язык запросов, содержащий доступные пользователю функциональные наборы (которые, равным образом, можно считать операторами языка запросов) или же произвольные функции на языке программирования.

Структура используемых языков (наборов функций и специализированных языков) напрямую согласована с моделью данных, используемой для хранения данных. Следовательно, модель задает особенности языка, и присутствие в нем определенных уязвимостей. Кроме того, некоторые уязвимости, такие как инъекция, реализуются разными способами (инъекция sql и инъекция java) исходя из синтаксиса языка.

При организации защиты баз данных требуется учесть несколько специфических угроз безопасности информации, базирующихся на концентрации в БД большого количества различной информации, а также с возможностью использования сложных запросов обработки данных. К таким угрозам относятся:

–инференция;

–агрегирование;

–комбинация разрешенных запросов для получения закрытых данных.

Под инференцией нужно понимать получение конфиденциальных данных из сведений с меньшей степенью конфиденциальности посредством умозаключений.

Существует аналогичный инференции способ добычи конфиденциальных данных – агрегирование. Агрегирование - это способ извлечения более значимых сведений по сравнению с важностью тех отдельно взятых данных, на основе которых и получаются эти сведения.

Если инференция и агрегирование являются способами получения информации, которые применимы не только по отношению к базам данных, то способ специального комбинирования запросов может быть использован только при работе с БД. Использование сложных, а также последовательности простых логически связанных запросов позволяет получать данные, к которым доступ пользователю закрыт.

Шифрование базы данных

Шифрование базы данных – применение технологии шифрования для преобразования информации, содержащейся в базе данных, в зашифрованный текст, что предотвращает чтение лицами, не имеющими ключей шифрования.

Прозрачное шифрование базы данных - это технология, используемая в продуктах Microsoft и

Oracle для шифрования входящей информации и дешифрования на выходе. Информация шифруется перед записью на диск и дешифруются во время чтения в память. Это, в свою очередь, сводит на нет проблему защиты «неактивных» данных, но, в то же время не гарантирует сохранность данных при передаче по каналам связи или во время использования. Достоинством прозрачного шифрования является то, что шифрование и дешифрование выполняются “прозрачно” для приложений, что снимает необходимость преобразования.

Стоить заметить, что традиционные методы шифрования баз данных обычно шифруют и дешифруют содержимое базы данных, администрирование которой обеспечивается СУБД, работающей поверх ОС. Это уменьшает уязвимость информации, потому как зашифрованная БД может быть запущена на открытой или незащищенной ОС. Например, Microsoft использует технологию шифрования файловой системы, которая предоставляет шифрование на уровне файлов. Каждый объект зашифровывается посредством ключа шифрования файлов, который, в свою очередь, защищен сертификатом. Этот сертификат может быть составным, это позволяет получать доступ к файлу более чем одному пользователю. За счет увеличения области шифрования, применение шифрования файловой системы может усложнить процесс администрирования и понизить производительность, потому как системному администратору для шифрования потребуется доступ к операционной системе.

Симметричное и асимметричное шифрование базы данных

Симметричное шифрование является одним из самых известных методов. Он состоит из закрытого ключа, по которому производится шифрование и дешифровка данных, хранящихся в базе данных и вызываемой из нее. Ключ преобразует данные так, что их чтение без расшифровки становится недоступным. Уязвимостью этого способа является то, что существует вероятность потери конфиденциальных данных, в том случае, когда ключ окажется у лиц, не имеющих разрешения на доступ к информации. Тем не менее, применение только одного ключа в процессе зашифровки позволяет упростить и ускорить процесс использования технологии.

Проблема попадания секретного ключа к злоумышленникам при отправке по каналам связи, которой располагает шифрование с закрытым ключом, решена в асимметричном шифровании, в нем имеется два взаимосвязанных ключа. Открытый ключ известен всем и может передаваться по незащищенному каналу связи. Закрытый ключ, в свою очередь, содержится в тайне и является особенным для каждого пользователя. Открытый ключ применяется для шифрования данных, а закрытый — для расшифровки. Асимметричное шифрование более безопасно в сравнении с симметричным, но, в тоже время, значительно медленнее.

Метод хеширования

Хеширование применяется в качестве метода защиты информации. Алгоритм хеширования создаёт строку определенной длины (хеш), за основу берутся введенные данные или сообщения. Хеширование отличается от шифрования тем, что его алгоритм нельзя обратить, иными словами, не существует такого преобразования, что позволило бы извлечь сообщение из его хеша.

Шифрование на уровне приложений

Преимущества

Одна из ключевых особенностей шифрования, интегрированного в приложение это - отсутствие необходимости применять дополнительное решение для защиты информации при передаче по каналам связи, потому как они отправляются уже в зашифрованном виде. Преимущество этого вида шифрования заключается в том, что хищение данных значительно усложняется, так как злоумышленник должен иметь доступ к приложению для расшифровки данных

Недостатки

Для шифрования на уровне приложений требуется применить изменения как на само приложение, так и на БД. Кроме того, шифрование приложений может привести к снижению производительности базы данных, которая, в результате, теряет возможность выполнения индексирования и поиска. Еще одним недостатком является управление ключами в системе с таким методом шифрования. Так как базу данных могут использовать сразу несколько приложений, то ключи хранятся во многих местах, исходя из этого, неправильное управление ключами может привести к краже информации или её повреждению. Таким образом, если требуется преобразование ключа, то нужно расшифровать все данные старым ключом, и только потом снова зашифровать, используя новый ключ.

Требования к безопасности базы данных

Исходя из принципа разделения уязвимостей, можно выделить зависящие и независящие от данных способы обеспечения безопасности БД.

К не зависящим от данных способам можно отнести следующие требования к безопасности:

Функционирование в доверенной среде.

Доверенная среда это инфраструктура предприятия и его механизмы защиты, сформированные политиками безопасности.

Следовательно, речь идет о функционировании СУБД согласно правилам безопасности, применяемым, в том числе и ко всем системам предприятия.

Организация безопасности файлов на физическом уровне.

Требования к физической безопасности данных СУБД по большей части ничем не отличаются от требований, применяемых к любым другим файлам пользователей и приложений.

Организация актуальной и безопасной настройки СУБД.

Это требование включает в себя основные задачи обеспечения безопасности, такие как своевременное обновление ПО, отключение неиспользуемых функций или применение эффективной политики паролей.

Требования зависящие от данных:

Безопасность пользовательского ПО.

Сюда относятся задачи создания безопасных интерфейсов и механизмов доступа к информации.

Безопасная организация и работа с данными.

Вопрос организации и управления данными остаётся ключевым в системах хранения информации. В данную область входят задачи по организации данных и контролю целостности, а также другие, характерные для СУБД проблемы безопасности. По сути, эта задача включает в себя большую часть зависящих от данных уязвимостей и защиты от них.

Заключение

В настоящее время базы данных, включенные в информационные системы с которыми мы взаимодействуем ежедневно. Бизнес ли это, промышленность, банковская и государственная деятельность или наша повседневная жизнь, все это основано на базах данных и их взаимодействии.

Несанкционированный доступ, полученный из-за недостаточной защиты, может привести к серьёзным последствиям как владельцев этих систем, так и для их пользователей. Независимо от того большая это организация или маленькое предприятие, в любом случае следует серьёзно подходить к вопросу защиты базы данных.

Чтобы эффективно управлять ситуацией, нужно оперативно её отслеживать и своевременно реагировать на её ухудшение. А ещё лучше – уметь предусмотреть возможные проблемы, чтобы предотвращать утечку данных. Цель защиты базы данных - уменьшить потери, вызванные заранее предусмотренными событиями. Принимаемые решения должны гарантировать эффективное использование понесённых затрат и исключать излишнее ограничение используемых пользователям возможностей. Ведь в вопросе безопасности, любой безопасности, требуется найти «золотую середину» между защищенностью и функциональностью. Следует помнить, что хотя отрезанный от сети компьютер - это самый защищенный компьютер, он же и самый нефункциональный.

Гарантия информационной безопасности баз данных - дело весьма сложное во многом в силу самой природы реляционных СУБД. Ведь информационная безопасность развивается чрезвычайно быстро. Разработка новых методов защиты и новых методов взлома - это настоящая «гонка вооружений», битва умов и навыков, непрекращающаяся борьба.

Главная трудность, существующая в этой области, заключается в том, что все применяемые методики, по сути, созданы лишь для того, чтобы оттянуть неизбежное. Любой шифр, рано или поздно будет раскрыт, любая защита рано или поздно будет пробита. Но с такой же скоростью теряют актуальность и методики взлома, например во многих современных системах уже существует защита от «брут-форса» - машинного перебора паролей, что лишило злоумышленников целой методики взлома.

Безопасность баз данных - это то, что необходимо постоянно совершенствовать, улучшать и изменять. В противном случае в этой «гонке вооружений» победа достанется злоумышленникам, вместе со всеми данными, на защите которых сэкономили.

Библиографический список

1. Дейт, К. Дж. Введение в системы баз данных / К. Дж. Дейт – «Вильямс» – 2005.

2. Свободная энциклопедия Википедия [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org (12.11.2017)

3. IT-сообщество Tproger: Основные аспекты безопасности СУБД [Электронный ресурс] – Режим доступа: https://tproger.ru (12.11.2017)

4. Библиотека научных работ Студопедия: Источники угроз информации баз данных. [Электронный ресурс] – Режим доступа: https://studopedia.org (12.11.2017)

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

Корнев М.И., студент
Научный руководитель: к. т. н., доцент Куралесова Н.О.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Корпоративные сети подвергаются постоянным сетевым атакам. Компаниям необходимо предоставлять безопасный доступ для сотрудников к сетевым ресурсам, для чего современные способы обеспечения сетевой безопасности должны учитывать ряд таких факторов, как повышение надежности сети, эффективное управление безопасностью и защиту от постоянно развивающихся угроз и новых методов атак. Проблема обеспечения надежной сетевой безопасности становится все более сложной, т.к. нынешние сотрудники, использующие личные смартфоны, ноутбуки и планшеты для работы, открывают новые возможности для злоумышленников. Сетевые атаки в наше время являются реальной проблемой для компаний. Что под собой подразумевает сетевая атака? Это удаленное действие, целью которого является повышение прав над системой, получение секретных данных или вывод самой системы из строя. В этих условиях ИТ-менеджеры должны быть бдительны, чтобы не затормаживать бизнес процессы своих компаний. Им нужно постоянно совершенствовать методы защиты сети.

Рассмотрим четыре основополагающих принципа защиты корпоративной сети от атак и взломов.

Основа этих принципов в том, что сеть должна работать даже под атакой. Для начала нужно определить конечные устройства. Что же такое конечное устройство? В данной модели конечным устройством является любое из устройств, на котором выполняется реальная работа, такими устройствами являются настольные компьютеры, серверы и мобильные устройства.

И так, определив конечные устройства, нужно начинать разрабатывать стратегии их защиты. Такая стратегия состоит из четырех принципов безопасности:

Укрепление защиты конечных устройств;
Отказоустойчивость конечных устройств;
Приоритизация сетей (контроль пропускной способности);
Отказоустойчивость сети.

Но нужно не забывать, что у каждого вышеперечисленного принципа есть и дополнительные цели.

Например, надо автоматизировать эти процессы как можно больше.

Далее, надо мониторить компьютерную сеть, чтобы видеть, что происходит в конкретный момент времени.

Так же нужно не забывать про организацию обратной связи. Потому что безопасность сети может быть надежной только при постоянных вложениях в её модернизацию.

Укрепление защиты конечных устройств

Основополагающей целью данного принципа является использования актуальных технологий безопасности.

Один из способов повышения защиты сети — использование антивируса. Так же начиная с Windows Vista и всех последующих ОС, присутствует механизм целостности, который представляет собой режим "песочницы". Так называемая "песочница" это режим безопасного исполнения программ.

Так же данный принцип тесно связан с мониторингом. Подразумевает под собой наблюдение и поиск кода со странным поведением.

Отказоустойчивость конечных устройств

Основополагающей целью данного принципа является постоянный сбор и мониторинг состояния устройств и приложений. Это нужно для того чтобы можно было автоматически восстанавливать вышедшие из строя устройства не прерывая работу компании.

Примеры технологий, которые позволяют сделать более надежными конечные устройства Network Access Protection (NAP) и Microsoft System Center. При объединении этих технологий автоматическое восстановление происходит быстро и легко.

Данный принцип так же связан с мониторингом. Подразумевает под собой поиск машин, не отвечающих техническим условиям и исправление этой проблемы.

Приоритизация сетей

Основополагающей целью данного принципа является организация способности инфраструктуры удовлетворять потребности приложений в пропускной способности. Но это относится не только к известным периодам самой высокой нагрузки, но и непредвиденных скачков в нагрузке сети или DDoS атак.

Пропускную способность для отдельного пользователя сети можно настроить в маршрутизаторе компании.

Данный принцип так же связан с мониторингом. Подразумевает под собой наблюдение за журналом маршрутизатора и любых изменений в прошлых отчетах.

Отказоустойчивость сетей

Основополагающей целью данного принципа является обеспечение самовосстановления сети и минимизировании усилий по управлению. Восстановление сети так же не должно занимать время пользователя и отвлекать его от работы, все должно проходить автоматически и не заметно для него.

Данный принцип так же связан с мониторингом. Подразумевает под собой получение отчетов о загруженности и неожиданных скачках сети.

Вышеперечисленными методами можно обезопасить свою сеть лишь на базовом уровне, но для более надежной защиты нужны различные дополнительные способы защиты от сетевых атак.

Существующие виды сетевых атак:

DDoS (Distributed Denial of Service) один из самых легко реализуемых и распространенных видов атак, представляет собой распределённый отказ, в обслуживании который вызывает нехватку пропускной способности сети, что в свою очередь вызывает остановку работы сервера. Данный вид атак не нацелен на получение доступа к сети или получение какой-либо информации из неё, он просто выводит из строя сервер.

Mailbombing - данная атака представляет собой спам почтового ящика большим количеством писем. После чего может вызвать отказ работы почтового ящика или даже всего почтового сервера. Проблемы этой атаки так же актуальны в данной теме, потому что многие крупные компании имеют в своем пользовании собственные почтовые сервера.

Ip-спуфинг(IP-spoofing) это вид атак суть которого использование чужого IP- адреса в целях обмана системы безопасности и получение доступа к ресурсам. Обычно ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных по одно ранговым устройствам.

Типовые способы защиты от описанных ранее сетевых атак

DdoS-атака является самым примитивным, но в то же время и трудно предотвратимым видом атаки. Невозможно обеспечить стопроцентную защиту. Но данную угрозу можно снизить тремя способами:

1. Функции анти-супфинга. Супфинг(Soopfing)-блокировка выхода за пределы сети пакетов с неправильным адресом отправителя. Правильная конфигурация функций анти-спуфинга на маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827.

2. Функции анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить работоспособность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

3.Ограничение объема трафика (traffic rate limiting). Организация может попросить провайдера ограничить объем трафика. Этот тип фильтрации позволяет уменьшить объем некритического трафика, проходящего в вашей сети.

Mailbombing довольно редкий вид атак и используется чаще всего "начинающими" злоумышленниками.

1. Не давать адрес электронной почти сомнительным и не проверенным источникам.

2. В качестве защиты от данной атаки Web-сайт провайдера, который иногда настаивают на определение почтовой атаки. Сообщения распознаются сервером посредством сравнения исходных IP-адресов, и если все сообщения приходят от одного источника, то сразу отправляются в Recycle Bin на сервере.

Ip-спуфинг часто является начальной точкой для других атак, обычно DDoS и начинается с чужого адреса, скрывающего истинную личность хакера.

Данную угрозу практически невозможно устранить, но можно ослабить этими методами:

1. Самый просто способ защиты это контролировать доступ в сети. Чтобы понизить эффективность IP-спуфинга нужно настроить контроль доступа на обрыв трафика поступающего из внешней сети.

2.Фильтрация RFC 2827. Позволяет ограничить любой исходящий трафик IP-адрес которого не является одним из адресов вашей компании.

На 100% обезопасить свою сеть на данный момент невозможно, но применяя эти способы комплексно с использованием модели синхронизации данных по угрозам и распараллеливание нагрузки системы защиты можно повысить безопасность корпоративной сети.

Заключение

Корпоративные сети часто подвергаются угрозам со стороны киберпреступников, желающих получить доступ к администрированию, данным или просто остановить работу сервера. Хотя перечисленные способы могут повысить безопасность сети, атаки становятся все более изощрёнными и находят способы обойти защиту, чтобы нанести вред компании.

Столкновение с разнообразными атаками требует быстрореагирующих решений по обеспечению новых стратегий надежности, отвечающих актуальным требованиям.

Перечисленные в этой статье методы помогут справиться с некоторыми атаками.

Из всего вышесказанного можно сделать вывод, что в современном мире нельзя обезопасить на 100% корпоративную сеть, а значит нужно продолжать искать новые подходы к реализации стратегий защиты информации и использовать новые методы и средства обеспечения сетевой безопасности.

Библиографический список

1. Гриффин, Д. Сетевая безопасность: Четыре основополагающих принципа безопасности оконечных устройств сети. [Электронный ресурс] – Режим доступа: https://technet.microsoft.com/ru-ru/library/gg213837.aspx.

2. Сетевая безопасность. Вместо введения. [Электронный ресурс] – Режим доступа: https://habrahabr.ru/company/hpe/blog/261913/ многофункциональный сайт, представляющий собой смешение новостного сайта и коллективного блога.

3. Боршевников, А.Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13. URL: https://moluch.ru/conf/tech/archive/5/1115/.

ВИРУСЫ В UNIX-ПОДОБНЫХ СИСТЕМАХ

Кочарян С.А., Алексеев К.О., студенты
Научный руководитель: к. т. н., доцент Федосеева О.Ю.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Unix-подобные системы всегда были известны как самые защищённые от вирусных атак. В прошлом не было широко известных вирусных программ для Linux, в отличие от Microsoft Windows, это связано в том числе с системой прав доступа, отсутствием (в большинстве дистрибутивов) предустановленных сетевых служб принимающих соединения, и незамедлительной модификацией и улучшением Linux при обнаружении новой вирусной атаки. Но все же, злоумышленники способны инфицировать файлы в незащищённых сетях Linux и осуществлять вредоносную деятельность, некоторые способны продолжать инфицировать другие системы.

В Linux-системах используется система для разграничения прав доступа, называемая root доступом, дающая определенные права пользователю. В целях инфицирования ПК, вирус пытается получить доступ к root правам. Однако, до тех пор, пока не будет приобретен root, либо юзеру не будет доступна административная учетная запись, система разделения прав не предоставит инфицированным файлам подобного шанса. Без прав суперпользователя вредоносное функционирование вирусных программ сводится к сканированию всех действий юзера (передачи введенных паролей, ключей информации о кредитках и т. д.), воровству пользовательских данных, рассылке вредоносных писем, спама и участию в DDoS-атаках.

Для получения прав суперпользователя, обычно необходимо применение специальных эксплойтов, использующих открытые дыры в ядре Linux или в сервисах, имеющих root-права для их собственной работы, либо методы социальной инженерии (к примеру, попытка преподнести

вредоносную программу за чистое и не пораженное вирусом приложение, требующее административных прав).

Использование уязвимостей усложняется скорым закрытием крупных уязвимостей, вследствие чего распространение вирусной программы останавливается сразу после модификации уязвимых мест в ОС, а методом социальной инженерии больших успехов во взломе не добиться по причине сильных технических знаний со стороны пользователей с root правами.

Все это, в совокупности с разными методами активации программ при запуске ОС в различных вариантах (дистрибутивах) Linux, приводит к тому, что мы очень вряд ли сможем найти вирусную программу способную быть запущенной на современных обновленных версиях Linux. Обнаружить вирусную программу, способную к самостоятельному распространению — на другие ПК практически не выполнимая задача.

1-ый вирус для Linux возник в сентябре 1996 года. В феврале 1997 года был выпущен обновленный вирус. В октябре 1996 года в электронном журнале, посвящённом вирусам VLAD, присутствовал исходный код вирусной программы Staog. Прежде, в 1995 г., была издана книга Марка Людвига «The Giant Black Book of Computer Viruses», в ней указаны исходные коды Snoopy для FreeBSD. Snoopy и Bliss, приведены в стиле Си и могут быть перекодированы практически в любую UNIX-подобную ОС с минимальными изменениями.

Число инфицированных программ под Linux возросло с 2005 года. В частности, произошло увеличение числа linux вирусов с 422 вплоть до 863. Имелись уникальные случаи выявления вставок вредоносных программ (троянских программ) в служебных сетевых репозиториях или распространенных веб-сайтах дополнений. Как правило, количество установок, подобных троянов измеряется сотнями либо тысячами, после чего троян удаляется, а пострадавшим юзерам необходимо осуществить инструкции по удалению трояна в собственных ПК, уже после чего, троян становится историей.

Вирусные сканеры легкодоступны для Linux-систем. Главное их назначение — выявление вирусов и иного вредоносного ПО для операционных систем Windows. Они могут проверять проходящую через них электронную почту, к примеру, для того чтобы уберечь ПК с системами Microsoft Windows, получающих почту через коллективный почтовый сервер. Эпизоды выявления антивирусами вирусов для Linux «в живую» («in the wild») или не имели места, или о них никак не известно. Перечислим некоторые методы инфицирования. Двоичные файлы и исходные коды, приобретенные от посторонних репозиториев, либо юзеров, имеют все шансы содержать вирус. Скрипты оболочки (shell scripts) уже после запуска могут выполнять программы и иметь доступ к файлам. Взамен специфической версии библиотеки может быть подставлена фальшивая библиотека. При поддержки Wine могут работать вирусы, предназначенные для Microsoft Windows (ввиду применения многими вирусами незадокументированных системных вызовов Windows, которые весьма слабо реализованы в Wine, угроза инфицирования меньше). Как правило, посредством Wine вирусы готовы жить только вплоть до перезапуска операционной системы, так как обычные способы автозапуска программ в Windows не работают в Wine. Исключение — файловые вирусы, то есть заражающие исполнимые файлы легитимных программ. Вирус вновь запустится, как только юзер запустит заражённую программу. Необходимо отметить то, что класс файловых вирусов почти прекратил существовать, уступив роль троянам и бэкдорам, существующих в 1 (реже в 2-х) экземпляре (файле) в диске, и запускающихся посредством обычных (или не очень) механизмов автозапуска в Windows.

Примеры известных вирусов:

Черви: Adm; Adore; Cheese; Devnull; Kork; Lapper.

Компьютерные вирусы: Alaeada; Bliss; Brundle; Dawn; Diesel; Hasher; Kagob; Lacrimae; Pilot; Staog; Winter; Winux (или PEElf); ZipWorm.

Троянские программы: Kaiten — Linux.Backdoor.Kaiten; Rexob — Linux.Backdoor.Rexob.

В 1988 г. Робертом Моррисом-младшим был основан 1-ый общественный сетевой червь. 60000-байтная программа разрабатывалась с расчётом на разрушение операционных систем UNIX Berkeley 4.3. Вирус первоначально разрабатывался как безопасный и обладал целью только незаметно проникнуть в вычислительные системы, сопряженные сетью ARPANET, и остаться затем необнаруженным. Вирусная программа содержала элементы, позволяющие выявлять пароли, существующие в инфицированной системе, что, в собственную очередь, позволило программе скрываться под задачу легальных пользователей системы, в самом процессе занимаясь размножением и рассылкой копий. Вирус не остался скрытым и полностью безопасным, как замышлял создатель, в

силу небольших ошибок, допущенных при разработке, которые повергли к быстрому неконтролируемому саморазмножению вируса.

По самым умеренным анализам происшествие с червём Морриса обходился выше 8 млн. часов потери доступа и больше млн часов прямых потерь в возобновление трудоспособности систем. Единая цена данных расходов расценивается в 96 млн. $ (в эту сумму, кроме того, не совсем обосновано, введены расходы по доработке операционной системы). Вред был бы значительно больше, если бы вирус первоначально формировался с разрушительными целями.

Червь Морриса сразил больше 6200 ПК. В следствии вирусной атаки большая часть сетей вышло из строя в срок до 5 дней. ПК, исполнявшие коммутационные функции, работавшие в качестве файл-серверов либо исполнявшие прочие функции обеспечения работы сети, кроме того вышли из строя.

Вредоносное ПО и Mac OS

Пока у компьютеров есть какой-то контакт с внешним миром, и люди изготавливают программы, есть риск того, что на ПК попадет вредное ПО. Тот или иной исходный код может быть наиболее безопасным, чем прочий код, однако нет ровным счетом ничего, что невозможно было бы взломать (по крайней мере, в реалиях потребительского ПО).

До возникновения OS X, было огромное количество вирусов, которые были способны инфицировать Mac OS. Однако, Mac OS была полностью переписана при переходе на OS X это привело к тому, что вирусы способные навредить Mac OS до OS X не могут инфицировать сегодняшнее обновления Mac OS. На сегодняшний день, в сети отсутствует вредоносное ПО, которое могло бы инфицировать ваш ПК. Отсутствуют вирусы, отсутствуют трояны, отсутствуют логгеры тексты, отсутствуют бот-сети. Вы можете находиться в сети, просматривать электронную почту, просматривать видео, и никто и ничто не сможет инфицировать ваш ПК.

Но все же, всегда есть риск того, что завтра кто-то создаст вирус, который будет использовать неизвестный ранее эксплоит или уязвимость в OS X, и к вечеру он зашифрует все файлы на всех ПК, подключенных к сети. Большая часть вредоносных программ функционирует с помощью использования эксплоитов в ОС. Apple регулярно публикует обновления ОС, по этой причине на нынешний период, упущения в ОС не оказались достаточны для злоумышленников.

Mac OS по своей сути является глобально модифицированной версией Unix. Unix применяется уже много лет, и успел стать довольно безопасной ОС, за годы существования ОС были обнаружены и исправлены многие ошибки.

Антивирусные программы

С целью выявления, удаления и защиты компьютеров от вирусов, были разработаны программы, способные выявлять и подавлять вирусы. Подобные программы именуются антивирусными. Сегодняшние антивирусы способны поражать вирусы до их активации, то есть превентивно, так и сканировать ОС пользователя для профилактики заражения, а также способен восстанавливать зараженные файлы. На данный момент число вирусов для UNIX-подобных систем мало, но в любой момент злоумышленники могут перехитрить систему и найти дыру в системе, для этого и нужны антивирусные программы. И любые антивирусы не подойдут, качественный антивирус должен отвечать следующим характеристикам.

Стабильность и надежность работы. Именно эти параметры являются главными при выборе антивируса. Даже самый дорогой антивирус окажется бесполезным, если он перестанет нормально функционировать на вашем компьютере, в случае какого-либо сбоя в работе программы процесс анализа ПК не пройдет до конца. В таком случае всегда существует возможность того, что какие-то инфицированные файлы не будут найдены.

Масштабы вирусной базы антивируса (вирусы, зарегистрированные в сформированной базе для их идентификации). С учетом непрерывного возникновения более свежих вирусов, базы данных должны постоянно обновлять. Важным, кроме этого, будет является наличие резидентного монитора, выполняющего анализ загруженных файлов.

Возможность обнаружения даже неизвестных программе вирусов – эвристическое сканирование. Сюда же следует отнести возможность восстанавливать инфицированные файлы.

Возможность обнаружения даже неизвестных программе вирусов – эвристическое сканирование. Сюда же следует отнести возможность восстанавливать инфицированные файлы.

Популярные антивирусы для систем Linux: NOD32; Kaspersky; AVG; Avast; Symantec; McAfee; Comodo; ClamAV.

Библиографический список

1. Безопасность Unix подобных систем [Электронный ресурс]: https://en.wikipedia.org/wiki/ Linux_malware.
2. Mac OS [Электронный ресурс]: https://ru.wikipedia.org/wiki/Mac_OS.
3. Mac OS Virus possibility - [Электронный ресурс]: http://utilware.com/viruses.html.
4. The Early Mac OS - AndyF.Mesa – [Электронный ресурс]: http://applemuseum.bott.org/ sections/os.html.
5. Антивирусы в LINUX среде [Электронный ресурс]: https://cdn.comss.net/img/antivirus_linux.

ОРГАНИЗАЦИЯ ЗАЩИТЫ СЕРВЕРА

Медведев Д.И., студент
Научный руководитель: ст. преподаватель Еремкина М.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Для организации защиты необходимо провести анализ основных видов атак на сервера и средства защиты сервера от хакеров. Статья ориентирована на администраторов *nix + Apache + PHP + Perl + (MySQL | PostgreSQL) и защите серверов от удаленных атак.

Атаки делятся на две подгруппы:

1. Атака на сервисы, которые уязвимы и доступны через Интернет
2. Атака через динамическое содержимое сервиса

Пример деления атак: существует вымышленный скрипт, который удаленно атакует Apache на 80 порту и в результате атаки Apache завершает свою работу и вы остаетесь без своего сайта, так как некому выдавать web-страницы. Вашему почтовому серверу sendmail отправили в качестве параметра для VRFY 1000 символов, а не короткое имя пользователя, sendmail не ожидал такого развития событий и закрылся, оставив вас без почты. Общий смысл атак этого условного класса, в том, что эксплуатируется какая-либо уязвимость приложения. Существуют три пути атак:

1. Приложение «упадет» и сервис будет не доступен, ситуация DoS.
2. Приложение начнет захватывать ресурсы и, истощив их, сделает DoS.
3. Приложению «скормят» Shell cod и выполнится код атакующего.

Атаки на сервис (см. пункт 1) ликвидируются только одним способом: администратор оперативно узнает от разработчика о наличии уязвимости и обновляет данную программу.

Динамический сервис (атака по пункту 2), реализованный на некотором языке программирования, допускает получение параметров и, не проверяя их, выполняет. Например, с помощью браузера атакующий, ползая по сайту под управлением Apache, ищет уязвимости в самом сайте и эксплуатируя их, получает желаемое. Написанный на языке Tcl, бот для моделирования канала IRC сервера принимает запросы от пользователя и хакер, воссоздавая работу программного кода бота (reverse engineering), конструирует запросы, которые не были учтены автором бота.

Атака на уязвимые сервисы и сам сервер

Атаки возможны из ошибок в реализации программы, такие как переполнение буфера (buffer overflow).

Переполнение локального буфера дает:

1. Перезаписать адрес возврата на злонамеренный код.
2. Удаленно позволяет выполнить произвольный код на целевой системе.
3. Локально, если программа запущена под root'ом, это позволит получить привилегии администратора системы.
4. Код, вызывающий переполнение буфера и выполняющий действия для хакера, называют shell code.

Защита от атак на уязвимые сервисы и сам сервер

1. Security tuning. Чтобы хакеры не взломали Ваш сервер необходимо произвести тюнинг безопасности: прочитать рекомендации производителя операционной системы по безопасности (man security).
2. Firewall. Настройка firewall: скан портов типа nmap и скан уязвимостей (выставить флаг запрещения фрагментированности пакета) - сервер. Система обнаружения вторжений (несанкционированный доступ) – доступ в Интернет.

Правило необходимого минимума:

1. Минимизировать доступные сервисы для Интернета.
2. Настроить MySQL сервер, работающий в паре с Apache на одну машину, на своем стандартном порту 3306.
3. Разграничение прав доступа (политика идентификации / аутентификации пользователей).

Таблица 1 - Виды атак на уязвимые сервисы и сам сервер

№	Название атаки	Описание	Защита от атаки
1	Атака DoS (Отказ в обслуживании)	хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам, либо этот доступ затруднён	1. Обновление программы, которой манипулируют для атаки DoS. 2. Настроить квотирование ресурсов для учетной записи, от которой работает данная программа. *nix системы позволяют настроить процент использования процессора, оперативной памяти, кол-во порождаемых процессов, открытых файлов. 3. Настройка логирования в программе. 4. Настройка программы как советует разработчик.
2	DDoS распределённая атака типа «отказ в обслуживании»	сетевой ресурс выходит из строя в результате множества запросов к нему, отправленных из разных точек. Обычно атака организуется при помощи ботнетов	1. Если DDoS направлен на приложение, попытайтесь в логах найти отличия от легитимных пользователей, и автоматизируя скриптом, заносите в правила firewall в deny. 2. Настроить квотирование ресурсов для учетной записи, от которой работает данная программа. *nix системы позволяют настроить процент использования процессора, оперативной памяти, кол-во порождаемых процессов, открытых файлов.
3	Атака bruteforce пароля	вычисляют необходимый для проникновения в сеть пароль методом подбора - на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов	1. Ограничивайте кол-во попыток неудачных логинов/паролей. 2. Если приложение позволяет, то настройте увеличение времени перед новой попыткой логин/пароль. 3. Если с приложением должен работать узкий круг людей, создайте такое правило и ограничьте им.

Атака через динамическое содержимое сервиса

Данный вид атак часто происходит на связку Apache + (PHP | PERL) + (MySQL | PostgreSQL) для мира *nix и IIS + ASP + Microsoft SQL Server для мира MS Windows с помощью простого браузера. Языками программирования являются ASP, PHP, Perl, SQL - для составления своих деструктивных конструкций. Пример некоторых подобных связок: Веб-сервер + CGI скрипты; IIS + сервер приложений ColdFusion; механизм SSI (Server Side Includes).

Таблица 2 - Виды атак на динамическое содержимое (Web-сайт)

№	Название атаки	Описание	Защита от атаки
1	XSS (Cross Site Scripting)	атаки на web-системы, заключающийся во внедрении в выдаваемую web-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с web-сервером злоумышленника: кража cookie (информация идентификации пользователей); deface сайта -замена стартовой страницы сайта (index.html); троянизация удаленного пользователя; DoS-атаки.	Для блокировки записи html тегов в базу данных из полей ввода информации, примените подобные конструкции htmlspecialchars для PHP, которые заменят < на <, > на >, & на &amp. Проверяйте и фильтруйте в своих скриптах все параметры (применяйте регулярные выражения для разбора поступающих данных). Используйте приемы безопасного программирования. Ознакомьтесь с безопасными методами работы с cookie (ограничивайте их действия во времени и по IP адресам).

Продолжение таблицы 2

№	Название атаки	Описание	Защита от атаки
2	SQL injection. SQL инъекция	атака, направленная на веб-приложение, в ходе которой конструируется SQL-выражение из пользовательского ввода путем простой конкантенации.	1. Активно используйте такие средства серверов SQL как представления (view) и хранимые процедуры. 2. Проверяйте и фильтруйте в своих скриптах все параметры, которые вводит пользователь и передающиеся скрипту через адресную строку. Для своего языка программирования найдите материал, обучающий приемам безопасного программирования. 3. Хакерам очень нравится, когда язык программирования на сайте позволяет запускать системные команды (нужно запретить вызов таких функций в вашем языке программирования - в настройках PHP есть возможность указать список «запрещенных» функций с помощью disable_functions в php.ini.

АНАЛИЗ ВИДОВ УГРОЗ БЕЗОПАСНОСТИ WEB-САЙТОВ

Никитин В.А., студент
Научный руководитель: к. п. н., доцент Горбачевская Е.Н.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

В настоящее время при создании web-сайта нужно уделить внимание логотипу, названию, дизайну, контенту, а самое главное - это его безопасности. Незащищенный сайт подвергается огромному количеству атак злоумышленников и если пренебрегать безопасностью, то возможно не только временное прекращение работы сайта, но и потеря пользователей.

Создавая свой web-сайт, первое, что нужно учесть, как его защитить от внешних атак хакеров, а также предоставить пользователям полную безопасность при работе с сайтом.

Рассмотрим типы угроз информационной безопасности веб-сайта:

– Угрозы конфиденциальности – несанкционированный доступ к данным.
– Угрозы целостности – несанкционированное искажение или уничтожение данных.
– Угрозы доступности – ограничение или блокирование доступа к данным.

Основным источником угроз информационной безопасности веб-сайтов являются внешние нарушители, т.е. хакеры или иными словами лица, имеющие высокую квалификацию в вопросах безопасности сайтов и имеющий опыт в проведении сетевых атак.

Распространенность атак на веб-приложения обусловлена двумя ключевыми факторами: низкий порог входа злоумышленников и халатное отношение к безопасности сайта.

Чаще всего, сайты не используют спецсредства для мониторинга, обнаружения и защиты. Кроме того, ответствует персонал компетентный в области угроз безопасности сайта.

Распространенность различных утилит и сканеров веб способствует проникновению потенциальных злоумышленников. Кроме того, различные хакерские форумы распространяют техники атак для всех желающих. А также этому способствует довольно широкая огласка новейших обнаруженных слабых мест и технической составляющей атак.

Есть два вида атак на web-сайты:

1. Целевые атаки – это атаки, изначально имеющие цель получения конфиденциальной информации, проводятся квалифицированными взломщиками, а также носят скрытый характер. Проводятся скрытно, в большинстве случаев достигают своей цели.

2. Нецелевые атаки — это атаки, жертвами которых становятся случайные веб-сайты независимо от популярности. Нецелевая атака на сайт – это попытка получения несанкционированного доступа к веб-ресурсу, при которой злоумышленник не ставит целью взломать конкретный сайт, а атакует сразу сотни или тысячи ресурсов, отобранных по какому-то критерию. Например, сайты, работающие на определенной версии системы управления сайтом.

Основные действия злоумышленников над подверженными взлому сайтами:

Публикация информации не соответствующей действительности;

Получение доступа к серверу, содержащему потенциально ценную информацию;

Атака на базу данных с последующим хищением информации о владельцах банковских карт;

Создание вирусов с легкостью взламывающих пароли почтовых аккаунтов с целью спам рассылки;

Распространение вирусов приводящих к понижению производительности или скорости обмена данными в сети;

Dos-атаки на сеть с целью прерывания трафика путём спама запросами;

Получение доступа к информации SecurlD, которая в свою очередь, используется для обеспечения безопасности в сетях, эта информация может поспособствовать реализации новых атак на беззащитные ресурсы.

Необходимо не забывать о соблюдении базовых мер безопасности при разработке и поддержке работы сайта: Нужно обновлять программное обеспечение, регулярно менять пароли; оградить себя от использования устаревших протоколов, ограничивать физический доступ к вашему серверу, правильно настраивать хостинг и следить за доступами к сайту, хакеры используют новые способы и реализуют все более изощренные атаки с целью взлома систем и кражи данных.

Борьба с новыми атаками требует решений по обеспечению безопасности веб-сайтов, отвечающей требованиям надежности. Выработанные решения должны быть надежными, обеспечивать защиту от атак на уровне приложений и позволять идентифицировать трафик.

Исходя из перечисленного, следует вывод - в настоящее время нужно со всей серьезностью подходить к вопросу безопасности; возникающие угрозы требуют незамедлительного ответа в виде новейших методов и средств обеспечения безопасности, а также решений по реализации защиты веб-сайтов.

Библиографический список

1. Митчелл, К., Конев, А. Обеспечение безопасности веб-сайтов. // Australia: SophosLabs. [Электронный ресурс]. URL:https://yandex.ru/support/webmaster/protecting-sites/contents.xml.

2. Шиффман, М. Защита от хакеров / Шиффман Майк, 2002г. Вильямс.

3.Бирюков, А.А. Информационная безопасность: защита и нападение – М.:ДМК Пресс, 2012. - 474 с.

ВИДЫ СЕТЕВЫХ АТАК И МЕТОДЫ ЗАЩИТЫ

Плотников Д.М., Опалихин Д.В., студенты
Научный руководитель: к. т. н., доцент Трубачева С.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Интернет, возможно, величайшее изобретение в истории человечества. Его появление ознаменовало новую эпоху в нашей истории. Не удивительно, что нечистые на руку люди не смогли пройти мимо интернета, начав изучать нелегальные способы получения информации, а также нанесения ущерба тем или иным лицам. Но какими способами?

Чтобы хорошо разобраться в этом вопросе, следует начать с базового определения. Сетевая атака - комплекс действий, целью которых является получение контроля над удаленной, либо локальной вычислительной сетью; дестабилизация, либо отказ в обслуживании, а также получение конфиденциальных данных пользователей, либо внесение заведомо ложных данных. Различают такие виды атак, как DDoS, mailbombing, MITM (Man-in-the-Middle) , сетевая разведка, ip-spoofing, вирусы, brute force и.т.д. Разновидностей много, каждый вид атаки можно долго рассматривать под разными углами, поэтому рассмотрим лишь некоторую часть.

По данным лаборатории Касперского, в 2014 году их продукты успешно заблокировали 6 167 233 068 вредоносных атак на компьютеры и мобильные устройства пользователей. Решения «Лаборатории Касперского» отразили 1 432 660 467 атак, проводившихся с интернет- ресурсов, размещенных в разных странах мира. На мобильных устройствах было обнаружено 4 643 582 вредоносных установочных пакета. А в течение года с мобильными угрозами по крайней мере один раз встречались 19% пользователей- почти каждый пятый. Одних этих цифр должно быть достаточно, чтобы всерьез забеспокоиться о своей сетевой безопасности.

DDoS

DDoS, возможно, самая распространенная сетевая атака в мире. Расшифровывается как Distributed Denial of Service (распределенный отказ в обслуживании). Есть множество разновидностей DDoS.

Первый тип связан с уязвимостями на атакуемой машине. Зачастую люди забывают своевременно обновлять установленное программное обеспечение, а устаревшие версии содержат в себе ошибки и недоработки. Порой достаточно лишь дать определенную команду такому ПО, и оно перестанет работать корректно, чем и пользуются атакующие.

Второй вариант DDoS- это ping-flood (пинг-флуд). Злоумышленник насыщает канал сервера ping-запросами. Но работает данный метод лишь в том случае, если канал атакующего шире, чем канал сервера. Но поскольку практически все серверы обладают огромной пропускной способностью канала, хакерам приходится использовать «зомби»- зараженные компьютеры. С их помощью они и проводят данную атаку. Также существует схожий тип атаки, HTTP-flood. Разница заключается в том, что при HTTP-flood на сервер поступает множество небольших по размеру HTTP-пакетов, но серверу приходится отвечать на них пакетами, размер которых в десятки раз больше принятых пакетов, что приводит к заполнению канала.

Третий вариант - это DoS-атаки на уязвимости в программном обеспечении DNS-серверов. DNS-сервер преобразует имена хостов в IP-адреса, благодаря чему мы можем заходить на сайты, используя понятные нам имена, а не IP-адреса. В процессе атаки злоумышленник подменяет IP-адрес DNS-сервера домена жертвы. Жертва обращается к определенной HTML-странице, после чего он либо попадает в «черную дыру» (если IP-адрес был заменен на несуществующий), либо попадает на сервер хакера, что наиболее опасно (хакер может получить доступ к данным жертвы).

Способы защиты от DDoS:

1. следить за актуальностью программного обеспечения;
2. никому не сообщать свой IP-адрес;
3. отказаться от Windows Server. Не важно, какого он года. Практика показывает, что перед DDoS Windows Server обречен;
4. использовать оборудование для отражения атак (например, собрать роутер на базе PFSense, также на рынке есть множество решений для этого);
5. правильно настраивайте оборудование и ПО.

Mailbombing

Mailbombing- вид сетевой атаки, при которой злоумышленник, имея электронный адрес жертвы, отправляет на него огромное множество электронных писем. Результат- отказ работы почтового ящика, а иногда и самого сервера. Для защиты достаточно ограничить круг лиц, знающих ваш электронный адрес, а также грамотно настроить почтовые фильтры на стороне сервера.

MITM (Man-In-The-Middle, человек посередине)

MITM — это атака, при которой злоумышленник перехватывает канал связи между двумя системами, получая доступ ко всей передаваемой информации. Также он может модифицировать информацию нужным ему образом, чтобы достичь своих целей. Целями таких атак служат незаконное получение, кража или фальсифицирование передаваемой информации, или же получение несанкционированного доступа к сети. Отслеживается трудно, поскольку обычно злоумышленник находится внутри организации. Рассмотрим схему данной атаки (рисунок 1).

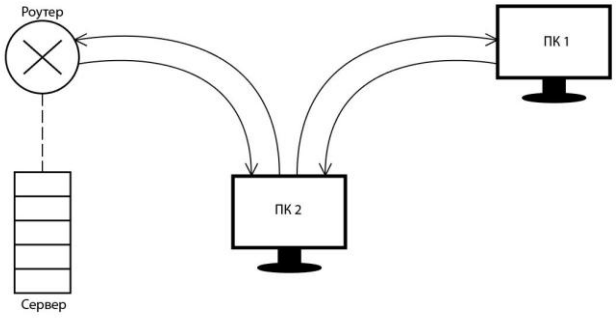

Рисунок 1 — Схема атаки MITM

В нормальных условиях, машина клиента (ПК 1) должна соединяться с сервером по защищенному соединению HTTPS, используя шифрование SSL. Но в случае атаки соединение разрывается, и вместо того, чтобы отправлять данные на ПК 1, роутер отправляет данные на ПК 2 (компьютер зло-

умышленника), который, в свою очередь, пересылает их на ПК 1. Все отправляемые и получаемые машиной ПК 1 данные проходят в незашифрованном виде через ПК 2. Полученные данные можно записывать в текстовый файл, а затем обрабатывать. Если ввести данные в поля для логина и пароля на любом сайте, и произошла ошибка, то данные уже попали к хакеру. Одним из признаков того, что вы подверглись этой атаке, служит подобное предупреждение браузера:

Рисунок 2— Предупреждение браузера о возможной атаке

Следующие методы защиты помогут не стать жертвой MITM-атаки:

1. устаревшие браузеры могут не выдавать предупреждения о нарушении безопасности, необходимо использовать актуальную версию браузера;
2. не стоит передавать конфиденциальную информацию в открытых сетях, в них хакеры способны массово похищать информацию пользователей;
3. не игнорировать предупреждения браузера;
4. использовать плагины для браузера, которые самостоятельно устанавливают защищенное соединение всякий раз, когда эта опция доступна на стороне сервера.

Сетевая разведка

Сетевая разведка - это сбор информации о сети с помощью общедоступных данных и приложений. Сетевая разведка не является атакой на компьютерную систему, т.к. никаких "зловредных" действий хакер при этом не производит. Однако она всегда предшествует нападению, так как при его подготовке злоумышленникам необходимо собрать всю доступную информацию о системе. Вся эта информация собирается с использованием большого набора общедоступных данных и приложений, т.к. хакеру необходимо получить как можно больше полезной информации.

Полностью избавиться от сетевой разведки невозможно. Если отключить эхо ICMP и эхо-ответ на периферийных маршрутизаторах, тогда можно избавиться от эхо-тестирования но потерять данные, необходимые для диагностики сетевых сбоев. А сканировать порты можно и без предварительного эхо-тестирования. Однако это займет больше времени, так как сканировать придется и несуществующие IP-адреса. Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке. А при добросовестном отношении администратора к своим обязанностям это позволяет лучше подготовиться к предстоящей атаке и даже принять упреждающие меры, например, оповестив провайдера, из сети которого кто-то проявляет чрезмерное любопытство.

Вирусы

Компьютерный вирус— вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Основные лазейки, по которым вирусы «пробираются» в компьютер:

1. уязвимости браузеров;
2. бреши в операционной системе;
3. флешки и переносные внешние жесткие диски;
4. электронная почта.

Как обезопасить себя:

1. установить антивирусное ПО, не забывать обновлять его, проверять ПК по меньшей мере раз в неделю;
2. не открывать подозрительные вложения электронных писем, вложения от неизвестных отправителей;
3. использовать отличающиеся, безопасные, длинные пароли;
4. настроить антивирус на сканирование съемных накопителей;
5. проверять антивирусом все архивы и файлы после извлечения из архивов, поскольку не каждый антивирус настроен на их проверку.

6. использовать брандмауэр.

IP-спуфинг

IP-спуфинг- это подмена исходного адреса в заголовке пакетов. Каждый отправляемый по сети пакет имеет IP- адрес, с которого был отослан пакет. Предположим, что какой-то ПК может принимать пакеты только от определенных машин, которые имеют свои уникальные IP- адреса. Злоумышленник отправляет пакеты, в заголовке которых находится IP- адрес одной из допустимых машин. Однако IP- спуфинг не является уникальным способом скрытия/изменения IP- адреса. Удержать адрес из заголовка как свой не получится. Поэтому простейшим способом проверить, что пакет пришел от верного отправителя - отправить пакет на IP отправителя. Обычно для IP-спуфинга используется случайный IP, и вполне вероятно, что ответ не придет. Если же придет, имеет смысл сравнить поле TTL (Time to live) полученных пакетов. Если поля не совпадают — пакеты пришли из разных источников. На сетевом уровне атака частично предотвращается с помощью фильтра пакетов на шлюзе. Он должен быть настроен таким образом, чтобы не пропускать пакеты, пришедшие через те сетевые интерфейсы, откуда они прийти не могли. Например, фильтрация пакетов из внешней сети с исходным адресом внутри сети.

Одним из самых надежных методов защиты от подмены IP-адреса является сопоставление MAC-адреса (Ethernet кадр) и IP-адреса (заголовок протокола IP) отправителя. Например, если пакет с IP адресом из внутренней сети имеет MAC адрес шлюза — этот пакет стоит отбросить.

Brute force

Brute force- способ взлома учётных записей в компьютерных системах, платёжных/банковских сервисах и на веб-сайтах посредством автоматизированного подбора комбинаций паролей и логинов.

Принцип действия брутфорса следующий: хакер пишет специальную программу для подбора паролей, либо использует уже готовое решение своих коллег. Она может быть ориентирована на определённый почтовый сервис, сайт, соцсеть (т.е. предназначена для взлома конкретного ресурса). Далее выполняется подготовка к взлому. Она состоит из следующих этапов:

1. составление прокси-листа. Это нужно для сокрытия истинного IP-адреса, с которого будет производиться brute force;
2. поиск баз для брута. Как правило, брутфорс производится с помощью словаря. Словарь - некое множество комбинаций паролей и логинов, которые программа для взлома будет подставлять в форму авторизации. Так же, как и прокси-лист, словарь имеет вид списка в обычном текстовом файле. Добыть такие словари можно на хакерских форумах. Чем больше база, тем больше вероятность успеха;
3. настройка брутфорса (подключение словаря, прокси-листа);
4. запуск.

Способы защиты:

1. на сайтах стоит ввести политику блокировки учетной записи на определенное время после нескольких попыток ввода;
2. использовать тест запроса-ответа на странице входа в систему (например, reCAPTCHA);
3. использовать утилиты, которые автоматически считывают журналы интернет-событий и оповещают администратора о неоднократных попытках авторизации, исходящих с одного IP-адреса.
4. использовать сложные, уникальные пароли.

Библиографический список

1. Эриксон, Д. Хакинг, Искусство эксплойта / Д. Эриксон. - СПб.: Символ, 2010. -503 с.
2. Касперски, К. Техника и философия хакерских атак - записки мыщ`а / К. Касперски, - М.: СОЛОН-Пресс, 2004. -272 с.

ЗАЩИЩЕННЫЕ ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ

Романов М.А., студент
Научный руководитель: ст. преподаватель Гринцевич Э.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Современный мир требует не только шифровать информацию, но и изолировать от посторонних лиц при передаче. Открытые каналы передачи данных используют в государственных структурах, на промышленных предприятия, в банках и в других сфера жизни и деятельности общества, об-

мен информацией происходит непрерывно и возрастает с ростом технологий. Информация должна поступать вовремя, целая, достоверная и безопасная, ведь она оказывает важное влияние на функционирование во всех отраслях.

Задачи информационной безопасности при передаче данных реализуются с помощью программных средств и с соблюдением критериев: конфиденциальности, целостности и доступности.

Защищенная передача данных реализуется на базе протоколов сетевой безопасности разного уровня модели OSI, направленных на создание удаленного доступа к ресурсам сети через открытую сеть, в настоящее время из наиболее используемых стоит выделить:

Протокол Layer 2 Tunneling Protocol (L2TP) – протокол сеансового уровня, для создания туннелей в сетях IP, ATM, X.25, Frame Relay. В связке с протоколом IPSec задействует транспортную безопасность.

Рекомендации по безопасному использованию протокола L2TP:

1) Аутентификация обоих концов туннеля.
2) Общий секретный ключ для реализаций LAC и LNS.
3) Использование вместе с протоколом IPSec.

Протокол Secure Shell (SSH) - сетевой протокол прикладного уровня, предназначен для создания защищенного соединения с удаленным сервером, может сжимать данные.

Рекомендации по безопасному использованию SSH:

1) Запрет на доступ по SSH с правами root.
2) Установка время бездействия для закрытия неработающей сессии.
3) Доступ SSH к 22 порту через брэндмауэр.
4) Настройка межсетевого экрана для ограничения ip – адресов.
5) Установка сложных паролей.
6) Запрет на доступ с пустым паролем.
7) Анализ отчетов об ошибках.
8) Установка программного обеспечения для предотвращения атак на сервера SSH.

Протокол SOCKET Secure (SOCKS) - сетевой протокол, способный пересылать незаметно пакеты через прокси-сервер от клиента к серверу, проходить межсетевой экран и использовать сервисы за ним.

Уязвимости протокола SOCKS:

1) Возможность фильтрации и подмены данных прокси - сервером.
2) Атаки через плагины и XSS (межсайтинговый скрипт).
3) Сохраненная история на сервере.
4) DNS запросы на стороне клиента.

Рекомендации по обеспечению безопасности протокола SOCKS:

1) Регулярное обновление браузера.
2) Установка расширений для браузера с XSS – фильтрами, для блокировки запуска скрипта.
3) Использование доверенных серверов.

Протокол Ip Security (IPSec) - набор протоколов, передаваемых по межсетевому протоколу IP. IPSec может работать в двух режимах: транспортном - для защиты туннелей между шлюзами, созданных на базе L2TP и туннельный режим - для создания защищенного соединения между удаленными компьютерами.

Рекомендации к безопасному использованию протокола IPSec:

1) Своевременная установка обновлений.
2) Использование стойких ключей и сложных паролей.
3) Совместное использование с протоколом L2TP для создания транспортной безопасности.

Создания защищенного соединения на базе сетевых протоколов безопасности зависит от требуемых задач, настройки и конфигурации оборудования.

Самый оптимальный в использование протокол IPSec, являлся протоколом сетевого уровня с возможностью шифрования, аутентификации и защита при транспортировке IP – пакетов, использование протокола на сетевом уровне никак не отражается на последующих уровнях.

IPSec состоит из трех основных протоколов:

Authentication Header (AH) отвечает за целостность передаваемых данных, аутентификацию отправителя и предотвращает повторную передачу пакетов.

Encapsulating Security Payload (ESP) отвечает за шифрование, ограничение потока зашифрованного трафика. Может выполнять функции протокола Authentication Header.

Internet Security Association and Key Management Protocol (ISAKMP) протокол первичной настройки соединений, взаимной аутентификации конечными узлами друг друга и обмен секретными ключами. Использование протокола Internet Key Exchange, Kerberized Internet Negotiation of Keys, DNS IPSECKEY.

Установление безопасного соединения предполагает связь двух устройств и передачу данных по заранее описанной концепции, возможна настройка степени защиты. Выбор конкретных алгоритмов шифрования из возможных схем, ведется база данных первичных подключений. Используя правила фильтрации можно настроить межсетевой экран для просмотра пакетов.

Работа протокола IPSec.

Фаза 1.

– Аутентификация обеих сторон.

– Security Association (SA) – создание общих параметров, характеризующий безопасное соединение (алгоритм шифрование, хэш-алгоритм, секретные ключи, номера пакетов). Обмен происходит нешифрованными пакетами, по три пакета – агрессивный режим, или по шесть пакетов – стандартный.

– При успешном завершении создаётся Phase SA 1 (IKE SA).

Фаза 2.

– Генерация данных ключей, определение политики безопасности.

– При успешном завершении создается Phase 2 SA (IPSec SA).

– Установка тоннеля завершена.

– Смена ключей Phase 2 происходит через 60 минут, Phase 1 через каждые 24 часа.

– Развитие и совершенствование протоколов безопасности передачи данных исключает получение несанкционированного доступа к информации, передающейся по открытым каналам.

Библиографический список

1. Сетевой уровень модели osi [Электронный ресурс]. Режим доступа: https://studfiles.net/preview/909640/page:13/

2. RFC 1928 — Архитектура протокола SSH [Электронный ресурс]. Режим доступа: https://rfc2.ru/1928.rfc

3. RFC 4251 — Протокол SOCKS 5 [Электронный ресурс]. Режим доступа: https://rfc2.ru/4251.rfc

4. IPSec — протокол защиты сетевого трафика на IP-уровне [Электронный ресурс]. Режим доступа: http://www.ixbt.com/comm/ipsecure.shtml

5. Организация защищенного канала связи [Электронный ресурс]. Режим доступа: http://www.itsec.ru/articles2/Oborandteh/organizaciya-zaschischennogo-kanala-svyazi

6. IPSEC как протокол защиты сетевого трафика [Электронный ресурс]. Режим доступа: http://www.ciscolab.ru/security/page,2,15-ipsec-kak-protokol-zaschity-setevogo-trafika.html

7. 20 советов по безопасному использованию сервера OpenSSH [Электронный ресурс]. Режим доступа: http://rus-linux.net/nlib.php?name=/MyLDP/sec/openssh.html

8. Протокол туннелей на сетевом уровне L2 (L2TP) [Электронный ресурс]. Режим доступа: http://citforum.ru/nets/semenov/4/44/l2pr.shtml

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ АСУ ТП

Савин А.Н., студент
Научный руководитель: к. п. н., доцент Горбачевская Е.Н.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

В настоящее время на современных предприятиях, как производственных, так и непроизводственных, активно внедряются и используются автоматизированные системы управления технологическим процессом (АСУ ТП, SCADA). Это сложнейший программно – аппаратный комплекс, который включает в себя несколько сегментов. Сюда следует отнести контролируемую и управляемую аппаратуру, которая представлена датчиками и исполнительными механизмами; контроллеры специального назначения; программное обеспечение АСУ ТП; сети, с помощью которых указанные компоненты взаимодействуют друг с другом.

В современных реалиях информационно – вычислительные сети взаимодействия АСУ ТП нельзя назвать изолированными, так как они используют общераспространенные технологии передачи данных. Сюда можно отнести TCP/IP в сочетании со специализированными протоколами верхнего уровня.

Обеспечение информационной безопасности (ИБ) АСУ ТП должно реализовывать следующие функции:

- целостность программной среды;
- защиту физических носителей данных;
- комплексную антивирусную защиту АСУ ТП;
- межсетевое экранирование;
- обязательную регистрацию событий ИБ и их расследование;
- способность к обнаружению и противодействию атакам различного характера;
- комплексная защита АСУ ТП и ее компонентов.

Интерес широкого круга специалистов к вопросам защищенности промышленных систем управления возник сравнительно недавно, а именно после серии инцидентов с узкоспециализированными вирусами Stuxnet и Flame. Именно тогда стало понятно, что вопросам информационной безопасности АСУ ТП и ее компонентов уделяется недостаточное внимание.

Среди угроз ИБ, которые в большей степени свойственны АСУ ТП, можно выделить три основные группы: угрозы несанкционированного доступа; угрозы антропогенного характера; угрозы техногенного характера. Рассмотрим наиболее распространенные угрозы безопасности современным АСУ ТП более подробно:

- вирусы;
- инсайдеры;
- хакерские атаки.

Говоря о *вирусах*, нельзя не упомянуть об одном из самых опасных из обнаруженных ранее вирусов - Stuxnet, в июле 2010 года. Этот вирус содержал в себе код, который удовлетворял целому ряду специальных требований, способных реализовать полноценную атаку на АСУ ТП (в данном конкретном случае речь идет о системе производства компании Siemens). Для реализации своего вредоносного потенциала вирус требовал наличия специального оборудования, работающего на определенных частотах. Речь идет о частотных конверторах производства двух компаний.

Согласно проведенному экспертному анализу, специалисты компании Symantec установили, что Stuxnet реализовал атаку сразу на нескольких уровнях. Помимо того, что атака была совершена на уровне операционной системы семейства Windows, также она была совершена на уровне программного обеспечения АСУ ТП компании Siemens, и, непосредственно на уровне контроллеров программируемой логики, которые обслуживали конверторы частоты. В свою очередь, контроллеры управляли скоростью вращения электромоторов.

При попадании на обычный компьютер Stuxnet вел себя как обычный вирус, а именно занимался распространением своих копий и делал попытки установить связь с командным центром. Но если вирус попадал на компьютер с установленным ПО Siemens, Stuxnet реализовывал следующий уровень атаки – он перехватывал управление контроллерами программируемой логики. На третьем “успешном” уровне атаки Stuxnet внедрял в память контроллеров программируемой логики “боевую” часть своего вредоносного кода.

На настоящий момент известно о нескольких модификациях вируса. Они различаются своим наполнением. Наибольший резонанс в сфере информационной безопасности вызвала одна из модификаций, которая периодически проводила изменение частоты инверторов. В результате действий вируса электродвигатели раскручивались до максимальных оборотов, а затем резко останавливались. Технологический персонал, который контролировал удаленно работу оборудования, не фиксировали изменений в работе динамического оборудования. Этот резонанс дошел до правительств ряда стран.

Инсайдеры – являются одной из самых неприятных угроз любой системы управления. Многие предприятия уже внедрили соответствующие меры предосторожности против данного вида угрозы. В первую очередь, это серьезные меры контроля на входе на предприятие, а также между его подразделениями. Во – вторых, это всевозможные предписания и регламенты, которые строго описывают поведение персонала на предприятии. В третьих, большинство в большинстве АСУ ТП реализована ролевая модель, то есть, например, рядовой оператор имеет начальный уровень доступа к системе, и не может выполнять функций, доступных высшим уровням. Старший смены имеет более высокий уровень доступа, так, к примеру, он может управлять системой блокировок, сигнализаций и противоава-

рийной защиты (ПАЗ). Высший уровень доступа имеет системный инженер. Ему доступны функции перепрограммирования, сброс отдельных параметров и прочие функции, недоступные уровням ниже.

В ролевой модели вычислить инсайдера, попытавшегося совершить попытку несанкционированного доступа к конфиденциальной информации, будет достаточно несложно.

Хакерская атака – также чрезвычайно опасное явление, как атака вирусная и инсайдерская. При этом виде атаки злоумышленник способен осознанно повлиять на технологический процесс предприятия. Получая доступ к системе, он подстраивается под специфику ее работы и может атаковать конкретные узлы и сегменты системы. Если сеть хотя бы в одном месте имеет подключение к другим сетям, имеется опасность удаленного доступа. Также не исключается беспроводной доступ к сети.

Самая большая опасность хакерской атаки на сегодняшний день заключается в том, что при современном низком уровне безопасности АСУ ТП для ее успешного проведения достаточно знать лишь сетевой пароль, и иметь доступ в промышленную сеть. Промышленная сеть предприятия зачастую является изолированной, поэтому злоумышленнику не требуется доступ в Глобальную Сеть.

Все эти факторы связаны с тем, что в АСУ ТП крайне редко обновляется программное обеспечение, операционная система и СУБД. Каждый из этих компонентов имеет ряд общеизвестных уязвимостей.

Так как АСУ ТП является важнейшим элементом бизнес – процесса предприятия, вопрос обеспечения информационной безопасности встает в общий ряд с обеспечением физической безопасности предприятия. Это связано с тем, что любое изменение целостности и конфиденциальности данных может привести к нарушению технологического процесса, что, в свою очередь, непременно выльется в финансовые потери, а также может привести к техногенным авариям.

Считаю целесообразным создавать комплекс информационно – технической системы информационной безопасности на каждом предприятии, имеющем у себя на вооружении АСУ ТП. Этот процесс необходимо разделить на три этапа:

1. Определение требований к системе защиты АСУ ТП. На данном этапе необходимо разработать модель возможных угроз и уязвимостей системы;
2. Разработка системы защиты, ее внедрение и ввод в эксплуатацию.
3. Обеспечение информационной безопасности на всем протяжении срока эксплуатации АСУ ТП, с момента ввода в эксплуатацию до момента вывода из нее.

К наиболее подверженным атакам компонентам АСУ ТП относятся: SCADA (от англ. Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных), далее – системы человеко-машинного интерфейса, еще реже подвергаются атакам логические программируемые контроллеры, и крайне редко – используемые в системе протоколы.

Программно – технический комплекс мер призван создать набор основных средств, которые призваны обеспечить информационную безопасность АСУ ТП. На этом уровне должны быть реализованы следующие функции:

- безопасное управление доступом;
- обеспечение целостности данных;
- обеспечение безопасного взаимодействия между различными сегментами сети;
- комплексная антивирусная защита;
- анализ защищенности системы;
- предотвращение и обнаружение попыток несанкционированного доступа;

Подводя краткий итог, необходимо еще раз отметить чрезвычайную актуальность вопроса обеспечения информационной безопасности АСУ ТП на предприятиях и производствах, пренебрежение которой может привести к самым неприятным, и, подчас трагическим последствиям, а также снижением экономической эффективности предприятий.

Библиографический список

1. Информационная безопасность АСУ ТП: Дон Кихот в эру кибероружия. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/post/316184/.

2. АСУ ТП: нужна ли информационная безопасность? [Электронный ресурс]. Режим доступа: https://www.osp.ru/lan/2015/04/13045289/.

3. ИБ АСУ ИП. Персональный сайт Алексея Комарова. [Электронный ресурс]. Режим доступа: https://zlonov.ru/ics-security/.

4. Современные угрозы информационной безопасности АСУ ТП. [Электронный ресурс]. Режим доступа: https://dsec.ru/ipm-research-center/article/how_not_to_disconnect_the_city_modern_ threats

_to_information _security_apcs/.

5. BISA. Обеспечение информационной безопасности АСУ ТП. [Электронный ресурс]. Режим доступа: http://bis-expert.ru/articles/49501.

6. Global CIO. Безопасность АСУ ТП – коммерческие домыслы или практическая необходимость? [Электронный ресурс]. Режим доступа: http://www.globalcio.ru/workshops/39/.

7. AMT Group. Безопасность технологических процессов и АСУ ТП. [Электронный ресурс]. Режим доступа: http://www.amt.ru/pas-security.

8. Anti – Malware. Защита критически важных объектов. [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/security/scada-security.

9. Диалог Наука. Обеспечение безопасности АСУ ТП – Краткий обзор семейства стандартов IEC 62443. [Электронный ресурс]. Режим доступа: http://www.dialognauka.ru/press-center/article/12816/.

10. Vercom. Защита АСУ ТП. [Электронный ресурс]. Режим доступа: http://www.vercom.biz/services/zashchita-asu-tp/.

АНАЛИЗ БЕЗОПАСНОСТИ ПРОГРАММНОГО КОДА

Савкин А.М., Гурко В.В., Куликов К.М., студенты
Научный руководитель: ст. преподаватель Третьякова Т.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Чем сложнее задача автоматизации, тем ответственнее область, в которой использование компьютерных информационных технологий, все больше становятся критическими свойствами, такими как надежность и безопасность информационных ресурсов, используемых в процессе сбора, хранения, обработки, передачи и хранения компьютерных данных. Вредным воздействием на информацию при эксплуатации компьютерных систем (ЭС) для различных целей является нарушение ее конфиденциальности, целостности и доступности. Решение проблем, связанных с предотвращением воздействия непосредственно на информацию является частью комплексной проблемы информационной безопасности и имеет развитую научно-методическую базу.

Мировые исследования последних лет показали, что функциональные и надежные характеристики КС определяются качеством и надежностью программного обеспечения, которое они включают. Кроме проблем качества и надежности программного обеспечения

Безопасность программного обеспечения (ПО) в широком смысле является свойством данного ПО функционировать без проявления различных негативных последствий для конкретной компьютерной системы. Под уровнем безопасности ПО понимается вероятность того, что при заданных условиях в процессе его эксплуатации будет получен функционально пригодный результат.

Угрозы безопасности программного обеспечения возникают как в процессе эксплуатации, так и при их создании, что особенно характерно для процесса разработки ПО, баз данных и других информационных компонентов КС.

Верификация и валидация – это деятельности, по контролю качества программного обеспечения и обнаружение ошибок в нем. Имея общую цель, они различаются в проверке по своим свойствам, правилам и ограничениям, нарушение которых считается ошибкой.

Рисунок 1 - Соотношение верификации и валидации

Термин верификации ПО, означает символьное выполнение программы или проверку кода на

наличие ошибок и уязвимостей методами проверки модели.

На рисунке 2 рассматриваются методы верификации ПО, в основном нацеленные на оценку технических аспектов жизненного цикла, разделяются на следующие группы.

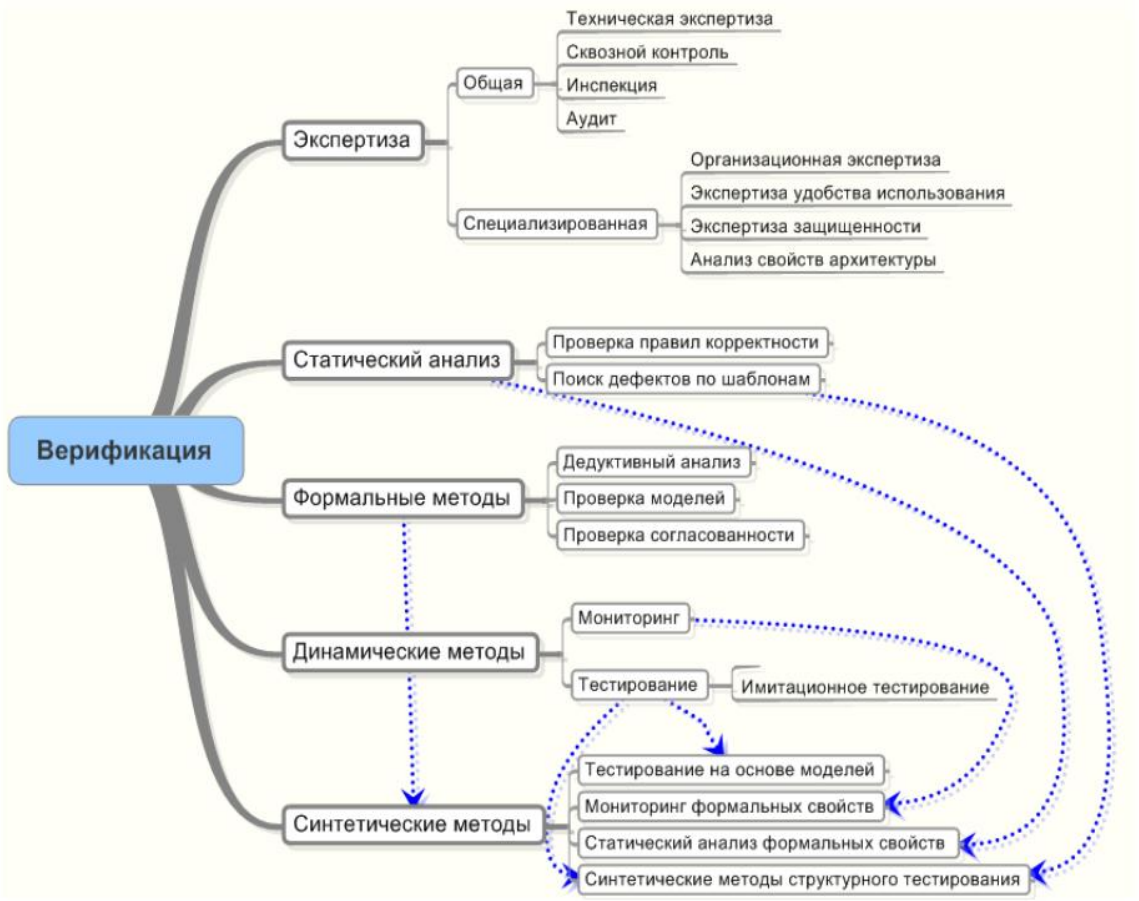

Рисунок 2 - Классификации методов верификации

Одним из важных этапов верификации ПО является проверка ПО на соответствие заявленным качественным характеристикам. Наиболее важные характеристики программного обеспечения:

- корректность (соответствие системы своему предназначению);
- безопасность системы;
- устойчивость системы в случае недетерминированного поведения окружения (например, неверные входные данные);
- эффективность использования ресурсов времени и памяти;
- адаптируемость системы к небольшим изменениям окружения;
- переносимость и совместимость.

Наиболее эффективным и всеобъемлющим методом динамического анализа является тестирование.

Тестирование программного обеспечения направлено на поиск тех ситуаций в программном коде, в которых поведение программы становится недетерминированным, не правильным и не соответствующим спецификации. Обычно тестирование осуществляется в рамках известных, заданных сценариев. На рис. 3 представлены основные виды тестирования ПО.

Обычно методы тестирования включают мониторинг. Этим методы позволяют создать контролируемую среду выполнения программы, что позволяет опробовать различные наборы тесты и запротоколировать полученные результаты. Полноценное тестирование характеризуется тем, насколько хорошо определены цели тестирования, обеспечена полнота тестирования и определены критерии полноты тестирования.

Подготовка тестов производится вручную, процесс тестирования и мониторинга могут быть автоматизированы.

Автоматизированный анализ исходного кода многие считают самым эффективным методом тестирования безопасности на ранних этапах жизненного цикла, поскольку он позволяет оценить лю-

бой фрагмент кода, не требуя завершения работы над приложением в целом. Лучшие технологические решения в этом классе предоставляют наиболее ценные результаты, позволяя точно указать места уязвимости в коде вместе с подробной информацией о типе дефекта, степени критичности и способах исправления. Тестирование на преодоление защиты также является важным элементом обеспечения безопасности программного обеспечения, но его ценность проявляется на более поздних этапах жизненного цикла разработки, когда его можно провести на готовом приложении с функциональным интерфейсом.

Вопросы обеспечения безопасности включают несколько аспектов: авторизация управлением доступом, надлежащая обработка конфиденциальных данных, надлежащее использование данных и доступ к хранилищам и методам шифрования.

Некоторые требования к безопасности классифицируются как нефункциональные требования, например, использование алгоритма шифрования. С другой стороны, другие требования к безопасности, больше полномочий в конкретных случаях и требуют определения основного действия сценария (например, пользователь входит в систему, введя имя пользователя и пароль), альтернативные пути (например, пользователь вводит неправильный пароль) и способы исключения (например, хакер пытается фальсифицировать процесс входа в систему).

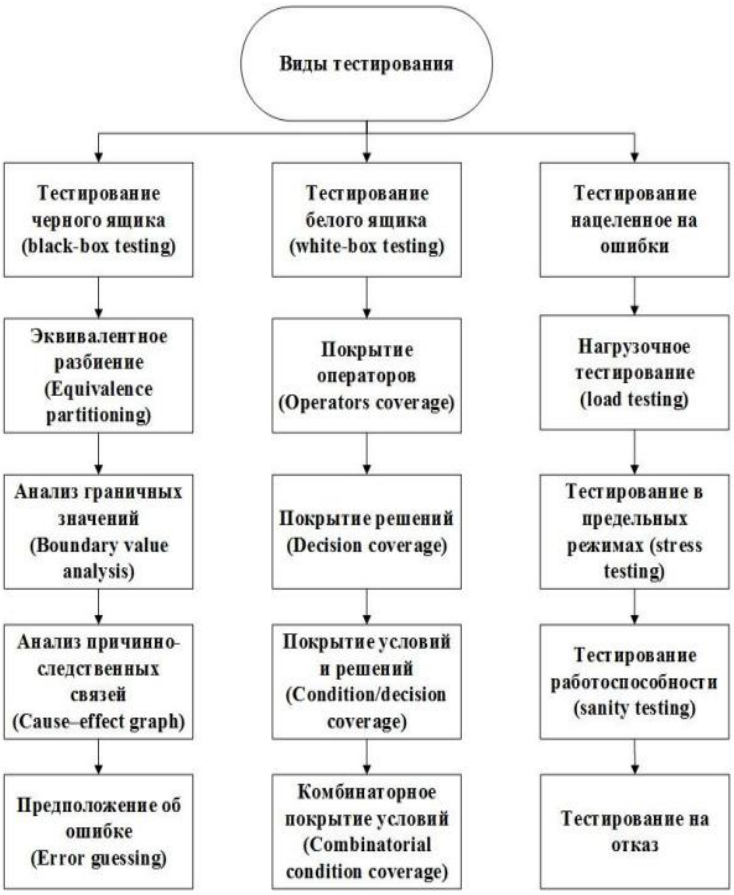

Рисунок 3 – Виды тестирования

Если не определить функциональные и нефункциональные требования и не встроить их должным образом в программное обеспечение, то ошибки в программном коде и дефекты проекта могут возникнуть в приобретенном программном обеспечении и подвергнуться риску критически важную информацию и операций.

Тестирование безопасности и защищённости программных продуктов (ПП) проводится для проверки эффективности используемых механизмов защиты информации, их устойчивости к атакам, а также с целью поиска уязвимостей. Традиционно используются два основных метода тестирования: по методу «черного ящика» и по методу «белого ящика».

Долгое время основным способом тестирования был метод тестирования "черного ящика" программы, куда подавались некоторые данные и проверялись результаты, в надежде найти несоответствия. При этом, как работает программа, считается незначительным. Обратите внимание, что даже при таком подходе необходимо иметь спецификацию программы, чтобы было с чем сравнивать результа-

ты.

Такой подход по-прежнему является наиболее распространенным в повседневной практике, но имеет ряд недостатков. Во-первых, таким способом невозможно найти взаимоуничтожающихся ошибок, во-вторых, некоторые ошибки возникают достаточно редко (ошибки памяти) и потому их трудно найти и воспроизвести.

Метод тестирования, которые изучают не только внешнее поведение программы, но и ее внутреннее устройство (исходные тексты). Такие методики обобщенно называют тестированием "белого ящика". Назовем некоторых представителей этого класса методик: чтение программ, формальные просмотры программ, инспекции и т.п.). Основной трудностью подобных методов является сложность отслеживания вычислений времени выполнения.

При тестировании программы как белый ящик происходит проверка логики программы. Полным тестированием в этом случае будет такое, которое приведет к перебору всех возможных путей. Даже для средних по сложности программ числом таких путей может достигать десятков тысяч.

Основные недостатки и ограничения тестирования по методу «чёрного ящика»:

– сложность, а в некоторых случаях — невозможность полного тестирования всех функций ПП (задача в некоторых случаях эквивалентна достижению 100% покрытия исходного кода ПП в ходе проведения тестирования);

– сложность проверки факта соответствия конкретного ПП его спецификации;

– в основе тестирования по методу «чёрного ящика» зачастую лежит принцип того, что ключевыми моментами для тестирования являются граничные значения возможных входных данных. Т.е. для тестирования функций ПП (в случае слишком большого числа вариантов тестов) достаточно протестировать граничные значения и некоторые (возможно случайные) промежуточные значения входных данных. В случае же тестирования по методу «белого ящика» легче убедиться, путём анализа исходных текстов функций ПП, в том, что действительно код не делает никаких исключений для входных данных и что действительно, те или иные граничные значения достаточно хорошо охватывают то, что нужно протестировать функциональными методами;

– сложность осуществления ряда функциональных тестов, связанная с различного рода техническими трудностями (особенностями используемых операционных систем, временные задержки в работе сети и т.д.);

– особенностью «тестирования безопасности и защищённости ПП» является то, что требования по большой степени являются негативными, т.е., например, «неавторизованные пользователи не должны иметь доступ к защищаемым ресурсам». Подобные требования очень сложно представить в виде конкретных функциональных тестов в форме: «сделать то, сделать то — получить результат». В результате проверка выполнимости таких требований сводится к задаче осуществления полного функционального тестирования, что, как уже отмечалось, достаточно сложно осуществимо или даже невозможно.

Основным же преимуществом тестирования по методу «чёрного ящика» является его объективность. Т.е. потенциальные ошибки, которые могут быть обнаружены методом «белого ящика» требуют практического подтверждения, что они действительно являются ошибками и что существует путь реализовать эти ошибки (т.е. ошибка не отсекается на каком-либо другом уровне проверок), что зачастую проще выполняется именно функциональными методами, как и в случае метода «чёрного ящика».

Преимущества тестирования Белого ящика:

– обнаружение дефектов в "скрытом" коде;
– благотворные побочные эффекты;
– оптимизация;
– приближение к разделению, осуществляемому выполнением эквивалентности;
– необходимость разработчика тщательно обдумывать реализацию.

Недостатки методики тестирования Белого ящика:

– метод обладает недостаточной чувствительностью к ошибкам, упущенным в коде;
– дорогостоимость.

Подготовка и проведение тестирования в проекте создания или сопровождения ПО проходят примерно по следующему плану.

Определение целей тестирования на основе задач и рисков проекта. Эти задачи очерчивают план проверки характеристик и свойств ПО, тщательность тестирования отдельных компонентов и подсистем. Они также определяют используемые в проекте типы тестирования и методы построения

тестов.

Критерии определения тестирования, который будет использоваться в этом проекте. Критерий полноты должен быть согласован с целями тестирования, он управляет выбором тестовых ситуаций для тестирования, а также определяет, когда можно прекратить тестирование.

Построение набора тестов, нацеленных на достижение выбранного критерия полноты и проверяющих определенные ранее требования и ограничения.

Отладка, выполнение тестов и окончательных результатов тестировщиков в виде сообщений о выполненных действиях и нарушениях ограничений проверки. Отладка тестов включает пробные прогоны, устранение обнаруживаемых ошибок в самих тестах, а также описаниях проектных решений и требований, на основе которых получены тесты. По результатам отладки может потребоваться пополнение набора тестов для достижения максимального возможной полноты тестирования в рамках выделенных ресурсов.

Анализ результатов тестирования, сообщение об обнаруженном дефекте и об оценках качества ПО.

Существует большое количество коммерческих и бесплатных статических анализаторов кода. Большой список статического анализатора доступен на Википедии: List of tools for static code analysis. Список языков, для которых существуют статические анализаторы кода, также достаточно велик (Си, Си++, C#, Java, Ada, Fortran, Perl, Ruby, ...).

Aegis - средство автоматического обнаружения дефектов в программах на языках C/C++ на основе статического анализа исходного кода, разрабатывается в лаборатории Digitek Labs с 2008 года. Aegis позволяет выполнять полный и точный анализ многофайловых программных проектов, обеспечивается полная поддержка стандартов и основных расширений языков программирования.

Aegis состоит из набора программ: ssadump, ssald, ssaar и s2a. Утилиты ssadump, ssald и ssaar осуществляют разбор проекта на языке C и формируют внешнее представление модели программы. Приложение s2a выполняет статический анализ и обнаружение дефектов.

Aegis позволяет анализировать многофайловые программные проекты, имеющие одну и более целей сборки. Под целью сборки понимается исполняемый файл, статическая или динамическая библиотека, являющаяся результатом сборки. Обеспечивается возможность анализа частей программ, в том числе отдельных файлов.

Aegis предоставляет несколько интерфейсов пользователя:

- плагин для среды разработки Eclipse
- плагин для среды разработки Netbeans
- web-интерфейс обнаружения дефектов
- интерфейс командной строки

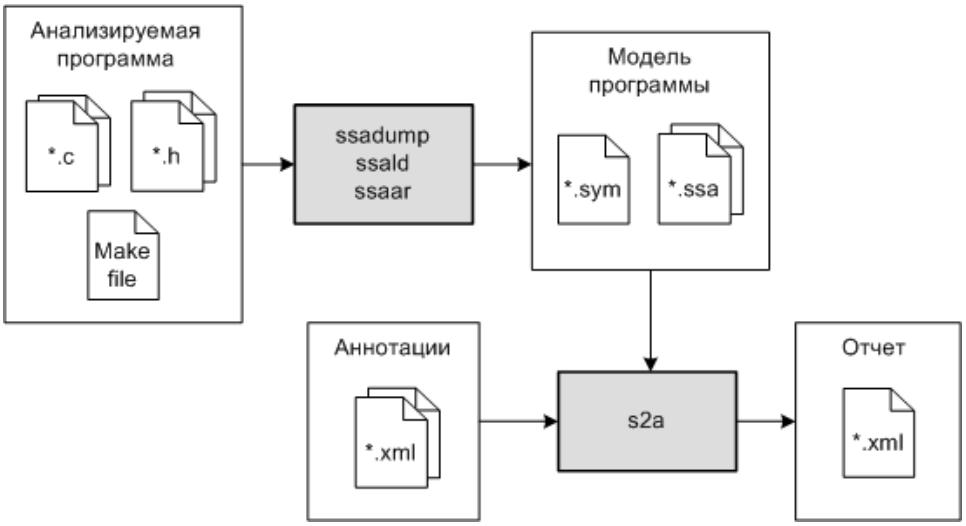

Рисунок 4 – Состав Aegis

Типы дефектов, обнаруживаемых средством Aegis приведены в таблице. Для каждого типа дефектов приведено описание и пример программы на языке C, в котором содержится такой дефект.

Обнаружить дефекты можно воспользовавшись открытым сервисом обнаружения дефектов. Для этого просто копируем пример в буфер обмена и запускаем сервис обнаружения дефектов.

Результаты анализа обнаружения дефектов кода

Длительность анализа: 6 seconds and 472 milliseconds

Путь	Код	Дефекты, контексты
	01: *// Удобный пример с несколькими дефектами*	
	02:	
	03: void **f**(void) {	
	04: int a1[10];	
	05: int a2[15];	
	06: int *pa1 = a1;	
	07: int *pa2=a2+7;	
	08: int diff = (pa2 - pa1); *//BUF-05*	Операции с указателями int pa2 и int pa1 на разные объекты (BUF-05)
	09: }	
	10:	
	11: void **g**(void) {	
	12: int a1[10];	
	13: int a2[15];	
	14: int *pa1 = a1;	
	15: int *pa2=a2+7;	
	16: int diff = (pa2 - pa1); *//BUF-05*	Операции с указателями int pa2 и int pa1 на разные объекты (BUF-05)
	17: }	
	18:	
	19: **main2**(int argc, char* argv[]) {	
	20: **if** (argc == 1) **f**(); **else g**();	
	21: **if** (argv[0][0] == 'c') **f**();	
	22: }	
	23:	
	24: **main1**(int argc, char* argv[]) {	
	25: **main2**(argc, argv);	
	26: }	
	27:	
	28: **main**(int argc, char* argv[]) {	
	29: **main1**(argc, argv);	
	30: }	
		Отсутствует возвращаемое значение у функции main2 (FUNC-03)

Пояснения анализа

Графы таблицы имеют следующие назначения:

Путь — последовательность вызовов функций в программе от вызова из тела main() и до того места, где обнаружен дефект. Другие названия пути — стек вызова, контекст. Когда просматривается дефект и один из его контекстов, доступна навигация по элементам контекста. Начальная точка стека помечается (1), каждая последующая — (2), (3) и т. д. Последняя точка пути — место, где имеется дефект.

Код — проанализированный исходный код. При просмотре дефекта элементы его стека подсвечиваются розовым. Текущая просматриваемая строка подсвечивается красным. В строке, соответствующей дефекту, подчеркиваются переменные, связанные с дефектом.

Дефекты, контексты — графа для выбора просматриваемого дефекта и одного из его контекстов. Контекстов может быть несколько, если существует более одного пути достижения строки с

дефектом. В этом случае в правой части графы доступен выпадающий список, где можно выбрать для просмотра один из контекстов.

Найденные дефекты

Строка	Описание	Стеки вызовов
8	Операции с указателями int pa2 и int pa1 на разные объекты (BUF-05)	+ Дефект 1
16	Операции с указателями int pa2 и int pa1 на разные объекты (BUF-05)	+ Дефект 2
—	Отсутствует возвращаемое значение у функции main2 (FUNC-03)	+ Дефект 3

Длительность анализа: 6 seconds and 613 milliseconds

Исходный файл

```
01: // Удобный пример с несколькими дефектами
02:
03: void f(void) {
04: int a1[10];
05: int a2[15];
06: int *pa1 = a1;
07: int *pa2=a2+7;
08: int diff = (pa2 - pa1); //BUF-05
09: }
10:
11: void g(void) {
12: int a1[10];
13: int a2[15];
14: int *pa1 = a1;
15: int *pa2=a2+7;
16: int diff = (pa2 - pa1); //BUF-05
17: }
18:
19: main2(int argc, char* argv[]) {
20: if (argc == 1) f(); else g();
21: if (argv[0][0] == 'c') f();
22: }
23:
24: main1(int argc, char* argv[]) {
25: main2(argc, argv);
26: }
27:
28: main(int argc, char* argv[]) {
29: main1(argc, argv);
30: }
```

Пояснения

Графы таблицы дефектов имеют следующие назначения:

Строка — номер строки, содержащей дефект. Кликнув на номер строки, можно быстро к ней переместиться.

Описание дефекта содержит характеристику дефекта и его обозначение. Описание, как правило, включает в себя переменные, относящиеся к дефекту, однако, в некоторых случаях вместо имен реальных переменных выводятся внутренние имена, назначенные компилятором.

Стеки вызовов — дефекты и соответствующие им контексты. Особенность данной формы представления состоит в том, что можно просматривать одновременно неограниченное количество дефектов и контекстов. Для просмотра дефекта или контекста необходимо кликнуть соответствующий + слева от его имени. Как и в стандартной форме представления, включенные дефекты и контексты подсвечиваются в коде. Каждый контекст подсвечивается своим оттенком. Доступна навигация по элементам контекста. Текущий элемент выделяется более темным цветом того же оттенка.

Библиографический список

1. Астахов, А. Анализ защищенности корпоративных автоматизированных систем // Jet Info [Эл. ресурс] – URL: www.jetinfo.ru\2002\7\1\article1.7.2002.html
2. Галатенко, В.А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2008. – 208 с.
3. Кулямин, В.В. Методы верификации программного обеспечения. 2008. 117 с. // Единое окно доступа к информационным ресурсам: интернет-портал. Режим доступа: http://window.edu.ru/resource/168/56168
4. Лаборатория программно-аппаратных разработок (Digitek Labs)// Единое окно доступа к информационным ресурсам: интернет-портал. Режим доступа: http://www.digiteklabs.ru/

ПОВЫШЕНИЕ ИНФОРМИРОВАННОСТИ ПЕРСОНАЛА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Садова К.В., аспирант
ФГБОУ ВО «Самарский государственный технический университет»
г. Самара, Россия

Аннотация: В работе рассмотрены подходы к повышению информированности персонала в области информационной безопасности и различные способы их реализации.

Abstract: The paper considers approaches to raising staff awareness in the field of information security and various ways to implement them.

Ключевые слова: информационная безопасность, работа с персоналом, корпоративная сеть, контроль доступа, информационные технологии, сохранность ресурсов, защищенность данных, безопасность информации, утечка данных, информированность

Keywords: Information security, work with personnel, corporate network, access control, information technology, safety of resources, data security, information security, data leakage, awareness.

Трудно отрицать, что мы живем в эру бурного развития информационных технологий. Они становятся неотъемлемой частью нашей повседневной жизни, изменяя ее до неузнаваемости. Как следствие этого, программно-технические и аппаратные средства защиты информации каждый год существенно улучшаются. Но при этом в системе работы каждой компании остается элемент, остающийся критично уязвимым, несмотря на все подобные улучшения. И элемент этот — человек.

Статистика подтверждает это. Почти 75% нарушений информационной безопасности происходит из-за человеческого фактора (Рис. 1). В подавляющем большинстве случаев инциденты вызваны ошибками персонала, возникшими вследствие недостаточной информированности или непонимания важности защиты информации [1]. То есть это те инциденты, которых можно было бы избежать при должном уровне информированности персонала в области информационной безопасности.

Повышение уровня информированности персонала в области информационной безопасности входит в обязанности Chief Information Security Officer (CISO). Chief Information Security Officer - это директор по информационной безопасности, который отвечает, главным образом, за разработку и реализацию политики безопасности компании, адекватной происходящим в ней бизнес-процессам. Также в обязанности CISO входит реализация комплексного подхода к обеспечению безопасности, зачастую они полагаются лишь на технические и правовые методы. Неумение и нежелание специалистов по информационной безопасности работать с персоналом приводит к приведенной выше статистике. Текущие практики показывают, что сотрудники отдела безопасности не готовы к обучению среднестатистического работника, не понимают его интересы и мотивацию.

Сейчас, когда многие отрасли российской экономики столкнулись с кризисом, расходы компаний на информационную безопасность могут быть подвергнуты сокращению. Подразделения компаний менеджеры зачастую разделяют на «доходные» и «расходные», а защита информации в большинстве компаний относится именно ко второй категории, то есть не создает для компании дополнительную прибыль, а лишь сокращает возможные убытки.

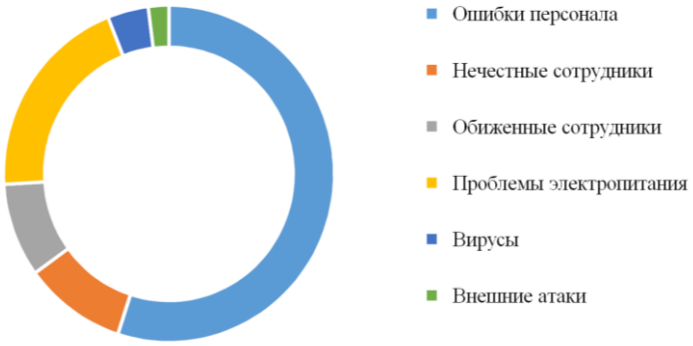

Рисунок 1 - Диаграмма причин инцидентов информационной безопасности

Экономический результат от уменьшения расходов проще просчитать именно на подобных отраслях, поэтому они зачастую лишаются части финансирования. И если даже в 2015 г. в банковской и других сферах доля бюджета информационной безопасности уже была относительно небольшой (рис. 2) [2], то сейчас ситуация может измениться в еще более печальную для обеспечивающих информационную безопасность сотрудников сторону.

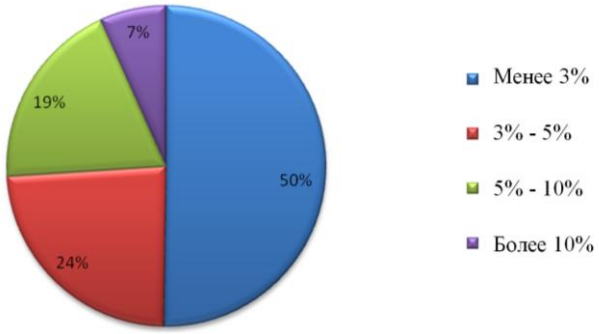

Рисунок 2 - Диаграмма доли бюджета информационной безопасности от бюджета IT в российских банках на 2015 г.

Все это должно подтолкнуть CISO к оптимизации применяемых методов обеспечения безопасности — то есть либо к сокращению расходов на определенные средства с приемлемым падением уровня защищенности, либо к значительному повышению эффективности определенных средств, ведущему к заметному снижению общих рисков, при незначительном изменении расходов. И если будет избран второй путь, то одним из наиболее эффективных методов его реализации может стать внедрение в процесс повышения информированности персонала в области информационной безопасности комплексного подхода.

В общем случае к системе повышения информированности работников компании предъявляются следующие требования [3]:

– возможность регулярного обучения любого количества работников, независимо от их территориального местонахождения и без отрыва от рабочего процесса;

– простота и доступность учебных материалов для различных категорий работников;

– возможность оперативного внесения изменений в программы повышения информированности и учебные материалы.

Во многих практиках основополагающим считается первое требование, причем воспринимается оно скорее, как требование идентичности материалов для повышения информированности для каждого работника. Однако подобный подход ведет к нарушению требования, поэтому целесообразность его применения весьма сомнительна.

Простота и доступность одного и того же материала меняется из-за разной эффективности способов восприятия у людей, различия в их мотивации и сфере деятельности. Поэтому CISO, внедряя общую для всех систему повышения информированности, часто сталкиваются с негативной обратной связью и незначительным снижением частоты инцидентов информационной безопасности, связанных с ошибками персонала.

Необходимость соответствия указанным выше требованиям ведет к внедрению в систему повышения информированности персонала комплексного подхода. Он базируется на диверсификации

подаваемого работникам материала, основанной на определенных признаках. Различные методы комплексного подхода можно классифицировать следующим образом (Рис.3).

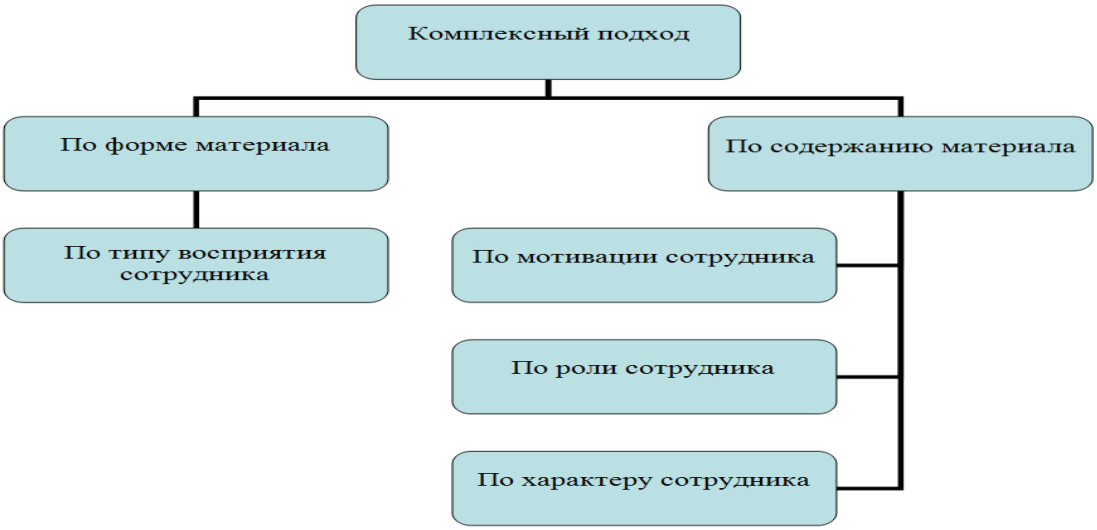

Рисунок 3 - Классификация методов комплексного подхода

Разумеется, интеграция лишь одного из приведенных выше методов зачастую малоэффективна. Необходимо грамотно сочетать их, исходя из доступных ресурсов, временных рамок, размеров и целей компании.

Разберем особенности, преимущества и недостатки приведенных выше методов.

По содержанию материала. Подобный подход предполагает повышение информированности персонала в области информационной безопасности различными по семантической составляющей материалами.

По роли сотрудника. Это один из наиболее часто встречающихся на практике способов внедрения комплексного подхода. Он подразумевает предоставление пользователям только такого материала, который соответствует их уровню доступа и исполняемым функциям. То есть уборщик, например, не будет получать материалы по криптографии в компании. Разумеется, этот подход не предполагает отсутствия общих материалов, таких как информация о коммерческой тайне, но предполагает предоставление пользователям информации лишь о тех системах, с которыми они теоретически могут столкнуться в ходе исполнения своих служебных обязанностей. Благодаря такому подходу возможна реализация одного из основополагающих принципов повышения информированности — многоуровневость, то есть эффективное обучение в организации на каждом уровне, начиная от техника и заканчивая генеральным директором. Впрочем, на практике верхние уровни организации зачастую отчуждают себя от процесса повышения информированности в области информационной безопасности.

В некоторых организациях подобный подход реализован частично, то есть присутствуют специальные документы, однако есть и слабо категоризированная информация, например, перечень сведений, относящихся к коммерческой тайне, найти в котором данные, применимые именно к его роду деятельности, каждому сотруднику может быть довольно проблематично.

Преимущества:

– низкая стоимость и сложность реализации;

– высокая эффективность.

Недостатки:

– не всегда возможно четко очертить круг деятельности сотрудника;

– специалисты по информационной безопасности могут быть вынуждены делегировать распределение материалов руководителям подразделений.

По характеру сотрудника. Довольно очевидно, что рассеянные люди с большей вероятностью оставят записку с паролем на мониторе или забудут носитель с важной информацией, а люди, склонные к получению личной выгоды и обладающие низким показателем морально-нравственных качеств имеют больший шанс начать сотрудничать с конкурирующей компанией, чем прочие сотрудники. Кому-то будет достаточно общего, теоретического обоснования различных требований, другим потребуется практический пример. Выделение влияющих на это черт у персонала и изменение на их основании подаваемого материала может значительно повысить эффективность обучения.

Для внедрения этого метода требуется проведение тестирования особенностей личности сотрудников. И хотя сегодня оно проводится лишь в небольшом числе компаний, с каждым годом подобная практика становится все популярнее. А, значит, через десять лет корректировка программы повышения информированности на его основании может стать довольно распространенной и эффективной практикой.

Однако выделение корреляции между чертами характера и потенциальными угрозами безопасности весьма затруднительно в рамках одной компании по причине недостаточного количества статистики и ресурсов на проведение подобной работы. Поэтому компании, реализующие и интегрирующие подобные решения, могут стать очень востребованными. Но на данный момент подобные компании на широком рынке не замечены.

Преимущества:

– крайне высокая персонифицированность и эффективность.

Недостатки:

– необходимость использования систем тестирования;

– высокая сложность использования собственного решения;

– отсутствие в настоящий момент готовых решений.

По мотивации сотрудников. С.А. Шапиро выделяет следующие типы мотивации сотрудников[4]:

– «инструменталист», заинтересованный в незамедлительном заработке и индифферентный ко всему остальному;

– «профессионал», ставящий во главу угла реализацию и развитие себя как специалиста;

– «патриот», руководящийся моральными и нравственными принципами;

– «хозяин», стремящийся к приумножению собственных богатств, готовый ради этого пойти на серьезный риск;

– «люмпен», желающий перераспределения благ.

Использование при повышении информированности персонала информации о типе мотивации может несколько повысить эффективность обучения. Апеллирование к материальным потерям, порицанию в компании или остановке карьерного роста будет иметь разную значимость для людей с разными типами мотивации.

Преимущества:

– некоторое повышение эффективности.

Недостатки:

– необходимость использования систем тестирования;

– низкая экономическая обоснованность в отрыве от других завязанных на тестировании способов;

– большой объем работы при составлении материалов.

По форме материала (по типу восприятия). На сегодняшний день психологи выделяют четыре типа восприятия:

– визуальный;

– аудиальный;

– кинестетический;

– дискретный.

Эффективность восприятия этими типами различных форм подачи информации может существенно отличаться. Поэтому создание материалов в различной форме: текстовой, звуковой или в виде изображений значительно повысит эффективность программы повышения информированности.

Подача же пользователям информации в соответствующем их типу восприятия виде положительно скажется на мотивации и конечном результате обучения.

Преимущества:

– заметный рост эффективности и мотивации;

– улучшение «фидбека».

Недостатки:

– большой объем работы по созданию материалов в различной форме;

– необходимость использования систем тестирования для максимальной эффективности.

Как видно из приведенной выше информации, интеграция комплексного подхода в систему повышения информированности персонала в области информационной безопасности может существенно повысить эффективность подобных систем. Она позволяет решить основные проблемы, с которыми сталкиваются CISO в процессе проведения программ повышения информированности — низкой

мотивацией и усвояемостью материала. Многие методы, впрочем, требуют использования систем тестирования личности, таких как ЭСКАЛ [5], популярность которых растет с каждым годом, что позволяет надеяться на отсутствие сложности внедрения комплексного подхода уже через несколько лет.

На данный момент на рынке отсутствуют системы, комплексно реализующие подобный подход, однако необходимость в подобных системах растет с каждым годом. Их появление может дать существенный толчок общему уровню информационной безопасности в компаниях.

Библиографический список

1. Официальный сайт компании Микротест / Решение задач в области информационной безопасности URL: http://security-microtest.ru/.

2. Галатенко, В.А. Комплексная защита информации в корпоративных системах: учебное пособие для вузов. – М.: Форум, 2010. – 592 с.: ил:

3. Башлы, П.Н. Информационная безопасность и защита информации: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.- М.: Евразийский открытый институт, 2012. - 311 с. - Режим доступа

4. Шапиро, С.А. Мотивация и стимулирование персонала. — М.: ГроссМедиа, 2005. — 224 с.

5. Официальный сайт экспертной системы комплексного анализа личности (ЭСКАЛ) URL: http://эскал.рф/.

БЕЗОПАСНОСТЬ ОБЛАЧНОГО МИКРОСЕРВИСНОГО РЕШЕНИЯ

Семибратов М.Г., студент
Научный руководитель: ст. преподаватель Плюснина Е.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

При разработке программного решения сложно представить ситуацию, которая полностью избавила бы вас от необходимости обеспечения безопасности. При использовании микросервисного подхода некоторые проблемы становятся более отчетливыми и сложными. Тем не менее, этот подход открывает возможность использовать некоторые особенности данной архитектуры, способные укрепить безопасность.

При использовании микросервисной архитектуры узким местом по-прежнему является сеть. Такая вещь, как контроль доступа, который успешно применяется в рамках монолитных приложений, приобретает новый, почти неожиданный уровень сложности. Это открывает возможности для обсуждения и анализа того, действительно ли архитектура микросервисов решает больше проблем, чем создает.

В тот момент, когда вы обратили должное внимание на выбор архитектурного подхода и решили, что для вас актуальны микросервисы, самое время убедиться, что безопасность в вашем приложении обеспечена на должном уровне. В данной статье будут рассмотрены рекомендации по защите облачного решения, основанного на микросервисной архитектуре.

1. Использование открытого протокола авторизации пользователей и управления доступом OAuth.

Подавляющему большинству приложений требуется обеспечивать контроль доступа и авторизации. Вы, скорее всего, не захотите изобретать колесо с нуля (разве что в академических целях). OAuth / OAuth2 – это открытый протокол авторизации, который, де-факто, является отраслевым стандартом в индустрии, в вопросе идентификации пользователей.

Тем не менее, создание собственного протокола авторизации открывает явные преимущества в ряде случаев, хотя, это крайне не рекомендуется, если у вас нет особых причин для этого.

В то время как стандарт авторизации OAuth не идеален, это широко распространенный стандарт. Преимущество его использования заключается в том, что вы можете полагаться на библиотеки и платформы, которые значительно ускорят этапы разработки приложения и выхода на рынок. Большинство решений для повышения уровня безопасности вашего авторизационного сервиса на основе OAuth уже созданы некоторыми из крупнейших компаний с участием очень умных инженеров.

2. Использование «Защиты в глубину» для определения приоритетности ключевых служб.

Предположение, что одного лишь брандмауэра на вашем сетевом периметре достаточно для обеспечения защиты вашего программного обеспечения, является большой ошибкой. Оборона в глу-

бину – это концепция обеспечения информации, в которой несколько средств контроля безопасности (защиты) размещаются во всей информационной системе. На простом языке это означает, что вам нужно определить самые уязвимые службы и обеспечить им безопасность на различных уровнях, чтобы потенциальный злоумышленник, способный преодолеть один из ваших уровней безопасности, все равно задержится на одном из следующих уровней.

Безопасность – это работа, которую лучше оставить экспертам, а не любителям. Правильная стратегия защиты в глубину, скорее всего, будет успешной, если она будет установлена людьми, которые действительно знают, что они делают.

Микросервисная архитектура упрощает принятие этой стратегии очень грамотным способом: сосредоточив усилия и ресурсы безопасности на конкретных микросервисах. Архитектура дает разнообразие уровней безопасности, которые вы сможете использовать в каждом микросервисе. Таким образом, злоумышленник, который способен использовать одну из ваших служб, может не суметь использовать вторую.

3. Использование существующих библиотек шифрования

На протяжении многих лет люди вкладывали невероятные деньги, время и ресурсы в создание библиотек, которые производят шифрование и дешифрование. Если вы наймете 10 умных и компетентных сотрудников службы безопасности, поместите их в комнату и попросите их придумать лучшую библиотеку для шифрования и дешифрования, я сомневаюсь, что они придумают что-то лучше, чем криптографические библиотеки с открытым кодом, которые уже существуют.

В большинстве случаев, когда речь заходит о безопасности, вы не должны пытаться внедрять свои собственные новые решения и алгоритмы. Даже если у вас есть весомые причины для этого и в вашем распоряжении имеются достаточно опытные люди, вы вряд ли сможете создать что-то такое же хорошее, как инструменты с открытым исходным кодом, которые уже доступны и тщательно протестированы сообществом.

В большинстве случаев вы должны использовать NaCl / libsodium для шифрования. Он существует уже множество лет, надежный, быстрый и простой в использовании. Хотя первоначальная реализация NaCl написана на языке C, она также поддерживает C ++ и Python. И благодаря ответвлениям libsodium доступны несколько адаптеров для других языков, таких как PHP, JavaScript и Go.

4. Использование автоматических обновлений безопасности.

Если вы хотите, чтобы ваша архитектура микросервисов была одновременно защищена и масштабируема, на ранней стадии разработки стоит подумать о том, как автоматизировать или, по крайней мере, контролировать обновления вашего программного обеспечения.

Высокий уровень тестирования здесь более важен, чем когда-либо. Каждый раз, когда часть вашей системы обновляется, вы хотите убедиться, что вы поймаете какую-либо проблему достаточно рано и максимально подробно.

Убедитесь, что ваша платформа в основном атомарна. Это означает, что все должно быть обернуто внутри контейнеров, чтобы в последующем было проще тестировать ваше приложение с обновленной библиотекой или языковой версией – для этого нужно было бы просто обернуть сервис в новый контейнер. Если операция завершится неудачно, то откатить все изменения довольно просто и, самое главное, это можно автоматизировать.

5. Использование распределенного firewall с централизованным управлением

Это все еще неизведанная территория, но я считаю, что firewall, который позволяет пользователям более детально контролировать каждый микросервис (как это предпринимал Project Calico), должен выглядеть примерно так, как мы создаем брандмауэры для микросервисов. Если не сейчас, то по крайней мере, в ближайшем будущем.

Хотя приведенное выше не является исчерпывающим списком, оно затрагивает проблемы, с которыми вы, скорее всего, столкнетесь при создании приложений на основе архитектуры микросервисов.

Когда дело доходит до безопасности, изобретать колесо редко бывает хорошей идеей. Всегда изучайте лучшие практики, принятые в отрасли, и предлагаемые экспертами.

Библиографический список

1. Ньюмен, С. Создание микросервисов // Питер. – 2016. – Глава 9. – С. 213 – 235.

2. John Paul Mueller. Security for Web Developers: Using JavaScript, HTML, and CSS – O'Rally, 2016 P.8 P – 161 - 176.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Серенков А.Г., студент
Научный руководитель: ст. преподаватель Плюснина Е.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

В наши дни все появляется больше угроз информационной безопасности, в том числе и образовательным учреждениям. И список этих угроз постоянно увеличивается. Чтобы оставаться актуальными вслед за угрозами должны изменяться и способы противодействия этим угрозам. «Кто владеет информацией, тот правит миром» - в начале нового тысячелетия эти слова Н. Ротшильда верны как никогда. Ведь доступность информации неизмеримо расширяет возможности, как организаций, так и простых людей. А люди, обладающие ценной, эксклюзивной информацией, порой обладают немалой властью.

В современных учебных заведениях информационная инфраструктура – неотъемлемый компонент учебного процесса. Аудитории комплектуются вычислительной техникой, без которой невозможно полноценное обучение. Поэтому реализация работоспособности и информационной безопасности вычислительных ресурсов является необходимой составляющей качественного обучения. В этой статье я опишу свой взгляд на проблемы информационной безопасности и пути их решения.

В обеспечении информационной безопасности выделяют технический, организационный и документационный аспекты. Технический аспект связан с вычислительной техникой и программными продуктами, организационный – с проведением мероприятий для реализации законов об обороте информации и персональных данных, а документационный – с созданием локальных нормативных актов колледжа. В наших реалиях организационный и документационный аспекты в частично пересекаются.

Для начала рассмотрим технический аспект. Как студенты, так и преподаватели в целях поиска информации активно используют глобальную сеть Интернет. Но знают ли они, какие угрозы их поджидают в Интернете? К сожалению, Интернет далеко не самое безопасное место. В интернете можно встретить случаи мошенничества и обмана, так же Интернет может использоваться для похищения ваших данных. Для защиты от атак используется множество средств, многие из которых дополняют друг друга. В качестве первой ступени защиты часто используются программы, фильтрующие входящий сетевой трафик – прокси-серверы. Подобные программы дают возможность блокировать потенциально опасные и не желательные ресурсы, задавать временные рамки для работы в Интернете. Часто подобное программное обеспечение используется для блокировки развлекательных ресурсов на предприятиях и в учебных заведениях.

Так же на каждый компьютер должен быть установлен антивирус, так как компьютерные вирусы представляют огромную угрозу для данных, хранящихся на компьютере. Вирусы распространяются с зараженными файлами из Интернета, в письмах электронной почты, и на физических носителях. Антивирус осуществляет мониторинг соединений, проверяет скачанные файлы и подключенные устройства на предмет заражения. База сигнатур антивируса должна поддерживаться актуальной, так как список вирусов постоянно пополняется.

Еще для повышения уровня безопасности информационных систем практикуется разграничение доступа к информации и к ресурсам компьютера. Необходимо создать не менее двух учетных записей, одну для работы, вторую для администрирования. Пользовательская учетная запись должна быть ограниченной в правах так, что бы с нее можно было полноценно работать, но нельзя было изменять настройки системы безопасности и устанавливать программное обеспечение. Вторая запись предназначается администратору для настроек защитного программного обеспечения, она обязательно должна быть защищена паролем. Подобное разграничение снижает вероятность намеренного или неумышленного нанесения вреда системе и данным, хранящимся в ней.

Следующим аспектом информационной безопасности мы рассмотрим организационный аспект. Это регламентация учебной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или снижающая вероятность нанесения какого-либо ущерба вычислительной технике и данным, хранящимся на этой технике. Для продуктивной работы все участники образовательного процесса должны понимать проблемы информационной безопасности. К сожалению пользователи часто нарушают порядок работы с информационной системой, и не соблюдают предписания нормативно-правовых документов. По статистике в заражении компьютера в

подавляющем большинстве случаев виноваты именно пользователи. Мероприятия по созданию системы информационной безопасности не должны быть разовыми мероприятиями. Эти мероприятия должны быть направлены на постоянное совершенствование информационной системы. Подобный подход – важное звено в деле обеспечения безопасности информационной системы.

Одной из самых сложных проблем в безопасности информационной системы является присутствие «шпиона». Промышленный шпионаж в наше время не редкость, и порой информацию похищаю те, кто должен был ее защищать. Для предупреждения этой угрозы прививаются понятия «корпоративной этики», ведется мониторинг психологической стабильности преподавателей и работников, в коллективе поддерживается «дружественный» климат.

Перейдем к последнему, документационному аспекту. Ни одна организация не может игнорировать установленные законодательством требования к защите персональных данных граждан. Защита персональных данных это - ряд мер технического, организационного, организационно-технического и правового характера, направленных на защиту сведений, относящихся к субъекту персональных данных (сотруднику или студенту).

Положения о защите персональных данных работников регламентируются:

– Конституцией Российской Федерации;

– Федеральным законом от 27.07.2006 No 149-ФЗ "Об информации, информационных технологиях и о защите информации";

– Федеральным законом от 27.07.2006 No 152-ФЗ "О персональных данных"

– Трудовым кодексом РФ.

Для исполнения Закона No152-ФЗ проводится исследование информационной системы учебного заведения и определяется ее класс. В соответствии с этим разрабатываются: уведомление для Роскомнадзора, приказ об ответственных лицах по сотрудникам, а также положение о защите персональных данных. Это положение является основным локальным актом учебного заведения. Настоящий локальный акт является обязательным к исполнению учебным заведением, а отсутствие подобного квалифицируется государственными органами контроля как нарушение закона.

В сумме защита данных в учебных заведениях сводится к созданию схем обработки данных, включающих:

– формирование внутренней документации, содержащей указания по работе с персональными данными;

– создание системы защиты персональных данных;

– интеграция технических мер защиты персональных данных.

Отличительная черта учебных заведений заключается в том, что обработке подвергаются не только данные сотрудников, но и данные учащихся и их родителей. Соответственно разрабатываются формы получения согласия на обработку персональных данных от учащихся и, если учащийся не совершеннолетний, от его родителей.

В заключение следует сказать, что, обеспечение информационной безопасности учебного процесса в современных условиях становится одним из видов деятельности учебных заведений. Мир бросает все новые вызовы, и информационная безопасность обязана успевать отвечать на них разрабатывая новые подходы к обеспечению безопасности, постоянно находясь в поиске новых форм и способов обеспечения информационной безопасности.

Библиографический список

1. Иноземцев, В.Л. Творческие начала современной корпорации // Мировая экономика и международные отношения. – 2011. - No 11. – С. 18 – 30.

2. Скиба, В.Ю. Курбатов, В.А. Руководство по защите от внутренних угроз информационной безопасности / Скиба В.Ю.: Питер. – 2008. – 320 с.

3. Романец, Ю.В., Тимофеев, П.А., Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. М: "Радио и связь", 1999. – 328.

4. Федеральный закон от "О персональных данных"

5. Федеральный закон от "Об информации, информационных технологиях и о защите информации"

6. Трудовой кодекс Российской Федерации

БЕЗОПАСНОСТЬ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ НА НОУТБУКАХ И КПК

Тихов И.М., студент
Научный руководитель: к. т. н., доцент Федосеева О.Ю.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Защита и безопасность конфиденциальной информации от несанкционированного доступа - одна из самых злободневных проблем на сегодняшний день. В данной статье Вы узнаете технологии, которые смогут надёжно защитить данные на ноутбуках и КПК, используя технологии шифрования и сильной аутентификации. По результатам экспериментов профессионалов, это самый эффективный, а зачастую и единственный способ, который позволит обезопасить информацию и одновременно удобство доступа к ней.

Основной проблемой является то, что за несанкционированным доступом к конфиденциальной информации часто следует её кража. В связи с этим явлением убытки компании могут возрасти в n-ое количество раз, в зависимости от ценности похищенных данных. Плюс ко всему, зачастую фирмы сталкиваются и с физической кражей мобильных устройств. В результате кражи также возникает угроза несанкционированного доступа к данным.

Важно подчеркнуть, что помимо защиты конфиденциальных данных от угрозы несанкционированного доступа, необходимо оберегать и Ваше физическое устройство. При этом необходимо учесть, что разработанная система безопасности не должна доставлять пользователю трудностей и каких-либо неудобств. Она, наоборот, должна быть прозрачной и удобной для него, где бы ни использовался физический носитель.

Технологии шифрования данных

Технология шифрования является наиболее эффективным, широко распространённым и доступным способом защиты данных от несанкционированного доступа. Но для того, чтобы надёжно защитить свои данные, нужно обладать соответствующими знаниями в этой области.

Рассмотрим основные виды технологии шифрования:

1. **Пофайловое шифрование.**

В этом случае юзер сам выбирает файлы, которые следует зашифровать. Эта технология не требует глубокой интеграции средства шифрования в систему. Она позволяет производителям криптографических средств реализовать мультиплатформенное решение для Windows, Linux, MAC OS X и т.д.

2. **Защита процесса загрузки.**

ОС не сможет запуститься, если зашифрован весь диск целиком. Это будет продолжаться до тех пор, пока какой-либо механизм не расшифрует файлы загрузки. В связи с этим, шифрование всего диска обязательно подразумевает и защиту процесса загрузки. Как правило, пользователю требуется ввести пароль, чтобы операционная система могла стартовать. Поэтому, если пользователь введет пароль правильно, то программа шифрования получит доступ к ключам шифрования, что позволит читать дальнейшие данные с диска.

3. **Шифрование виртуальных дисков.**

Эта технология подразумевает создание большого скрытого файла на жестком диске. В дальнейшем этот файл доступен пользователю как новый логический диск.

4. Шифрование всего диска. В данной технологии шифруются все системные файлы.

5. Шифрование каталогов. Пользователь создает папки, все данные в которых шифруются автоматически. Шифрование каталогов довольно удобно и прозрачно. Данный подход зависит от платформы и требует глубокого взаимодействия с операционной системой.

Использование сильной аутентификации

Самым эффективным способом хранения ключей шифрования, паролей, цифровых сертификатов является применение строгой двухфакторной аутентификации на основе аппаратных ключей или смарт-карт. Для того, чтобы успешно пройти процедуру сильной аутентификации, пользователю необходимо предъявить USB-ключ или смарт-карту операционной системе, а потом доказать свое право владения этим электронным ключом (то есть ввести пароль). Тем самым Вы сильно усложните задачу злоумышленнику, пытающегося получить доступ к данным, так как ему потребуется не просто ввести пароль, но и обладать физическим носителем.

Вывод

Надёжная защита данных подразумевает использование надежных средств шифрования, а также средств сильной аутентификации. Для применения технологии пофайлового шифрования стоит выделить программу PGP. Данная программа сможет удовлетворить большинство запросов пользователя.

Эффективную защиту данных на мобильных устройствах, ноутбуках и КПК Вам поможет обеспечить «Лаборатория Касперского». В его состав входят: антивирус и средства шифрования, которые обеспечат полноценное шифрование конфиденциальных данных.

Библиографический список

1. Гатченко, Н.А., Исаев, А.С., Яковлев, А.Д. Криптографическая защита информации.
2. Бауэр, Ф. Расшифрованные секреты. Методы и принципы криптологии.
3. Мао, В. Современная криптография. Теория и практика.
4. Алферов, А.П., Зубов, А.Ю., Кузьмин, А.С., Черемушкин, А.В. Основы криптографии. М.: Гелиос АРВ, 2001.
5. Сингх, С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006.

СРАВНЕНИЕ АНТИВИРУСНЫХ ПРОДУКТОВ КОРПОРАТИВНОГО СЕГМЕНТА

Филимонов Е.О., студент
Научный руководитель: ст. преподаватель Плюснина Е.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

На текущий момент на рынке представлен огромный выбор антивирусных продуктов корпоративного сегмента, однако у каждого из таких продуктов имеются как слабые, так и сильные стороны. На российском рынке корпоративных антивирусных продуктов наиболее популярными являются Kaspersky Endpoint Security производства АО “Лаборатория Касперского”, ESET Endpoint Security производства компании “ESET” и Dr.Web Enterprise Security Suite производства ООО «Доктор Веб». Рассмотрим указанные выше продукты подробнее в таблице 1.

Таблица 1 - Сравнение функционала антивирусных продуктов

Продукт / Функции	Kaspersky Endpoint Security	ESET Endpoint Security	Dr.Web Enterprise Security Suite
Наличие консоли мониторинга и управления	Да, входит в пакет	Да, не входит в пакет	Да, входит в пакет
Шифрование конфиденциальной информации	Да	Нет	Да
Контроль подключения устройств	Да	Да	Нет
Антивирус для мобильных устройств	Да, входит в пакет	Да, не входит в пакет	Да, входит в пакет
Управление мобильными устройствами и приложениями	Да, входит в пакет	Нет	Да, входит в пакет
Средняя стоимость на 1 устройство	2800руб.	1465руб.	1320руб.

По данным таблицы 1 видно, что наибольшим функционалом обладает продукт Kaspersky Endpoint Security производства АО “Лаборатория Касперского”, однако средняя стоимость данного продукта более чем в 2 раза выше чем аналогичный продукт Dr.Web Enterprise Security Suite производства ООО «Доктор Веб».

Однако, немаловажным фактором в выборе продукта комплексной защиты является оказываемое воздействие продуктом антивирусной защиты на быстродействие операционной системы и прикладных программ. Рассмотрим результаты тестирования, указанных выше антивирусных продуктов, в таблице 2.

По данным таблицы 2 видно, что наилучшим быстродействием обладает продукт ESET Endpoint Security производства компании “ESET”, затем идет Kaspersky Endpoint Security производства АО “Лаборатория Касперского” и замыкает тройку Dr.Web Enterprise Security Suite производства ООО «Доктор Веб».

Таблица 2 - Результаты тестирования быстродействия

Наименование проверки	Результаты без продукта	Kaspersky Endpoint Security	ESET Endpoint Security	Dr.Web Enterprise Security Suite
Старт системы, секунд	21,05	48,38	28,40	35,13
Запуск браузера, секунд	2,5	9,5	4,7	7,3
Распаковка архива, минут	2:27	2:45	2:30	2:36
Сканирование системного диска, минут	-	10:08	6:04	30:12
Потребляемый объем ОЗУ при простое, МБ	-	65	60	110
Потребляемый объем ОЗУ при сканировании, МБ	-	170	65	200

В результате проделанной работы видно, что по соотношению функционал/быстродействие лучшие результаты показал антивирусный продукт Kaspersky Endpoint Security производства АО “Лаборатория Касперского”.

Библиографический список

1. Официальный сайт АО «Лаборатория Касперского» - Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ. https://www.kaspersky.ru/small-to-medium-business-security/endpoint-advanced
2. Официальный сайт компании «ESET» - ESET Endpoint Security для Microsoft Windows. https://www.esetnod32.ru/business/products/ees_win/
3. Официальный сайт ООО «Доктор Веб» - Dr.Web Enterprise Security Suite. https://products.drweb.ru/enterprise_security_suite/
4. Рейтинг быстродействия антивирусов Dr.Web, ESET NOD32, Kaspersky и Norton. https://www.olof.ru/wikibase/softreviews/reyting/

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX

Финагеев И.С., студент
Научный руководитель: к. т. н., доцент Трубачева С.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Аннотация

Обзор стандартных и не стандартных средств защиты, предоставляемых операционной системой Linux для безопасного функционирования системы, безопасной работы всех пользователей и безопасного хранения информации, для которой эта ОС может использоваться. В данной работе также будут затронуты вопросы сетевой безопасности, поскольку к основным назначениям ОС Linux относят работу в сети.

Для различных категорий людей понятие «безопасность» имеет разное значение. При этом этот термин имеет множество разновидностей связанных со всеми сферами деятельности человека. Безопасность жизнедеятельности или государственная безопасность, политическая или строительная безопасность, все это примеры понятия «безопасность» Обобщенное же определение термина «безопасность» можно сформулировать так: **безопасность** – это набор средств и требований, направленных на предотвращение запрещенных действий, выполнение которых может привести к нежелательным последствиям.

Под безопасностью операционной системы понимается безопасность самого ядра операционной системы, а также безопасность программного обеспечения, установленного на ней. Но можно выразиться и другими словами, **безопасность операционной системы** – это комплекс мер, направленных на предотвращение действий со стороны пользователя или других программ, которые могут привести к нарушению нормального функционирования операционной системы.

Производители ОС по-своему взглянули на безопасность своих ОС. Это привело к тому, что одни системы имели достаточную защиту, защиту других обойти было не просто, а третьи практически не обладали механизмами защиты перед взломщиками. В данной работе рассматривается степень защищенности ОС Linux – одной из UNIX-подобной ОС.

Linux является сетевой ОС, что приводит к тому, что провести границу между сетевой и локальной безопасностью очень затруднительно. Однако, компьютер, на котором установлена ОС

Linux, может выступать как в качестве сервера, так и использоваться как пользовательский компьютер, его подключение к сети не гарантируется. Если сеть говорить о сетевой безопасности абсолютно не уместно, поскольку сетевой угрозы в данном случае не существует. Таким образом, деление общей безопасности системы на две составляющие вполне целесообразно.

Это приводит нас к следующему выводу, что локальная безопасность необходима в любом случае, кроме тех, когда к компьютеру имеет доступ только один пользователь – его владелец. В случае с сетевой безопасностью, ее актуальность проявляется только тогда, когда на компьютере с ОС Linux имеется выход в сеть. Сетевая безопасность относится к дополнительному звену локальной безопасности, которые совместно определяют общую безопасность системы в целом.

Так какие же средства предоставляет система Linux для обеспечения локальной безопасности.

В ОС Linux каждый пользователь имеет свой уникальный числовой идентификатор, по которому он идентифицируется в системе. Этому идентификатору соответствует имя пользователя. Имена всех пользователей ОС Linux и соответствующие им идентификаторы хранятся в специальном файле passwd. Файл passwd располагается в каталоге etc находящийся в корневом каталоге системы /. Файл имеет обычную текстовую форму.

Поскольку Имя пользователя не является секретной информацией, ведь его могут узнать другие пользователи системы появляется опасность входа одного пользователя под именем другого. Однако этого не происходит, так как применяется механизм аутентификации.

Для аутентификации в ОС Linux используется надежное средство – пароль.

Каждый пользователь в системе имеет свой собственный пароль. Наличие пароля – одно из составляющих политики безопасности пользователей Linux. Без пароля, зная только имя пользователя, проникнуть в систему невозможно.

Пароли хранятся в отдельном файле /etc/shadow. В ранних версиях Linux имена и пароли пользователей хранились в одном файле /etc/passwd. Однако, практика показала, что для обеспечения большей защиты паролей необходимо создание отдельного файла для их хранения. Таким образом, технология выделения отдельного файла shadow для хранения паролей получила название технологии «теневых паролей».

К файлу паролей имеет доступ только суперпользователь, и ни кто другой. Содержимое файла является недоступным для обычных пользователей, исключая возможность раскрытия зашифрованного пароля.

Для организации и постоянного хранения информации на различных ее носителях ОС использует файловую систему.

В ОС Linux для хранения информации используется файловая система ext2 (The Second Extended File System). Ext2 является файловой системой с огромными функциональными возможностями, а с учетом того, что ext2 была разработана специально для Linux, уже говорит о необходимости присутствия в ней средств контроля и безопасности.

Файловая политика безопасности Linux заключается в том, что любой файл системы делится на 3 категории владельцев: владелец файла (его создатель), группа пользователей, в которую входит владелец файла, и всех остальных. Таким образом, привилегированный пользователь или владелец файла, имеющий возможность изменять права доступа, может построить политику файловой безопасности, определяя права отдельно для владельца файла, для группы пользователей и для всех остальных пользователей системы.

Права доступа к файлу или каталогу описываются тремя восьмеричными цифрами, самая левая из которых – права доступа владельца, средняя – права группы, правая – права доступа для всех остальных. Каждая из этих восьмеричных цифр представляет собой битовую маску из 3-х бит. Эти биты отвечают за право на чтение, запись и исполнение файла или каталога. Если бит установлен в 1 – операция разрешена, если в 0 – запрещена.

Однако в структуре файлов любой операционной системы всегда есть файлы, которые не должны изменяться в процессе функционирования системы, например, исполняемые файлы или файлы, которые должны быть откорректированы только однажды при настройке системы и не должны изменяться впоследствии. Наличие средств, гарантирующих выполнение перечисленных условий, позволяет очень сильно повысить безопасность файловой системы, сохранив первоначальную целостность данных при различных типах атак.

В файловой системе Linux помимо прав доступа присутствует поддержка расширенных атрибутов файлов.

Политика безопасности, построенная на установке дополнительных атрибутов является только одной частью безопасности. Поскольку эти атрибуты хоть и предотвратят изменение защищенных

ими файлов даже со стороны процессов, которые выполняются от имени привилегированного пользователя, пользователь root все равно может убрать эти атрибуты и продолжить работу с файлами уже без этих них. Другими словами, ничто не мешает программе, исполняемой от имени пользователя root, перед началом работы выполнить проверку файла на наличие этих атрибутов и просто их отменить.

Дополняющим компонентом безопасности можно считать специальные возможности ядер 2.4 ОС Linux, позволяющие конфигурировать систему в режиме полной защиты файлов с атрибутами immutable и append до момента перезагрузки в однопользовательский режим.

Локальная безопасность – необходимая составляющая общей безопасности системы. Она позволяет устранить угрозу локального взлома. Однако, поскольку практически отсутствуют компьютеры подключённые к сети интернет возникает еще один тип угрозы – сетевой. Для устранения сетевой угрозы существуют различные средства и методы. Одним из ключевых средств защиты безопасности системы является брандмауэр.

Брандмауэр (firewall) - это система или группа систем, реализующих правила управления доступом между двумя сетями.

Ядро ОС Linux версии 2.4 и более поздних имеет встроенный межсетевой экран netfilter, который обладает следующими возможностями:

- позволяет осуществлять фильтрацию входящих, исходящих и транзитных пакетов, основываясь на содержании заголовка пакета, типе пакета, определяющего его состояние в соединении, IP адресе компьютера-отправителя и компьютера-получателя, MAC адресе отправителя и получателя и так далее.

- позволяет осуществлять трансляцию сетевых адресов NAT (Network Address Translation) и подмену портов NPT (Network Port Translation). Действие NAT заключается в подмене IP адреса компьютера-отправителя или компьютера-получателя на указанный.

- позволяет менять специальные поля заголовка пакета, такие как TOS (Type Of Service) и TTL (Time To Live), что предоставляет расширенные возможности для управления процессом маршрутизации.

Помимо стандартных средств безопасной работы Linux существует огромное количество дополнительного системного программного обеспечения, позволяющего расширить возможности стандартных средств и добавить новые, более гибкие и приспособленные к специфическим условиям.

Linux ACLs (Access Control Lists) – это набор заплаток для ядра операционной системы и приложений для работы с файловой системой и несколько дополнительных программ, дающих возможность устанавливать права доступа к файлам не только для пользователя-владельца и группы-владельца файла, но и для любого пользователя и группы.

Linux ACLs использует расширенные атрибуты для хранения данных о правах доступа к файлам пользователей и групп. Список расширенного контроля доступа существует для каждого файла в системе и состоит из шести компонентов. Первые три являются копией стандартных прав доступа к файлу. Они содержаться в единственном экземпляре в ACL и есть у каждого файла в системе.

LIDS (Linux Intrusion Detection/Defence System) – система обнаружения и защиты от вторжения. Эта система представляет собой дополнение к ядру операционной системы Linux, добавляющее дополнительные возможности для увеличения безопасности операционной системы. LIDS позволяет запретить или ограничить доступ к файлам, памяти, устройствам, сетевым интерфейсам и запущенным приложениям привилегированному пользователю, что дает возможность надежно оградить даже взломанную операционную систему от дальнейшего вмешательства.

В отличие от других средств защиты операционной системы Linux, эту систему невозможно отключить, не зная пароля администратора LIDS, который в зашифрованном виде хранится в специальном файле, видимом только программой администрирования LIDS.

AIDE (Advanced Intrusion Detection Environment) – расширенное окружение обнаружения вторжений. Основное назначение программного продукта AIDE – обнаружения изменения файлов, их атрибутов, прав доступа, пользователей владельцев, размера, количества ссылок на файл и других параметров, которые присущи файлу в Linux.

Программный пакет AIDE создает базу данных всех файлов, перечисленных в основном конфигурационном файле программы aide.conf. В базу помимо стандартных атрибутов файла записывается также криптографическая контрольная сумма или хэш каждого файла, вычисленных с использованием одного или комбинации следующих алгоритмов шифрования: SHA1, MD5, RMD160, TIGER.

В данной статье были рассмотрены средства безопасности, которыми располагает семейство ОС Linux для безопасного функционирования как в качестве пользовательской системы, так и в качестве сервера.

Библиографический список

1. Linux глазами хакера 4-е издание. Михаил Фленов, издательство «БХВ-Петербург», Санкт-Петербург, 2016.

2. Администрирование и безопасность операционных систем Linux, Бакланов В.В., издательство Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2005.

3. Техническая электронная документация по операционной системе Linux.

ЗАЩИТА ДАННЫХ 1С:ПРЕДПРИЯТИЯ

Ческидов Е.С., Баннов А.А., студенты
Научный руководитель: к. п. н., доцент Горбачевская Е.Н.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Информационная безопасность, как и защита информации – задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных, особо остро данная проблема стоит в области финансовых учетных систем. Наиболее популярной системой бухгалтерского учета, ведения продаж, CRM процессов в России является система 1С Предприятие.

Использование 1С с базами в файловом формате. Файловые базы 1С являются наиболее уязвимые к физическому воздействию. Связано это с особенностями архитектуры такого типа баз – необходимостью держать открытыми (с полным доступом) все файлы конфигурации и самих файловых баз для всех пользователей операционной системы. В результате, любой пользователь, имеющий право работать в файловой базе 1С, теоретически может скопировать или даже удалить информационную базу 1С двумя кликами мышки.

Использование 1С с базами в СУБД формате. Данный тип проблем возникает, если в качестве хранилища баз 1С используется СУБД (PosgreSQL, MS SQL), а в качестве промежуточной службы связи 1С и СУБД используется сервер 1С предприятия. Такой пример – во многих компаниях практикуется доработка конфигураций 1С под свои нужды. В процессе доработки, в условиях проектной «суеты», постоянных испытаний нового доработанного функционала – ответственные специалисты зачастую пренебрегают правилами сетевой безопасности.

В результате, некоторые личности, которые имеют прямой доступ к базе данных СУБД или имеют права администратора на сервере 1С Предприятие, пусть даже на временный тестовый период – могут либо сделать резервную копию на внешние ресурсы, либо вовсе удалить базу данных в СУБД.

Открытость и доступность серверного оборудования. При наличии несанкционированного доступа к серверному оборудованию сотрудники компании или третьи лица могут использовать этот доступ для кражи или порчи информации. Проще говоря – если злоумышленник получает доступ непосредственно к корпусу и консоли сервера 1с – круг его возможностей расширяется в десятки раз.

Риски кражи, утечки персональных данных. Под актуальными угрозами безопасности персональных данных здесь понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, например, ответственными сотрудниками, операторами ПК, бухгалтерией и т.д. Результатом этого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия ответственных лиц.

Сетевая безопасность. Информационная система предприятия, построенная с нарушением ГОСТ, требований к безопасности, рекомендаций, либо не имеющая надлежащей ИТ-поддержки – изобилует дырами, вирусным и шпионским программным обеспечением, множеством бэкдоров (несанкционированных доступов во внутреннюю сеть), что напрямую влияет на сохранность корпоративных данных в 1С. Это приводит к легкому доступу злоумышленника к коммерчески значимой

информации. К примеру, свободный доступ к резервным копиям, отсутствие пароля на архивы с резервными копиями злоумышленник может использовать в корыстных целях. Не говоря уже об элементарном повреждении базы 1С вирусной активностью.

Взаимосвязь 1С с внешними объектами. Еще одной потенциальной угрозой является необходимость (а иногда и специальная маркетинговая особенность) учетной базы 1С связываться с «внешним миром». Выгрузки/загрузки клиент-банков, обмен информацией с филиалами, регулярная синхронизация с корпоративными сайтами, порталами, другими программами сдачи отчетности, управления клиентами и продажами и многое другое. Поскольку в данной области 1С не приветствуются соблюдения стандартов безопасности и унифицированности сетевого обмена информации – утечка вполне реальна на любом отрезке пути ее следования. В результате потребностей в нестандартных доработках автоматизации процессов или сокращения бюджета на необходимые меры по защите трафика – в учетной системе мгновенно растет количество уязвимостей, дыр, небезопасных соединений, открытых портов, легкодоступных файлов обмена в незашифрованном виде и т.д. Можно смело представить себе, к чему это может привести – начиная от элементарного вывода из строя базы 1С на определенное время, заканчивая подделкой платежного поручения на несколько миллионов.

Для решения всех вышеизложенных проблем необходимо проводить следующие меры:

1. **При работе с файловыми базами 1С** обязательно внедрить ряд мер по обеспечению безопасности баз:

– Используя разграничения доступа NTFS, дать необходимые права только тем пользователям, которые работают с этой базой, тем самым обезопасив базу от кражи или порчи недобросовестными сотрудниками или злоумышленником;

– Всегда использовать авторизацию Windows для входа на рабочие станции пользователей и доступ к сетевым ресурсам;

– Использовать шифрованные диски или шифрованные папки, которые позволят сохранить конфиденциальную информацию даже при выносе базы 1С;

– Установить политику автоматической блокировки экрана, а также провести обучение пользователей для разъяснения необходимости блокировки профиля;

– Разграничение прав доступа на уровне 1С позволит пользователям получать доступ только к той информации, на которую они имеют соответствующие права;

– Необходимо разрешить запуск конфигуратора 1С только тем сотрудникам, которым он необходим.

2. **При работе с СУБД базами 1С** требуется обратить внимание на следующие рекомендации:

– Учетные данные для подключения к СУБД не должны иметь административных прав;

– Необходимо разграничивать права доступа к базам СУБД, например, создавать для каждой информационной базы свою учетную запись, что позволит минимизировать потерю данных при взломе одной из учетных записей;

– Рекомендуется ограничить физический и удаленный доступ к серверам баз данных и 1С предприятия;

– Рекомендуется использовать шифрование для баз данных, это позволит сохранить конфиденциальные данные, даже если злоумышленник получит физический доступ к файлам СУБД;

– Также одним из важных решений является шифрование либо установка пароля на резервные копии данных;

– Обязательным является создание администраторов кластера 1С, а также сервера 1С, так как по умолчанию если не созданы пользователи, полный доступ к информационным базам абсолютно все пользователи системы.

3. **Требования к обеспечению физической безопасности серверного оборудования *(согласно ГОСТ Р ИСО/МЭК ТО – 13335)*:**

– Доступ к зонам, где обрабатывается или хранится важная информация, должен управляться и быть ограничен только полномочными лицами;

– Средства управления аутентификацией, например, карточка управления доступом плюс персональный идентификационный номер **[PIN]**, должны использоваться, чтобы разрешать и подтверждать любой доступ;

– Контрольный журнал всего доступа должен содержаться в надежном месте;

– Персоналу вспомогательных служб третьей стороны должен быть предоставлен ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется;

– тот доступ должен быть разрешен и должен постоянно контролироваться;

– Права доступа в зоны безопасности должны регулярно анализироваться и обновляться, и отменяться, если необходимо;

– Должны быть учтены соответствующие нормы и стандарты по технике безопасности и охране труда;

– Ключевые средства должны быть расположены так, чтобы избежать доступа к ним широкой публики;

– Там, где это применимо, здания и комнаты должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;

– Указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.

4. **Конфиденциальность персональных данных.** Основной целью при организации защиты персональных данных является нейтрализация актуальных угроз в информационной системе, определенных ***Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»***, перечнем государственных стандартов и требований международных сертификаций по ИТ-безопасности ***(ГОСТ Р ИСО/МЭК 13335 2-5, ISO 27001)***. Достигается это путем ограничения доступа к информации по ее типам, разграничение доступа к информации по ролям пользователей, структурирование процесса обработки и хранения информации.

Вот ряд ключевых положений:

– Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

– Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным;

– Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– Обработке подлежат только персональные данные, которые отвечают целям их обработки;

– Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

– Фотографическое, видео, аудио или другое записывающее оборудование, такое как камеры на мобильных устройствах, не должны допускаться, если только не разрешено;

– Накопители со сменным носителем должны быть разрешены только в том случае, если для этого есть производственная необходимость;

– Чтобы исключить злонамеренные действия в отношении конфиденциальной информации, требуется бумажные и электронные носители информации, когда они не используются, хранить в надлежащих запирающихся шкафах и/или в других защищенных предметах мебели, особенно в нерабочее время;

– Носители с важной или критичной служебной информацией, когда они не требуются, следует убирать и запирать (например, в несгораемом сейфе или шкафу), особенно когда помещение пустует.

5. **Сетевая безопасность** - это набор требований, предъявляемых к инфраструктуре компьютерной сети предприятии и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа. В рамках рекомендуемых действий по организации и обеспечению сетевой безопасности, помимо базовых, можно рассмотреть следующие особенности:

– В первую очередь, в компании должен быть внедрен единый регламент информационной безопасности с соответствующими инструкциями;

– Пользователям должен быть максимально закрыт доступ к нежелательным сайтам, в том числе файлообменникам;

– Из внешней сети должны быть открыты только те порты, которые необходимы для корректной работы пользователей;

– Должна присутствовать система комплексного мониторинга действий пользователей и оперативного оповещения нарушения нормального состояния всех общедоступных ресурсов, работа которых важна для Компании;

– Наличие централизованной антивирусной системы и политик очистки и удаления вредоносных программ;

– Наличие централизованной системы управления и обновления антивирусным ПО, а также политик регулярных обновлений ОС;

– Возможность запуска съемных флэш носителей должна быть максимально ограничена;

– Пароль должен быть не менее 8 символов, содержать цифры, а также буквы верхнего и нижнего регистров;

– Должна быть защита и шифрование ключевых папок обмена информацией, в частности файлов обмена 1с и системы клиент-банк;

– Силовые линии и линии дальней связи, входящие в средства обработки информации, должны быть подземными там, где это возможно, или должны подлежать адекватной альтернативной защите;

– Сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны.

Подведя итог всего вышеизложенного хотелось бы отметить, что основными правилами при защите информации является ограничение прав и возможностей пользователей, а также контроль над ними при использовании информационных систем. Чем меньше пользователь имеет прав при работе с информационной системой, тем меньше шанс утечки или порчи информации по злому умыслу или по неосторожности.

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чижов А.С., студент
Научный руководитель: ст. преподаватель Павлова В.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Одним из аспектов обеспечения информационной безопасности является антивирусная защита. В этой статье рассмотрим некоторые общие формы таких вредоносных программ, их устройство, методы распространения и борьбы с ними.

Троянские кони

Родоначальником вирусов считается троян, который использует технологию: создать действительно полезную программу и встроить в нее вредоносный модуль. Это могут быть игры, специализированное программное обеспечение просмотра «взрослого» контента с привлекательной графикой и др. Когда бесплатная программа запускается, она вызывает функцию записи ее на диск, затем функцию, запускающую программу на выполнение. После запуска она выполняет свои инструкции, например, поиск, удаление, модификация файлов, их шифрование; может заниматься поиском номеров кредитных карт, паролей, других подобных сведений; может подключиться к ip-порту и будет ждать команд для передачи найденной информации по мэлу через интернет или другим способом. «Прелесть» троянского коня в том, что пользователю не надо взламывать ПК: с помощью внедренной программы ПК жертвы становится зомби, выполняющего команды хозяина.

В настоящее время интенсивно внедряются, так называемые, **программы - вымогатели.**

Программы-вымогатели бывают двух видов: шифровальщики; блокировщики.

Шифровальщики зашифровывают данные и требуют выкуп, взамен обещая восстановить данные.

Блокировщики блокируют доступ к устройству пользователя, на котором эти данные хранятся, и требуют выкуп, взамен обещая восстановить данные.

Программы-вымогатели маскируются под сообщения от правоохранительных органов, от налоговой инспекции и т.п.

Наиболее распространены программы-вымогатели Cerber и Locky.

Locky (по данным к. Касперского) распространился в 114 странах мира.

Несильно от них отстали вымогатели CryptXXX, CTB-Locker, CryptoWall.

По данным к. Касперского[1] в 2016 году количество модификаций программ-вымогателей выросло в 11 раз; атаки на компании осуществляются каждые 40 сек; усилилась интенсивность атак на обычного пользователя; каждая пятая компания, заплатив выкуп, так и не получила данные… Прогноз: программы-вымогатели становятся все более притягательными, привлекая менее квалифицированные слое киберпреступников… Мы ожидаем появления программ-вымогателей, созданных так называемыми «скрипт-кидди» (начинающими хакерами), которые будут блокировать файлы или доступ к системе, или удалять файлы, обманным путем заставляя жертв платить, но при этом не возвращая им доступ к файлам.

Пару лет назад Волжский университет столкнулся с программой-вымогателем следующим образом: было открыто электронное сообщение от налоговой инспекции. Была закодирована БД, содержащая персональную информацию. Получено требование заплатить выкуп в размере 10 тыс. руб.

Другие вирусы

Помимо троянских коней существует огромное количество разновидностей вирусов:

вирусы-компаньоны (запускается, когда запускается определенная программа);

вирусы, заражающие исполняемые файлы (прикрепляются к началу/концу кода, переписывают своим кодом код программы и пр.);

резидентные вирусы (резидентно находится в оперативной памяти, прячется в самых верхних адресах памяти или прячется «в траве» - в таблице прерываний и др.);

вирусы, поражающие загрузочный сектор (переписывают загрузочный сектор, содержащий программу с информацией об активном разделе диска, нанося огромные проблемы системе);

вирусы драйверов устройств (зараженные драйверы – чаще исполняемые программы - могут загружаться при загрузке системы и … Если зараженный драйвер работает в режиме ядра, то он может проникнуть, например, в таблицу векторов прерываний и …);

макровирусы (макросы к документам Word, Excel, могут содержать вредоносные программы; с ростом количества почтовых вложений отправка вложений с вирусами, встроенными в макросы, превратилась в серьезную проблему;

вирусы, заражающие исходные тексты программ (поиск программ, например, на языке С, включение вредоносного кода в текст программы, например, перед оператором return; при выполнении зараженной программы будут выполняться вредоносные инструкции).

Черви

Широкомасштабное посягательство на информационную безопасность произошло 2 ноября 1998 года. Аспирант Моррис Корнельского университета написал программу – червь, который распространился через Интернет и заразил несколько тысяч ПК.

Моррис был блестящим аспирантом, нашел «дыры» для несанкционированного входа на ПК через Интернет, написал саморазмножающуюся программу. Его шалость вышла из-под контроля. Он был наказан. Его осудили на 3 года (условно) и назначили штраф 10000 долларов.

Программы-шпионы. Шпионы – программы, которые тайно, без ведома владельца ПК (например, посредством троянских коней), загружаются на его машину, запускаются в фоновом режиме, производят: изменение домашней страницы браузера; добавление к браузеру панелей, значков, размещение рекламы, запуск которой генерирует другую рекламу и пр.

Антивирусные технологии

Антивирусы, исходя из реализованного подхода к выявлению или уничтожению вирусов, принято разделять на следующие категории: фаги; детекторы; прививки; вакцины; мониторы.

Фаги находят зараженные файлы в системе, а затем лечат их, то есть удаляют тела вирусов.

Детекторы гарантируют обнаружение вирусов с помощью просмотра выполняемых файлов и поиска так называемых сигнатур - устойчивых последовательностей байтов, существующих в телах популярных вирусов. Наличие сигнатуры в каком-либо файле может говорить о его заражении.

Прививки действуют по принципу самих вирусов, то есть зараженные файлы или программы помечаются для исключения «повторного заражения».

Вакцины предотвращают заражение файлов. Вакцинация модифицирует файл, возможна только, если вирус считается известным. В этом случае вирус считает, что он уже заразил программу, таким образом осуществляется предотвращение заражения файла.

Мониторы обеспечивают защиту системы, перехватывая вредоносное программное обеспечение.

[1] kaspersky.ru

Итак, как только антивирусная программа установлена на машине, она, прежде всего, сканирует на диске каждый исполняемый файл в поиске вирусов, известных ее базе данных. Кроме того, действием, выполняемым антивирусной программой, является запись на диск длины всех файлов и последующий анализ этих данных. Если файл стал длиннее, он может быть заражен. Но хорошо продуманный вирус может избежать увеличения длины файла за счет сжатия данных. Программы проверки целостности файлов вычисляют контрольную сумму для каждого исполнимого файла, проводят соответствующий анализ. Существует огромное количество механизмов, которые используются на практике для выявления, уничтожения вирусов, предотвращения заражения.

Вывод. В Интернете полно вредоносных программ, в число которых входят троянские кони, вирусы, черви и прочее. Каждая из этих программ представляет угрозу конфиденциальности, целостности данных.

Существует ряд способов самозащиты системы. Лучшей стратегией является глубокая эшелонированная, комплексная система защита, компонентом которой является антивирусная защита. Не стоит пренебрегать антивирусами, обновлять их, следует следить за чистотой компьютера и чистить диски от всякого мусора, использовать лицензионное программное обеспечение.

Библиографический список

1. Аджиев, В. "Мифы о безопасном ПО: уроки знаменитых катастроф" // Открытые системы [Электронный ресурс] [Проверено: 26.04.2014].
2. Олифер, В.Г., Олифер, Н.А. Сетевые операционные системы. - СПб.: Питер. -2008. -544с.
3. Таненбаум, Э. Современные операционные системы. 3 изд. - СПб.: Питер. -2011. -1120с.
4. kaspercky.ru - о вредоносном программном обеспечении.

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шемотюк С.Н., студент
Научный руководитель: к. т. н., доцент Куралесова Н.О.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Когда говорят про тему «Анализ угроз информационной безопасности», то под этим подразумевают любую угрозу, которая может нанести ущерб информационной системе, в зачастую упоминают три класса угрозы:

1) Доступности информации;
2) Целостности информации;
3) Конфиденциальности информации.

Рассмотрим для начала самые часто появляющиеся угрозы доступности. Случайные ошибки являются самыми вредными из всех для всех лиц связанные с информационной системой. Зачастую такими ошибками могут воспользоваться правонарушители, потому что в системе появляются уязвимые места. Самый практичный способ противостоять таким случайным ошибкам является автоматизация процесса и строгий контроль.

Существуют еще угрозы «отказа», они не приятны больше всего для пользователя информационной системы тем, что получают отказ в обслуживании, и штатному пользователю не понятно в чем причина, это может быть внутренним отказом информационной системы, или отказ поддержки инфраструктуры. Сам пользователь может рассматриваться, как угроза, нежеланием работать с новой информационной системой, или невозможность работать с системой из-за отсутствия нужной подготовки, или отсутствие технической поддержки, или могут быть Distributed-Denial-of-Service (DDoS-атака).

Внутренними отказами системы являются случайные или специальные отступления, неправильный выход из системы, а также преднамеренное разрушение данных или аппаратуры. Отказ поддержки инфраструктуры чаще всего случаются из-за стихийных бедствий – пожары, наводнения, землетрясения, ураганы, и грозы.

Не только пользователь или администратор сети может нанести ущерб, но и правонарушители, они создают вредоносные программы и вирусы и троянские программы, которые очень сильно могут повредить систему. По данным Intel вирус WannaCry заразил более 530 тысяч ПК.

Главными угрозами целостности являются непреднамеренные ошибки, зафиксированные неверные данные, которые могут нанести большой вред любой компании. С этой угрозой фальсифика-

цией борются методами подтверждения подлинности документов и поисками сравнений данных во всей системе.

Основные угрозы конфиденциальности это служебная информация. К служебной информации приписывают «login» и пароли пользователей. Штатный пользователь, который в своей работе использует несколько информационными системами, под разными именами и паролями, чаще всего записывают всю информацию в телефон или на бумаге. Информация, которая находиться не в безопасности пользователь может потерять, или забыть на своем рабочем месте, этим может воспользоваться злоумышленник, который не имеет навыков взлома.

Существует еще угроза перехвата данных, эта угроза опасна тем, что за ней стоит зачастую опытный злоумышленник. Защита каналов передачи информации может оказаться очень сложной и дорогостоящей. Защита сложна тем, что относиться к внешним угрозам и к внутренним. Потеря и похищение оборудования также являются угрозой. Существует еще практика злоупотребление полномочиями, администратор системы может прочитать и воспользоваться любым файлом, или сервисный рабочий имеет доступ ко всему оборудованию и ко всем защитным механизмов.

Само слово «угроза» является одним из важных тезисов в сфере информационной безопасности. К самым важным свойствам угрозы относят избирательность, предсказуемость и наносимый ущерб. Избирательность означает, что источник угрозы нацелен на важные для них места в информационной системе. Предсказуемость означает присутствие признаков возможного появления угрозы, с помощью предсказывания можно определить следующий удар угрозы.

Есть два типа угроз:

1. Замысел нанесения вреда, который выражается угрозами;
2. Нанесение вреда.

Особенность замысла нанесения вреда наличие неопределенности вероятных последствий, и не точной информации о средствах для реализации угроз. Угроза вреда, как и сам вред, несет только опасность сохранения информационной системы в безопасности.

Злоумышленники реализуют свои угрозы разными способами: получением информации о программно-аппаратной среде и средств вычислительной технике, получением данных о системах защиты, хищение или копирование информации, которые несут конфиденциальные данные, уничтожение вычислительной техники, заражение программными вирусами, и другие действия, которые будут причинять вред злоумышленники в своих корыстных целях.

Для защиты информационной безопасности создают различные программы, которые разделяются на два типа: проактивные и реактивные.

В основе проактивной защиты лежит идея эффективного контролирования всех спектров активности на ПК и предотвращения внутренние угрозы информационной безопасности.

Реактивный подход характеризуется «пассивностью» в отличии от проактивной, в реактивном подходе лежит принцип реагирования на угрозу, инцидент или попытку вторжения, такую технологию можно назвать «принципом черных списков». Именно так работают антивирусы, первые атаки изучаются и добавляются в черный список, в следующих случаях такие атаки будут остановлены.

Угроза безопасности всегда будет актуальной темой, потому что прогресс не стоит на месте, и с каждым годом появляются новые технологии, а с ними и новые угрозы. Для этого и выделяются большие бюджеты во всех крупных компаниях, чтобы изучить угрозу, и защититься от нее, прежде чем она появиться.

Библиографический список

1. Cyberpedia.su 2017. [Электронный ресурс] – Режим доступа: «https://cyberpedia.su/ 6x9949.htm».
2. Информационная безопасность. [Электронный ресурс] – Режим доступа: «https://informationsecurityweb. wordpress.com/2016/05/27».
3. Безопасник 2010-2017. [Электронный ресурс] – Режим доступа: «http://bezopasnik.org /article/21.htm».

ВЛИЯНИЕ КОМПЛЕКСООБРАЗОВАТЕЛЯ НА ХАРАКТЕРИСТИКИ ЭЛЕКТРОДОВ, ИЗГОТОВЛЕННЫХ ИЗ ГИДРОКСИДА НИКЕЛЯ, ПОЛУЧЕННОГО ИЗ ГАЛЬВАНОШЛАМА

*Бабиченко Е.Д., студент**
Научный руководитель: к. х. н., доцент Лазарева Е.Н., д. х. н., профессор Ольшанская Л.Н.**, к. т. н. Егоров В.Н.**
**ФГБОУ ВО «Энгельсский технологический институт (филиал) Саратовского ГТУ им. Гагарина Ю.А.»*
***ФГБОУ ВО «Саратовский государственный технический университет им. Гагарина Ю.А.»*
г. Энгельс, Россия

В настоящее время все без исключения предприятия оказывают негативное воздействие на состояние окружающей природной среды. Особенно это касается химической отрасли, а тем более гальванических цехов и участков. Опасность обусловлена не только воздействием растворов и сточных вод, но и накоплением большого количества гальванических шламов (ГШ), содержащих такие токсичные компоненты, как никель, цинк, железо, медь, хром, свинец, кадмий и др. [1].

При нахождении эффективной технологии утилизации эти компоненты могут стать источником необходимых производствам металлов и материалов. Оптимальной является утилизация ГШ, проводимая последовательно в две стадии:

1 - избирательное извлечение тяжелых металлов путем химического выщелачивание металлов из осадков, селективного осаждения соединений металлов при различных значениях кислотности растворов [2], электрохимического извлечения [3,4], а так же взаимодействием с комплексообразователями [5]. В дальнейшем извлеченные компоненты можно применять при изготовлении металлов и сплавов, пигментов-наполнителей, аккумуляторов, стеклоизделий, глазурей, иммобилизировать в полимерную матрицу, а так же использовать для изготовления полиоксидных катализаторов [6], никель-кадмиевых (Ni-Cd) и никель-железных (Ni-Fe) аккумуляторов [7].

На 2 стадии осуществляется утилизация пустых шламов при изготовлении, строительных материалов, дорожных покрытий, новых композиционных материалов.

Данная технология переработки ГШ позволяет получить необходимое производству сырье и снизить класс опасности образующихся отходов. Таким образом, нахождение оптимального способа утилизации гальваношламов с получением полезных компонентов, а так же изучение оптимальных условий их проведения, является актуальной и своевременной задачей.

Целью данной работе было проведение поэтапного извлечения ионов никеля и $\mathbf{Ni(OH)_2}$ из раствора гальваношлама в присутствии комплексообразователя пирокатехина, а так же и**зучение циклических характеристик электродов изготовленных** на основе полученного гидроксида никеля**.**

Экспериментальные данные и их обсуждение

Объектом исследований явился ГШ, образующийся после ванн никелирования и активации имеющий состав, приведенный в таблице 1.

Таблица 1 – Состав гальваношлама после ванн никелирования и активации

Состав ГШ	Ионы никеля	Ионы железа,	Ионы цинка	Ионы меди	Сульфат – ионы
Содержание, %	44	0,67	0,58	0,003	6,4

Предварительная обработка ГШ заключалась в разведении его водой. Полученная суспензия характеризовалась кислотностью со значением pH = 8,7.

Как было показано в работе [5] для проведения селективного извлечения ионов никеля из шламов в качестве комплексообразователя можно использовать пирокатехин ($C_6H_4(OH)_2$). Нами были проведено извлечение ионов никеля при добавке пирокатехина в количестве от 0 до 250 г/л. При этом кислотность растворов ГШ изменялась в диапазоне от 8,7 (без добавок) до 5,43(250 г/л).

Полученные вытяжки исследовались фотоколориметрическим методом. На оснвоании полученных данных бела определена концентрация ионов никеля в растворах. Результаты измерения оптической плотности растворов, приготовленных на основе ГШ при различных добавках пирокатехина, и концентрации ионов никеля в растворах приведены в таблице 2.

Таким образом, установлено, что повышение добавок пирокатехина от 50 до 250 мг/мл приводит к увеличению концентрации ионов никеля в растворе от 12,4 до 18,2 мг/мл.

Все металлы различаются своими строго индивидуальными значениями pH, при которых они выпадают из растворов в виде нерастворимых в воде гидроксидов. Для осаждения гидроксида никеля

из растворов ГШ с различными добавками ПК проводили их щелочную обработку, в результате которой произошло осаждение $Ni(OH)_2$.

Таблица 2 - Изменение концентрации ионов никеля в растворе при различных добавках пирокатехина

Концентрация пирокатехина, г/л	50	100	150	200	250
Оптическая плотность, А	1,870	1,964	2,125	2,439	2,789
Концентрация $Ni^{2+} \cdot 10^3$, мг/мл	12,4	13,2	14,2	16,1	18,2

Состав выделенного гидроксида никеля определяли согласно ТУ 48-3-63-90 «Гидрат закиси никеля»: содержание Ni определяют комплексонометрическим (ГОСТ 4465-74 «Комплексонометрический метод анализа») и титрометрическим (с трилоном Б) методами; содержание Fe определяют атомно-адсорбционным методом (с использованием спектрометра). Полученные результаты анализа состава приведены в таблице 3.

На основании полученных данных было установлено, что наибольшее количество ионов никеля (29,9%) присутствует в **$Ni(OH)_2$**, полученном при концентрации пирокатехина 50г/л. Поэтому именно эта добавка (Спк=50 г/л) выбрана нами для изготовления катодов. Состав активной массы (АМ) катодов аккумуляторных батарей приведен в таблице 4.

Таблица 3 – Состав гидроксида, полученного из ГШ с различным содержанием пирокатехина

$C_{пк}$, г/л	Определяемый ингредиент, %		
	Ni	Fe	Mg
0	0,4	0,	0,00
50	29,9	8,3	0,04
100	24,6	6,9	0,03
150	23,1	6,2	0,03
200	18,9	5,2	0,02
250	18,7	5,1	0,02

Таблица 4 – Состав активной массы для изготовления катода на основе $Ni(OH)_2$

Вещество	$Ni(OH)_2$	$CoSO_4$	Графит	$Ba(OH)_2$	KOH
Количество, %	34,4	2,4	18,4	2,6	9,1

Изучение циклических характеристик изготовленных электродов проводилось при постоянном токе в трехэлектродной ячейке с разделенным фильтрами Шотта катодным и анодным пространствами, что позволяет предотвратить смешение продуктов реакции. В качестве рабочих электродов использовали изготовленные нами электроды, в качестве вспомогательных электродов – сталь, в качестве электрода сравнения – хлор-серебряный электрод (ХСЭС). **Рабочим электролитом является щелочной раствор КОН+10 г/л LiOH (плотность 1,19-1,21 г/см^3).**

Заряд электродов (то есть его формирование) проводили гальваностатическим методом (при i=const). Разряд сформированных электродов осуществляли в диапазоне i=40÷120 мА/см^2 (шаг 20 мА/см^2) до начала спада потенциала на кривой (рис. 1а). На основании полученных данных был построен графики зависимости емкости сформированных электрода от времени разряда (рис. 1б).

На основании анализа полученной зависимости было предложено проводить разряд при i=80 мА/см^2, так как при этих условиях достигается наибольшая отдаваемая емкость, а при большей плотности тока наблюдаются скачкообразные изменения величины потенциала, свидетельствующие о неустойчивом состоянии и возникновении дополнительных изменений структуры.

Полученные результаты были использованы для оценки обратимости электродов, ресурса их работы при циклировании, для определения величин отдаваемой электродами при разряде емкости, а так же расчета удельных разрядных характеристик (удельной емкости, энергии др.).

Таким образом, проведенные исследования подтвердили возможность использования пирокатехина для проведения селективного извлечения ионов никеля из отходов ГШ и изготовления на его основе активной массы катодов аккумуляторных батарей.

Выбраны оптимальные условия проведения извлечения гидроксидов никеля из ГШ (Спк=50г/л) и проведения разряда изготовленных на его основе электродов (при i=80 мА/см).

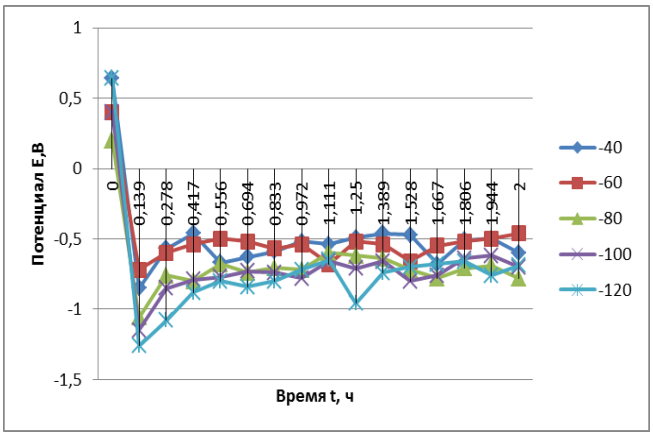

Рисунок 1 – Зависимости E,t (а) и Q-t (б) полученные для электрода, изготовленного из **$Ni(OH)_2$** полученного при добавке $C_{пк}$=50 г/л при i=40÷120 мА/см^2

Библиографический список

1. Рубанов, Ю.К. Утилизация отходов гальванического производства / Ю.К. Рубанов, Ю.Е Токач // Экология и промышленность России. - 2010. – №10. - С.2-3.

2. Исследование выщелачиваемости ионов тяжелых металлов из ферритизированных шламов гальванического производства / А.В. Пинаев, В.В. Семенов, В.В. Савиных, Е.С. Климов // Экология и промышленность России. – 2006. – №8. – С.24-25.

3. Хранилов, Ю.П. Использование электрохимических технологий при переработке отходов гальванических производств с целью их утилизации / Ю.П. Хранилов, Т.В. Еремеева, М.Н. Бобров // Актуальные проблемы электрохимической технологии. Сб. статей молодых ученых. Т.1. – Саратов: ГАОУ ДПО «СарИПКиПРО», 2011. – С.240-244.

4. Извлечение металлического никеля из никельсодержащего гальваношлама ОАО «Роберт-Бош-Саратов» / Л.Н. Ольшанская, Е.Н. Лазарева, В.В. Егоров, Т.М. Цечоев // Экологические проблемы промышленных городов: материалы Всероссийской конф. Саратов 4-6 апреля 2009 г. Часть 1. Саратов: СГТУ, 2009. – С.298-302.

5. Завальцева, О.А. Комплексоны для извлечения ионов тяжелых металлов из гальваношламов // Экология и промышленность России.– 2010. – №2. – С.36-38.

6. Терещенко, А.Д. Катализаторы, полученные на основе отходов гальванических производств / А.Д. Терещенко, И.А. Фарафонова, А.С. Таратуто // Экотехнология и ресурсосбережение. – 1999. – №3. – С.86-90.

7. Ольшанская, Л.Н. Утилизация тяжелых металлов и их соединений из гальваношламов с получением пигментов-наполнителей и активной массы положительных электродов никель-железных (кадмиевых) аккумуляторов / Л.Н. Ольшанская, Е.Н. Лазарева, Л.А. Булкина // Химическое и нефтегазовое машиностроение . - 2016. - № 2. - С. 42-45.

ВОЗДЕЙСТВИЕ УФ – ОБЛУЧЕНИЯ НА ИЗВЛЕЧЕНИЕ ХРОМА (III) ИЗ ПОЧВЫ С ИСПОЛЬЗОВАНИЕМ ВЫСШЕГО РАСТЕНИЯ - СОИ

Баканова Е.М., магистрант
Научный руководитель: д. х. н., профессор Ольшанская Л.Н.
ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.»
г. Саратов, Россия

Почва является основной средой, в которую попадают тяжёлые металлы (ТМ), нефть и другие поллютанты из атмосферы и водной среды. Из почвы ТМ усваиваются растениями (фито). В фиторемедиационных технологиях, особенно в процессах очистки биосферных комплексов от ионов тяжелых металлов огромную роль играет растительная клетка, которая выступает в качестве биоэлектрохимического сенсора-реактора, распознающего и извлекающего катионы металлов из сточных, промывных вод и почв [1]. На эти процессы оказывают воздействие внешние физические поля (ВФП: постоянные магнитные (ПМП), электрические поля, ультрафиолетовое (УФ), инфракрасное (ИК) и лазерное излучения (ЛИ) и их комбинированное сочетание), которые создают дополнительные электрические токи в биообъектах, и могут изменять течение процессов роста и развития организмов [2], оказывая как стимулирующее, так и тормозящее влияние. Применение ВФП для обработки семян

растений является прогрессивным способом их подготовки к посеву, позволяющим не только вывести семена из состояния покоя, но и активизировать работу разнообразных биологических катализаторов - ферментов, обеспечивающих быстрый рост и развитие растений [3].

Нами исследованы процессы роста и развития высших растений сои и фасоли в процессе очистки почв от ионов хрома (lll) методом фиторемедиации при воздействии на семена сои УФ- излучением.

Выбор - сои (*Glycinemax*) сорт Самер 2 обусловлен тем, что в целях фиторемедиации обычно используют высокопродуктивные культуры. Загрязняющими веществами служили модельные растворы сульфата хрома $Cr_2(SO_4)_3$, которые содержали 1, 5 и 10 ПДК (*ПДК общесанитарный для Cr^{3+} 6 мг/кг почвы)* За систему отсчета концентрации катионов в почве в соответствии с литературными данными [4] была принята величина ПДК, а не количество элемента в мг/кг почвы. Это сделано из соображения, что разные металлы содержатся в почве в различных несопоставимых, если их выражать в мг, количествах, различающихся зачастую на два порядка, и, кроме того, они обладают различной степенью токсичности. Такой подход позволил сопоставить силу воздействия различных ИТМ между собой. Брали подвижную форму металла в почве [5].

В качестве источника УФ-излучения выступала бактерицидная лампа, марки СБПе 3х30 Вт, с длиной волны λ=257 нм. Обработку семян проводили при выбранном времени в течение 6 часов [6].

Проведенные исследования по влиянию природы и концентрации ионов Cr^{3+} на высоту растений и развитие листовых пластин сои (таблица 1) показали, что по истечении 14 - 21 суток у растений сои не проявлялись значительные признаки угнетения роста и отмирания листьев. На 28 день эти процессы начали проявляться, и они усилились с увеличением концентрации токсикантов. Растения уменьшились по высоте, выглядели увядшими, поникшими, проявились признаки плазмолиза и некроза.

Таблица 1 - Влияние концентрации ионов Cr^{3+} и УФ – облучения на рост и развитие сои

Высота растения, мм.					Длина листа, мм. УФ				Ширина листа, мм.УФ			
Дни	К*	1 ПДК	5 ПДК	10 ПДК	К*	1 ПДК	5 ПДК	10 ПДК	К*	1 ПДК	5 ПДК	10 ПДК
7	80	30	0	10	0	0	0	0	0	0	0	0
14	220	50	32	33	30	10	0	0	25	10	7	5
21	280	184	120	80	40	20	10	0	30	20	14	11
28	290	210	172	100	35	25	20	0	25	23	15	9

Примечание: К-контроль без УФ и ТМ.*

Худшие ростовые показатели растения проявили при концентрации иона Cr^{3+}равной 5 ПДК и УФ.

Авторами [7] установлено, что даже незначительные количества трехвалентного хрома стимулируют рост растений и образование клубеньков у бобовых растений, что объясняется строением атома хрома, его близостью по положению в периодической системе элементов к марганцу и молибдену, физиологическая активность которых общеизвестна.

Фиторемедиационная способность растений сои по отношению к хрому

Через 28 дней после внесения Cr^{3+} в почву растения сои были извлечены из почвы, высушены и взвешены. Отделяли корневую часть растений, так как по ранее проведенным гистохимическим исследованиям, накопление металлов происходило в основном в корнях растений-исключателей, к которым относятся фасоль и соя [8].

Определение остаточных концентраций ионов Cr^{3+} в почве проводили на спектрофотометре Промэколаб ПЭ 5300 В по ГОСТ 17.4.3.01-83 «Охрана природы почвы общие требования к отбору проб».

Результаты по величинам адсорбционной емкости и эффективности очистки ($Э= \{(c_{нач.}-c_{кон})/c_{нач.}\}\cdot 100$ %} почв от ионов хрома растениями – фитомелиорантами, семена которых были обработаны УФ -излучениями представлены в таблице 2.

Установлено, что лучшую эффективность очистки почв от ионов хрома показали растения сои при применении предварительной обработки семян УФ-облучением. При этом следует отметить, что при низких концентрациях Cr^{3+} (1 ПДК) эффективность очистки почв растениями сои снижалась, лучшая эффективность очистки (95,7 %) достигнута при концентрации хрома 10 ПДК.

Таблица 2 - Влияние концентрации ионов Cr^{3+} без и при воздействиях УФ – облучений на эффективность (Э, %) очистки почвы соей и адсорбционную емкость растения (A_i, мкг/кг) после 28 дней выдержки

Э, %				A_i, мкг/кг		
Концентрация Cr^{3+}	1 ПДК	5 ПДК	10 ПДК	1 ПДК	5 ПДК	10 ПДК
Без ВФП	68,4	91,3	93,3	70,1	81,6	116,4
УФ	69,2	93,5	95,7	80,7	98,5	125,3

Адсорбционную емкость растений сои по отношению к хрому устанавливали по количеству поглощенного ими металла после сушки и мокрого озоления фитомассы (мкг/кг в расчете на абсолютно сухой вес массы растений). Наиболее высокая величина адсорбционной емкости A_i для сои достигнута после УФ-облучении при 10 ПДК Cr^{3+}.

Известно, что нормальное содержание хрома в растениях равняется 0,1–0,5 мг/кг сухой массы и предположительно максимальное – 2 мг/кг сухой массы. ПДК хрома для растений составляет от 0,1 до 2,0 мг/кг сухой массы [20]. Согласно данным критическая концентрация металла, выше которой нарастание надземной массы растений снижается на 10 %, варьирует от 1,0 до 2,0 мг/кг сухой массы, а фитотоксическая концентрация хрома (снижение надземной фитомассы на 50 %) равна 100 мг/кг сухой массы [9].

В растениях семейства бобовых (горох, фасоль) обнаружено более высокое содержание хрома по сравнению с зерновыми культурами [10].

Выводы

1. Изучено влияние содержания хрома (III) на процессы роста и развития сои и фиторемедиацию ими почвы. Установлено, что с увеличением концентрации Cr^{3+} в почве, сильнее проявляется их токсическое действие на растения-фиторемедианты.

2. Установлено, что эффективность очистки почв загрязненных ионами Cr^{3+}, составила 93 – 98% и ее величина увеличивалась с ростом концентрации металла. Это обусловлено тем, что хром является микроэлементом, необходимым для роста и развития растений, и его концентрация в фитомассе контролируется.

3. Определена адсорбционная емкость растений сои по отношению к хрому. Обнаружена интересная зависимость, при увеличении концентрации металла A_i увеличивалась и составила для сои 80 ÷ 126 мкг/кг сухой фитомассы после обработки семян УФ- излучением.

Библиографический список

1. Ольшанская, Л.Н., Титоренко, О.В., Халиева, А.С. Влияние постоянного магнитного поля и ультрафиолетового излучения на процессы роста высших наземных растений и фиторемедиацию ими почв от тяжелых металлов и нефтепродуктов: монография.- Саратов: СГТУ имени Гагарина Ю.А., 2015. 124 с. (7,75 печ. л.) ISBN 978-5-7433-2864-2.

2. Савельев, В.А. Сибирский вестник науки. 1981. №5. С. 26 – 29.

3. Алтухов, И.В., Федотов, В.А., Очиров, В.Д. Изменение основных качественных показателей семян пшеницы после воздействия различными облучателями.- Иркутск: Вестник ИрГСХА. 2010. Вып. 40. С. 107-115.

4. Руководство по санитарно-химическому исследованию почвы. - М.: ГК СЭНР РРИАЦ, 1993.- С. 35.

5. ГН 2.1.7.2041-06 «Предельно допустимые концентрации (ПДК) химических веществ в почве». М.: Изд-во стандартов, 2006. 8 с. http://www.opengost.ru.

6. Ольшанская, Л.Н., Титоренко, О.В., Еремеева, Ю.А. // Химическое и нефтегазовое машиностроение. 2015. № 5. С. 43-45.

7. Алексеев, Ю.В. Тяжелые металлы в почве и растениях.– Л.: Агропромиздат, 1987. – 142 с.

8. Ольшанская, Л.Н., Халиева, А.С., Титоренко, О.В. // Известия высших учебных заведений. Химия и химическая технология. 2015, Т. 58, выпуск 6. С. 89 - 94.

9. Vazquez, M.D., Poschenrieder, C.H., Barcelo, J. // Ant. Bot. (USA), 1987. Vol. 59, № 4. P. 427–438.

10.Schroeder, H.A. Balassa, J.J., Tipton, I.M. // J. Chron. Dis. 1967. № 20. P. 147-151.

САНИТАРНО-МИКРОБИОЛОГИЧЕСКИЕ ИССЛЕДОВАНИЯ ПИЩЕВЫХ ПРОДУКТОВ

Гордукова А.А., студент
Научный руководитель: к. п. н., доцент Богатова И.Б.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Обеспечение безопасности продуктов питания имеет особое значение для жизни и здоровья людей. В последнее время проблема безопасности пищевых продуктов становится все актуальнее. Санитарные нормы и правила характеризуют безопасность пищевой продукции, как отсутствие опасности для жизни и здоровья людей нынешнего и будущих поколений, определяемое соответствием пищевой продукции требованиям санитарных правил, норм и гигиенических нормативов.

В настоящее время непрерывно расширяется ассортимент пищевых продуктов, изменяется характер питания. В производство, хранение и распределение продуктов питания внедряются новые технологические процессы, применяются все возрастающие количества различных химических соединений и т. п. Опасность с точки зрения попадания токсических веществ в пищевые продукты представляет загрязнение окружающей среды промышленными отходами, а также расширение использования химикатов в сельском хозяйстве.

Через пищевые продукты могут передаваться возбудители многих инфекционных болезней. Обсеменение их микробами может происходить на всех этапах заготовки, хранения и приготовления. Пищевые продукты обычно невозможно полностью освободить от присутствия микроорганизмов без риска изменения их вкусовых качеств. Таким образом, микробиологическое исследование пищевых продуктов являются важнейшей проблемой.

Целью настоящей работы является определение микрофлоры в пищевых продуктах.

Работа проводилась на базе центра гигиены и эпидемиологии г. Тольятти.

Отбор проб пищевых продуктов проводили в соответствии с ГОСТ 26668-85 (СТ СЭВ 3013-81) Продукты пищевые и вкусовые. Методы отбора проб для микробиологических анализов.

Подготовку проб пищевых продуктов к исследованию проводили в соответствие с ГОСТ 26669-85 (СТ СЭВ 3014-81) «Продукты пищевые и вкусовые. Подготовка проб для микробиологических анализов»; ГОСТ 8756.18-70 «Продукты пищевые консервированные. Методы определения внешнего вида, герметичности тары и состояния внутренней поверхности металлической тары».

Определение количества мезофильных аэробных и факультативно-анаэробных микроорганизмов (КМАФАнМ) проводили в соответствии с ГОСТ 10444.15-94 «Методы определения количества мезофильных аэробных и факультативно-анаэробных микроорганизмов».

Метод определения количества мезофильных аэробных и факультативно-анаэробных микроорганизмов посевом в агаризованные питательные среды основан на высеве продукта или разведения навески продукта в питательную среду, инкубировании посевов, подсчете всех выросших видимых колоний.

Проведение испытаний:

1) По 1 см³ из разведения (выбирают 3 последовательных разведения, отличающиеся по количеству высеваемого продукта в 10 раз) высевают в 2 параллельные чашки Петри;

2) Не позднее, чем через 15 минут заливают расплавленной и охлажденной до (45±1)ºС МПА (мясопептонный агар), высота слоя питательной среды должна быть 4-5 мм;

3) Инкубация: (30±1)ºС 72±3 ч в аэробных условиях;

Обработка результатов.

Подсчитывают количество колоний, выросших на чашках, для подсчета отбирают чашки, на которых выросло от 15 до 300 колоний.

По результатам подсчета вычисляют среднее арифметическое значение числа колоний из всех посевов одного разведения или в 2-3 разведениях отдельно.

Определение БГКП (колиформы) проводили в соответствии с ГОСТ Р 52816-2007 «Продукты пищевые. Методы выявления и определения количества бактерий группы кишечных палочек (колиформных бактерий)». Метод выявления колиформных бактерий основан на высеве определенного количества продукта и (или) разведений навески продукта в жидкую селективную среду с лактозой, инкубировании посевов, учете положительных пробирок, пересеве культуральной жидкости в жидкую селективную среду для учета газообразования или пересева, при необходимости, культуральной жидкости на поверхность агаризованной селективно-диагностической среды для подтверждения по

биохимическим и культуральным признакам роста принадлежности выделенных колоний к колиформным бактериям.

Определение Staphilococcus aureus в соответствии с ГОСТ Р 52815-2007 «Продукты пищевые. Методы выявления и определения количества коагулазоположительных стафилококков и Staphylococcus aureus».

Метод выявления посевом с предварительным обогащением основан на высеве навески продукта и (или) разведении навески продукта в жидкую селективную среду, инкубировании посевов, пересеве культуральной жидкости на поверхность агаризованной селективно-диагностической среды, подтверждении по биохимическим признакам принадлежности выделенных типичных и (или) атипичных колоний к Staphylococcus aureus .

Определение бактерий вида Escherichia coli проводили в соответствии с ГОСТ 30726-2001 «Продукты пищевые. Методы выявления и определения количества бактерий вида Escherichia coli».

Метод выявления E coli основан на высеве определенного количества продукта и (или) разведении навески продукта в жидкую селективную среду с лактозой, инкубировании посевов, учёте положительных колб (пробирок), пересеве культуральной жидкости на поверхность агаризованной селективно-диагностической среды для дальнейшего подтверждения по биохимическим и культуральным признакам роста принадлежности выделенных колоний к E coli. Результаты оценивали по каждой пробе отдельно. К бактериям E.coli относили оксидазоотрицательные не образующие спор грамотрицательные палочки, обладающие способностью ферментации лактозы при температуре (44±1)°С, ферментирующие лактозу и сорбит, дающие положительную реакцию с метил-рот, образующие индол, не образующие ацетоин и не утилизирующие цитрат.

Выявление бактерий рода Proteus проводили в соответствии с ГОСТ 28560-90 «Продукты пищевые. Метод выявления бактерий родов Proteus, Morganella, Providencia»

Метод основан на высеве определенного количества продукта или его разведения в жидкую селективную среду, культивировании посевов при(36±1)ºС в течение 48ч, последующим пересеве выросших культур на плотные дифферерециально-диагностические среды, культивировании посевов при(36±1)ºС в течение 48ч, выделение характерных колоний и подтверждении с помощью биохимических тестов их принадлежности к бактериям родов Proteus и (или) Morganella и (или) Providencia или к видам Proteus vulgaris или Proteus mirabilis.

Выявления бактерий рода Salmonella проводили в соответствии с ГОСТ Р 52814-2007 (ИСО 6579:2002) «Продукты пищевые. Метод выявления бактерий рода Salmonella».

Метод выявления и определения бактерий вида рода Salmonella распространяется на все пищевые продукты.

Метод основан на высеве определенного количества пищевого продукта в жидкую селективную питательную среду (с предварительным обогащением), последующем пересеве на агаризованные селективно-диагностические среды и культивировании посевов при оптимальных условиях. Принадлежность выявленных колоний к роду Salmonella определяют по биологическим свойствам.

Нами проанализированы пробы картофельного пюре на определение микрофлоры, результаты анализа представлены в таблице 1.

Таблица 1 – Результаты анализа пищевых продуктов

Наименование исследования Показатель	Число исследованных проб по микробиологическим показаниям		Предельно-допустимые концентрации (ПДК)
	Всего	Неуд	
КМАФАнМ	10	4	Не более $1*10^3$ КОЕ/г
БГКП	10	3	Не допускаются в 1,0 г
E. coli	10	2	Не допускаются в 1,0 г
S. aureus	10	-	Не допускаются в 1,0 г
Бактерии рода Proteus	10	-	Не допускаются в 0,1г

По результатам таблицы видно, что в основном пробы соответствуют требованиям качества пищевых продуктов по микрофлоре, но наблюдаются отклонения по показателям: КМАФАнМ, БГКП, E.coli. Установлено, что из 10 проб картофельного пюре - 4 имеют неудовлетворительные результаты по КМАФАнМ, 3 - по БГКП, 2 - по E. coli.

Нами проведен анализ качества пищевых продуктов по микрофлоре за 2015 год. Результаты анализов представлены в таблице 2.

Таблица 2 – Результаты анализа пищевых продуктов за 2015 год

Продовольственное сырье и пищевые продукты	Число исследованных проб по микробиологическим показателям				
	Всего	из них не соответствует санитарно-эпидемиологическим требованиям	в том числе на патогенные микроорганизмы		
			Всего	из них не соответствует санитарно-эпидемиологическим требованиям	в т.ч. выделены возбудители сальмонеллеза
Всего	4926	502	4836	18	18
мясо и мясные продукты	223	53	217	5	5
птица, яйца и продукты их переработки	339	72	322	13	13
молоко и молочные продукты	284	31	282		
масложировая продукция, животные и рыбные жиры	10	3	10		
рыба	211	31	205		
кулинарные изделия	3160	259	3140		
хлебобулочные изделия	284	18	284		
сахар	1		1		
кондитерские изделия	187	30	182		
плодоовощная продукция	26		26		
алкогольные напитки	93	4	89		
продукты детского питания	58	1	53		
консервы	7				
зерно (семена)	1		1		
минеральные воды	4		4		
биологически активные добавки к пище	38		20		

Анализ результатов проб пищевых продуктов по микробиологическим показаниям за 2015 год показал, что отклонения наблюдались практически во всех пищевых продуктах, кроме сахара, плодоовощной продукции, консервов, зерна (семена), минеральной воды, биологически активных веществ (БАД).

Исходя из выполненного исследования предложено:

1) В целях улучшения эффективности работы по выявлению некачественных продуктов следует предварительно не предупреждать производящие организации об отборе проб для микробиологических исследований.

2) Использовать экспресс диагностику методов бактериологического анализа за счет внедрения в работу новых и более быстрых методик.

3) Использовать среды, которые укорачивают время исследования (определение по цвету).

Библиографический список

1. Руководство по медицинской микробиологии. Общая санитарная микробиология. Книга 1/ Колл. авторов под редакцией Лабинской А.С., Волиной Е.Г. – М.: 2008.

ИННОВАЦИОННЫЕ ПОДХОДЫ К УТИЛИЗАЦИИ ОТХОДОВ ЛЕЧЕБНО-ПРОФИЛАКТИЧЕСКИХ УЧРЕЖДЕНИЙ

Лысечко М.С., студент
Научный руководитель: к. п. н., доцент Богатова И.Б.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Переработка медицинских отходов в настоящее время приобретает особую значимость, поскольку с каждым годом увеличивается номенклатура применяемых препаратов, объемы и степень опасности отходов, обрзующихся в результате деятельности медицинских учреждений. Путём внедрения в практическую деятельность предприятий новых методов и технологий по обеззараживанию и утилизации отходов, происходит минимизация негативного воздействия на окружающую среду.

Целью работы является разработка комплекса мероприятий по сбору, хранению и обезвреживанию отходов лечебно – профилактических учреждений.

В Российской Федерации проблема обращения с отходами лечебно-профилактических учреждений (ЛПУ) рассматривается как важная эпидемиологическая и экологическая компонента безопасности населения страны. Всемирная организация здравоохранения с 1979 г. относит медицинские отходы к группе опасных и рекомендовала создание специальных служб по их переработке. Специфичность отходов ЛПУ связана с присутствием в них, в той или иной степени, патогенной микрофлоры.

К отходам ЛПУ, в зависимости от их класса, предъявляются различные требования по сбору, временному хранению и транспортированию. Если от большинства отходов можно сравнительно безопасно избавиться путем депонирования, то медицинские отходы, подлежат обязательной переработке. Особую опасность представляют инъекционные иглы и шприцы, поскольку неправильное обращение с ними после применения может привести к повторному использованию. В любом ЛПУ должна быть организована система сбора, временного хранения, обработки и транспортирования отходов согласно СанПиН 2.1.7.2790-10 «Санитарно-эпидемиологические требования к обращению с медицинскими отходами»

Методы обработки отходов здравоохранения можно разделить на две группы.

Ликвидационные методы:

- захоронение (на специальном полигоне, без обеззараживания);
- обеззараживание химическими или физическими методами и складирование на полигонах ТБО;
- сжигание с последующим захоронением остатков от сжигания.

Для ликвидационных методов характерно значительное влияние на окружающую среду.

Утилизационные методы:

- повторное использование;
- использование отходов в качестве вторичного сырья.

Утилизационные методы, помимо экономических целей, направлены на ограничение неблагоприятного влияния деятельности человека на окружающую среду.

Для обеззараживания инфицированных отходов ЛПУ (классы Б и В в соответствии с классификацией СанПиН 2.1.7.2790-10) могут применяться химические и физические способы обработки.

При захоронении отходов, обработанных химическими дезинфектантами, возникает значительный риск загрязнения окружающей среды (особенно, водоемов) соединениями, главным образом хлора, ввиду того, что для дезинфекции отходов применяется группа хлорсодержащих препаратов. Разработка и подбор более экологичных препаратов для дезинфекции отходов является важным. Комбинация метода химической дезинфекции опасных (рискованных) отходов с механическим измельчением способствует более полному проникновению дезинфектантов в толщу отходов, повышая надежность и эффективность дезинфекции и существенно уменьшая объемы потребляемого дезинфектанта.

Сжигание - один из эффективных способов переработки отходов. Оно должно проводиться при температуре выше 800^0С, если в поток отходов учреждений здравоохранения не включены биологические отходы (части тел) и при температуре выше 1000^0С – если присутствуют биологические отходы.

В Российской Федерации пока нет развитой промышленности по сжиганию отходов. Поэтому сейчас поступает много предложений по установке небольших сжигающих устройств на территориях учреждений здравоохранения. Эти устройства разрабатываются, как правило, без системы очистки отходящих газов и основаны на технологии организованного сжигания. Оснащение небольших сжигающих устройств системами очистки отходящих газов увеличивает стоимость этих устройств в 5 - 10 раз.

Последние рекомендации ВОЗ основаны на отказе от применения технологий, связанных с химической дезинфекцией, а оптимальными технологиями для обезвреживания отходов ЛПУ предлагают считать технологии термического обеззараживания, особо выделяя методы автоклавирования (с учетом регламентов российской нормативной базы), что полностью согласуется с требованиями действующих санитарных правил и позволяет выполнить два основных требования при проведении обработки больничных отходов, а именно, предотвратить распространение инфекционного начала и обеспечить невозможность вторичного использования отдельных компонентов отходов. Хранение и транспортирование отходов по территории лечебно- профилактического учреждения классов А, Б, В допускается только в герметичных многоразовых контейнерах. Смешение потока удаления отходов класса В с другими потоками не допускается.

Для переработки, обеззараживания и утилизации медицинских отходов разработаны уникальные технологии.

Термическая установка Ньюстер основана на применении протеинового лизиса во влажном жаре. Технология термического обеззараживания обеспечивает стерилизацию массы потенциально инфицированных и инфицированных опасных медицинских отходов (включая споры грибков) на клеточном уровне, разрывая их мембраны, что принципиально отличает этот метод от методов поверхностного воздействия.

Установка "СТЕРИМЕД" обеспечивает комбинацию метода химической дезинфекции опасных отходов класса Б и В с механическим измельчением. Метод способствует более полному проникновению дезинфектанта в толщу отходов, повышая надежность и эффективность дезинфекции и существенно уменьшая объемы потребляемого дезинфектанта и удаляемых обработанных отходов.

Стерилизатор «Tuttnauer» позволяет осуществить обработку медицинских отходов паром под давлением (автоклавирование). Для этих целей также разработана **установка «ЭКОС»** (производитель ООО «Фармстер», Россия).

СВЧ-установка типа **УОМО 01/150 - «О-ЦНТ»** (СВМЕД, Россия)**,** применяет технологию СВЧ-воздействия на медицинские отходы.

По заключению ФГУЗ «Центр гигиены и эпидемиологии» отходы (классов Б и В) с внесением биологических и паразитологических тестов, обработанные насыщенным паром под давлением и насыщенным паром под давлением с измельчением (установки типа «Tuttnauer» и «Экос»), микроволновая обработка (СВЧ-установка типа «УОМО-01/150-«О-ЦНТ»), протеиновый лизис (установка типа «Newster-10») обеспечивают практически полное обеззараживание отходов. Обработка отходов химическим дезинфектантом с измельчением (установка «Стеримед – 1») показала, что спорообразующие микроорганизмы (B. Stearothermophilus) не подверглись полному уничтожению. Во всех остальных тест-культурах и отходах роста микроорганизмов не выявлено. Следовательно, эффективность обеззараживания отходов в установке Стеримед, использующей технологию химической дезинфекции с измельчением, оказалась ниже, чем в других установках.

Следует отметить, что существующие установки по утилизации медицинских отходов иностранных и. отечественных производителей, имея те или иные положительные стороны в эксплуатации, как правило, имеют принципиальные недостатки. В одних случаях это высокая стоимость в процессе утилизации, а в других - отсутствие возможности для утилизации изделий медицинского назначения из стекла и металла. Многие установки не могут быть размещены на территории лечебно-профилактического учреждения в силу больших габаритов и по соображениям экологической безопасности населения.

Библиографический список

1. СанПиН 2.1.7.2790-10 «Санитарно-эпидемиологические требования к обращению с медицинскими отходами».

2. Абрамов, В.Н. Удаление отходов лечебно-профилактических учреждений / В.Н. Абрамов. - М.: Материк, 1998. - 203 с.

3. НПФ Абрис+ «Оборудование для обеззараживания медицинских отходов. Оборудование для обеспечения инфекционной безопасности в ЛПУ» [Электронный ресурс] – режим доступа: www.abrisplus.ru.

ВЛИЯНИЕ УФ-ОБЛУЧЕНИЯ НА СЕМЕНА ФАСОЛИ И ИЗВЛЕЧЕНИЕ ИМИ ХРОМА(III) ИЗ ПОЧВЫ В ПРОЦЕССЕ ФИТОРЕМЕДИАЦИИ

Тареева А.А., магистрант
Научный руководитель: д. х. н., профессор Ольшанская Л.Н.
ФГБОУ ВО «Саратовский государственный технический университет им. Гагарина Ю.А.»
г. Саратов, Россия

Площадь загрязненных тяжелыми металлами (ТМ) земель в Российской Федерации достигла более 70 млн. га, из них около 1 млн. га имеют чрезвычайно опасный уровень загрязнения. Загрязнение почвы носит глобальный характер и может привести к непоправимым последствиям. Разрушение плодородного слоя неумолимо ведет к нарушению природного баланса, обмена веществ в природе, что может обернуться разрушением других экосистем. В стране необходимы срочные меры по снижению уровня загрязнения почв тяжелыми металлами. Из почвы тяжёлые металлы усваиваются растениями, почвы при этом восстанавливают свои свойства и этот процесс носит название фиторемедиации.

В последние десятилетия обнаружены многочисленные факты, свидетельствующие о высокой чувствительности растений к воздействию внешних физических полей различной природы (ВФП: УФ-, ИК-излучение, магнитные поля и др.), которые создают дополнительные электрические токи в биообъектах, и, изменяя величины мембранного потенциала растительной клетки, могут управлять течением процессов роста и развития, оказывая как стимулирующее, так и тормозящее влияние. Это воздействие зависит от характеристик внешних физических полей: длины волны, частоты колебаний электромагнитных излучений, интенсивности и времени [1]. Такая обработка семян является прогрессивным способом их подготовки к посеву, позволяющим не только вывести семена из состояния покоя, но и активизировать работу разнообразных биологических катализаторов – ферментов, обеспечивающих быстрый рост и развитие растений. В клеточной стенке имеются белки, пектины, фосфолипиды и др., содержащие фиксированные отрицательно заряженные группы (прежде всего – карбоксильные). Они определяют катионно-обменную способность и влияют на накопление катионов ТМ в клетке из почвенного раствора высшими растениями в процессе фиторемедиации.

В настоящей работе исследовано изменение роста и развития высших растений фасоли в процессе очистки почв от ионов кадмия (ll) методом фиторемедиации при воздействии на семена фасоли УФ - излучением.

Тестовая культура зерновая красная фасоль (*Phaseolus vulgaris*), сорт Рубин выбрана как высокопродуктивная культура, которую можно применять в целях фиторемедиации. Загрязняющими веществами служили модельные растворы сульфата кадмия $CdSO_4$, которые на основании литературных данных [2] содержали 1, 5 и 10 ПДК (*ПДК общесанитарный для Cr^{3+} 6 мг/кг почвы)*. Брали подвижную форму металла в почве [3].

В качестве источника ИК-излучения служила синяя лампа «Минина» с λ=780-1400 нм. Обработку семян проводили при выбранном времени в течение 6 часов [4].

Проведенные нами исследования по влиянию природы и концентрации ионов Cr^{3+} на высоту растений и развитие листовых пластин фасоли (таблица 1), рис. 1-3 показали, что по истечении 14 - 21 суток у растений фасоли не проявлялись значительные признаки угнетения роста и отмирания листьев. На 28 день эти процессы начали проявляться, и они усилились с увеличением концентрации токсикантов.

Таблица 1 - Влияние ИК и концентрации ионов Cr^{3+} на рост и развитие фасоли

Фасоль. Высота растения, мм.					Фасоль. Длина листа, мм.				Фасоль. Ширина листа, мм.			
Дни	К*	1 ПДК	5 ПДК	10 ПДК	К*	1 ПДК	5 ПДК	10 ПДК	К*	1 ПДК	5 ПДК	10 ПДК
7	130	0	0	20	0	0	0	0	0	0	0	0
14	210	80	80	210	70	40	10	53	65	20	10	60
21	290	260	260	265	70	60	60	54	65	60	60	57
28	300	270	280	284	60	63	50	55	60	63	52	60

Примечание: К-контроль без ИК-облучения и ТМ*

Известно, что присутствие хрома оказывает положительное воздействие на рост растений, концентрация этого элемента в нуклеотидах семян примерно в 100 раз выше, чем в общей массе растительной клетки [5], что, возможно, обусловлено его функциональной ролью.

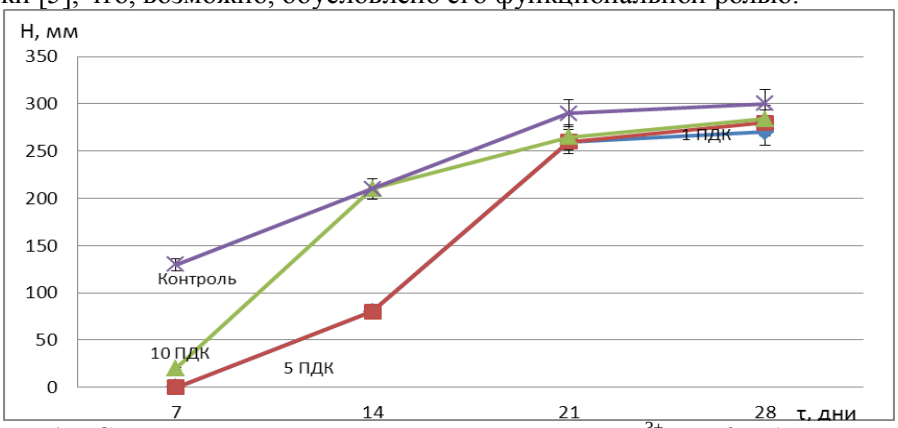

Рисунок 1 – Совместное влияние концентрации ионов Cr^{3+} и ИК- облучения семян ($\tau_{обл.}$= 6 ч.) на высоту растений фасоли

Хром повышает содержание хлорофилла и продуктивность фотосинтеза в листьях, положительное влияние этого элемента на продуктивность фотосинтеза кукурузы было показано А.Т. Щегловым. Так у выросших растений продуктивность увеличилась на 24–40 %, содержание хлорофилла - на 16–29 %, вес зеленой и сухой массы – на 34–65 % [6].

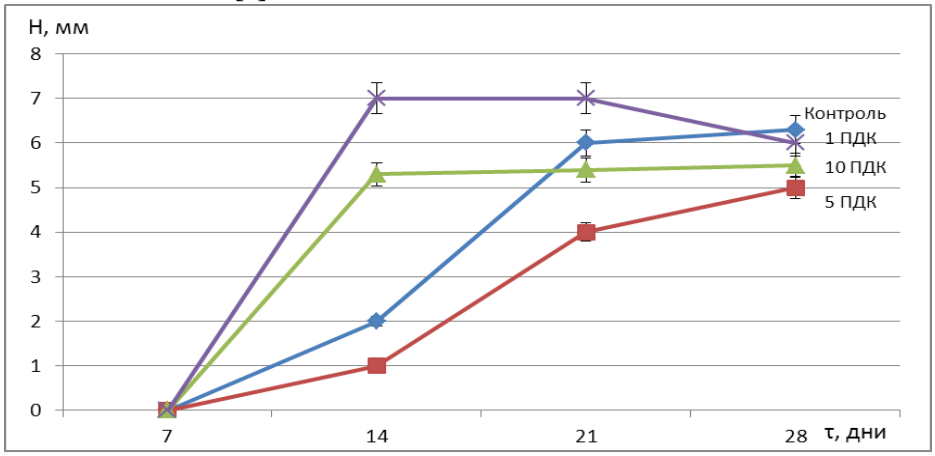

Рисунок 2 – Изменение длины листа фасоли во времени в зависимости от концентрации ионов Cr^{3+} и ИК- облучения семян ($\tau_{обл.}$= 6 ч.)

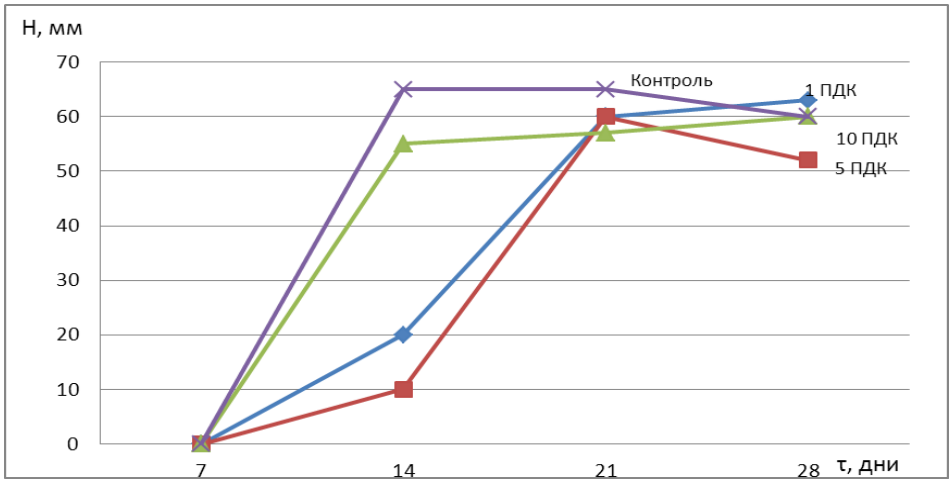

Рисунок 3 – Изменение ширины листа фасоли во времени в зависимости от концентрации ионов Cr^{3+} и ИК- облучения семян ($\tau_{обл.}$= 6 ч.)

Химические свойства дают основание предполагать, что хром, находясь в организмах, отнюдь не является индифферентным металлом, а играет важную роль в жизнедеятельности организмов [7].

Он относится к металлам с переменной валентностью, которые особенно активны в процессах комплексообразования [8].

Через 28 дней после внесения Cr^{3+} в почву растения фасоли извлекали из почвы, высушивали и взвешивали. Отделяли корневую часть растений, так как по ранее проведенным гистохимическим исследованиям, накопление металлов происходило в основном в корнях растений-исключателей, к которым относится фасоль [9, 10]. В корнях [10] образуются комплексы, которые частично иммобилизованы с донор-лигандами. По данным [11] значительное количество хрома передвигается также в листья и стебли.

Для оценки влияния концентрации ионов хрома, и его сочетанного воздействия с ИК-облучением на процессы фиторемедиации почвы проводили определение остаточных концентраций ионов Cr^{3+} в почве по ГОСТ 17.4.3.01-83 «Охрана природы почвы общие требования к отбору проб».

Готовили почвенные вытяжки и анализировали содержание в них остаточных концентраций металла фотометрическим методом.

Результаты по величинам эффективности ($Э_{оч}$, %) очистки почв от ионов хрома растениями – фитомелиорантами, семена которых были обработаны ИК-излучением и без обработки представлены в таблице 2.

Таблица 2 – Влияние концентрации ионов Cr^{3+}без и при воздействии ИК-облучения на эффективность (Э, %) очистки почвы фасолью и адсорбционную емкость растений (A_i, мкг/кг) после 28 дней выдержки

	Э, %			A_i, мкг/кг		
Концентрация Cr^{3+}	1 ПДК	5 ПДК	10 ПДК	1 ПДК	5 ПДК	10 ПДК
Без ИК	71,1	92,7	90,6	70,6	91,2	79,1
ИК	73,4	94,9	97,3	74,1	99,3	86,4

Установлено, что при низких концентрациях Cr^{3+} (1 ПДК) эффективность очистки почв растениями фасоли снижалась. Фасоль проявила лучшую эффективность очистки при концентрации хрома в почве 10 ПДК и ИК-облучении.

Адсорбционную емкость (*A_i, мкг/кг почвы)* растений (таблица 2) устанавливали по количеству поглощенного фасолью металла после сушки и мокрого озоления фитомассы (в расчете на абсолютно сухой вес массы растений). Наибольшая адсорбционная емкость фасоли оказалась при концентрации хрома 5 ПДК и при ИК-облучении семян.

Выводы

1. Изучено влияние природы и содержания хрома (III) на процессы роста и развития растений фасоли и фиторемедиацию ими почвы. Более сильное токсическое действие на растения проявляется с увеличением концентрации ТМ в почве.

2. Показано, что эффективность очистки почв загрязненных Cr^{3+}, составила для фасоли 73 – 97 % и росла с ростом концентрации металла. Это, возможно, обусловлено функциональной ролью металла. По литературным данным хром повышает содержание хлорофилла и продуктивность фотосинтеза в листьях, что способствует полноте извлечения поллютанта.

3. При определении адсорбционной емкости растений по отношению к хрому обнаружена экстремальная зависимость - максимум наблюдался при концентрации ионов Cr^{3+} равной 5 ПДК. Величины A_i для фасоли составили ≈ 74 - 99 мкг/кг сухой фитомассы.

Библиографический список

1. Алтухов, И.В., Федотов, В.А., Очиров, В.Д. Изменение основных качественных показателей семян пшеницы после воздействия различными облучателями. - Иркутск: Вестник ИрГСХА.- 2010. – Вып. 40 – С. 107-115.

2. Моделирование загрязнения чернозема свинцом с целью установления экологически безопасной концентрации / С.И. Колесников, М.Г. Жаркова, К.Ш. Казеев, В.Ф. Вальков // Экология и промышленность России. - 2009. – август. – С. 34-36.

3. Руководство по санитарно-химическому исследованию почвы. - М.: ГК СЭНР РРИАЦ, 1993. - с. 35-35.

4. Ольшанская, Л.Н., Титоренко, О.В., Еремеева, Ю.А. Влияние постоянного магнитного поля и ультрафиолетового излучения на рост высших растений и фиторемедиацию почвы от нефтепродуктов // Химическое и нефтегазовое машиностроение. - 2015. - № 5. - С. 43-45.

5. Мусиенко, Н.Н., Тернавский, А.И. Корневое питание растений. К.: Вища школа, 1989. – 203 с.

6. Щеглов, А.Т. Влияние хрома на некоторые физиологические показатели у кукурузы // Применение удобрений, микроэлементов и регуляторов роста в сельском хозяйстве: науч. труды. Ставропольского сельскохозяйственного ин-та. – В. 44, Т. 1. – Ставрополь, 1981. – С. 35–40.

7. Алексеев, Ю.В. Тяжелые металлы в почве и растениях. – Л.: Агропромиздат, 1987. – 142 с.

8. Добровольский, О.К. Биологическое действие микроэлементов в связи с их положением в периодической системе Д.И. Менделеева // Биогеохимия растений. – Улан-Уде, 1969. – С. 29–38.

9. Ольшанская, Л.Н., Халиева, А.С., Титоренко, О.В. Локализация тяжелых металлов (Pb, Ni) в тканях и органах фасоли и сои в процессе их извлечения из почвы без воздействия и при действии магнитного поля и Уф-облучения на семена растений // Известия высших учебных заведений. Химия и химическая технология.- 2015, Т. 58, выпуск 6. - С. 89 - 94.

10. Giovanni Micera. Chromium adsorption by plant roots and formation of long-lived Cr(VI) species: an ecological hozard? / Micera Giovanni, Alessandro Dessi // J. Inorg. Biochem. – 1988. – Vol. 34, № 3. – P. 157–166.

11. Wallace A., Soufi S.M., Cha J.W., Romney E.M. Some effects of chromium toxicity on bush bean plants grown in soil // Plant and soil. – 1976. – 44, N 2. – P. 421–473.

РАЗРАБОТКА ТЕХНОЛОГИИ ПОЛУЧЕНИЯ НОВЫХ УГЛЕРОДНЫХ СОРБЕНТОВ НА ОСНОВЕ ИНТЕРКАЛИРОВАННЫХ СОЕДИНЕНИЙ ГРАФИТА ДЛЯ КОМПЛЕКСНОЙ ОЧИСТКИ ВОДЫ

Чернова М.А., студент
Научный руководитель: к. х. н., доцент Яковлева Е.В.
ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.»
г. Саратов, Россия

Слоистая структура графита позволяет получать на его основе соединения внедрения с различными интеркалирующими агентами (анионы и молекулы кислот, катионы металлов, кислородсодержащие соединения и др.). Ряд соединений внедрения графита (СВГ) с кислотами, преимущественно азотной и серной, применяются для получения терморасширенного графита (ТРГ). Сейчас интеркалированные соединения графита получают преимущественно по химической технологии, окисляя углеродное сырье в концентрированных серной или азотной кислотах. Химический способ достаточно прост в технологическом плане и приборном оформлении, однако изменение концентрации кислоты, а в большей степени окислителя, в ходе процесса интеркалирования предопределяет неоднородность состава СВГ, по этой же причине синтез трудно управляем. Кроме того, получаемые соединения загрязнены окислителем и продуктами его восстановления. Электрохимический синтез обеспечивает ряд преимуществ, по сравнению с химическим: экологически более безопасен, осуществляется в контролируемом режиме, что позволяет получать СВГ необходимого состава и чистоты, использовать менее концентрированные растворы кислоты и т.д [1].

Терморасширенный графит является слоистым на микроуровне материалом с пористостью порядка 60 %. Размер частиц ТРГ в поперечном сечении составляет 0,5 – 1,0 мм, а толщина – 30 -50 нм. ТРГ и композиты на его основе, характеризуются высокой удельной адсорбционной и каталитической активностью, возможностью варьирования удельной поверхности в диапазоне $0{,}1\text{-}10^3$ м^2/г и эффективного размера пор от ангстрем до сотен микрон. Кроме того, ТРГ, благодаря особенностям своей структуры, могут прессоваться и прокатываться в изделия без участия связующего компонента. Как и графит, ТРГ химически инертен и термостоек [2].

Температурный интервал, обеспечивающий максимальное терморасширение СВГ, составляет 300 – 1000^{o}С, при этом время термообработки в зависимости от условий получения СВГ составляет от 6-10 секунд до 15 минут. Эффективность процесса терморасширения СВГ определяется либо коэффициентом вспенивания $K_v = V/m$ (см^3/г), то есть по геометрическому объему пенографита, полученному из единицы массы СВГ, либо насыпной плотностью терморасширенного графита $d_{трг}$ (г/дм^3). Насыпная плотность ($d_{ТРГ}$) в значительной степени зависит от условий получения и может колебаться в широких пределах от 1-5 г/дм^3 до 20-100 г/дм^3. ТРГ активно позиционируется как перспективный адсорбент органических соединений, в том числе нефтепродуктов с сорбционной емкостью по нефтепродуктам до 70-80 г/г сорбента, а по нефтепродуктам в водной эмульсии до 20-30 г/г сорбента. Сравнительный анализ поглощения нефтепродуктов из сточных вод при барботировании воздухом

систем с пенографитом ($S_{уд}$=30 м^2/г и $V_{пор}$=0,20 см^3/г) и с порошкообразным активированным углем марки ОУА ($S_{уд}$=1500 м^2/г и $V_{пор}$=0,52 см^3/г) широко применяющимся при очистке сточных вод, показывает практически одинаковую поглощающую способность у обоих сорбентов, а кинетика поглощения для ТРГ несколько выше [3,4].

Несмотря на высокие адсорбционные показатели по нефтепродуктам, широкое применение ТРГ в качестве адсорбента затруднено отсутствием технологии гранулирования ТРГ или изготовления компактных сорбционных модулей с сохранением большой удельной поверхности и удельной пористости.

Известно, что углеродные материалы помимо адсорбционных свойств, в зависимости от состояния поверхности, могут являться анионо- или катионообменниками. Некоторые углеродные материалы, в том числе и ТРГ, способны удерживать катионы металлов по ионообменному механизму.

Нами проведены исследования электрохимического интеркалирования дисперсного графита в кислотах. Установлено влияние потенциала анодной поляризации и сообщаемого количества электричества на состав и свойства соединений внедрения графита. Оптимизированы условия термообработки интеркалированного графита для получения терморасширенного графита (ТРГ) с регулируемыми свойствами (рисунок 1).

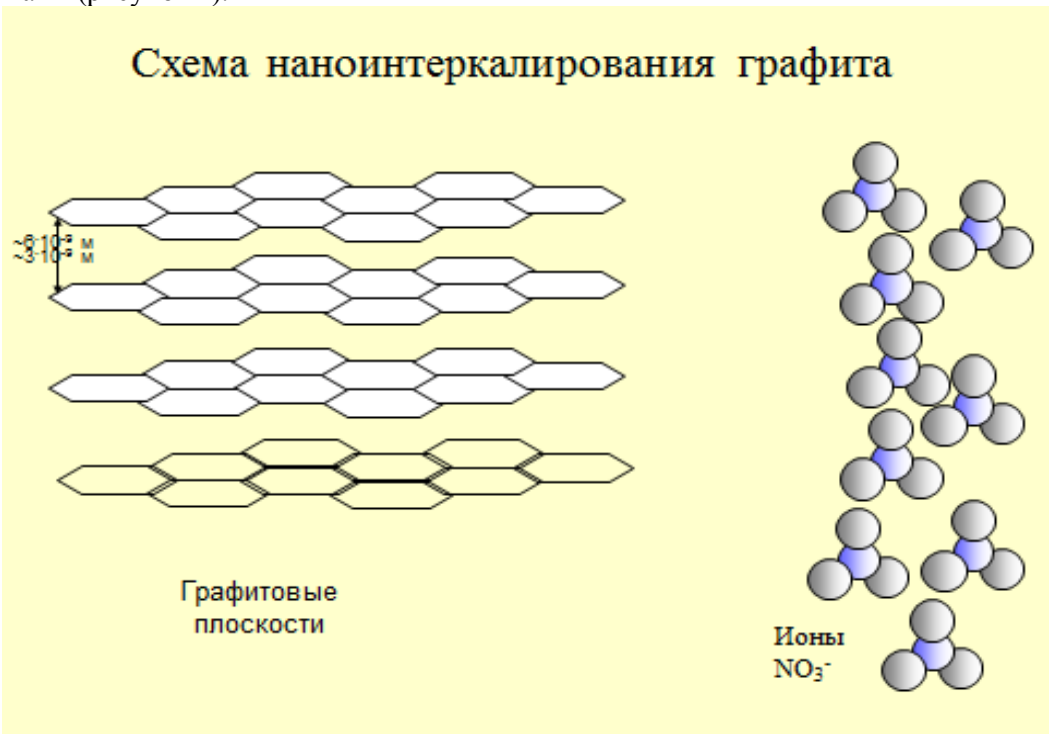

Рисунок 1 – Наноинтеркалирование графита анионами NO_3^-

Получены новые экспериментальные данные по ионообменным и адсорбционным свойствам ТРГ. Разработана методика и оснастка для создания пористых композиционные изделий на основе терморасширенного графита для использования в процессах водоочистки и водоподготовки. Проведены испытания сорбентов в процессе очистки стоков гальванических производств, локализации и сбора загрязнений нефтепродуктами в открытых природных водоемах. Разработаны технологические аспекты регенерации и утилизации сорбентов из терморасширенного графита. Исследовано влияние терморасширенного графита на биологические объекты. Оценена возможность использования терморасширенного графита для изготовления биофильтров.

Таким образом, ТРГ, является перспективным материалом для изготовления неорганических мембран, в которых углерод может выполнять функцию адсорбента и ионообменника. В связи с этим, особый интерес представляет изучение адсорбционных и ионообменных свойств ТРГ и материалов на его основе, возможности применения ТРГ в процессах комплексной водоочистки и водоподготовки. Многообразные области применения ТРГ и материалов на его основе, возрастающий спрос потребителей стимулируют развитие технологии производства и переработки СВГ. Изучение электрохимического синтеза СВГ, обладающих свойствами, обеспечивающими их переработку в ТРГ, создаст предпосылки для разработки новой высокоэффективной технологии, позволяющей получать углеродные материалы с регулируемыми свойствами для различных областей науки и техники.

Библиографический список

1. Применение терморасширенного графита в процессах водоочистки и водоподготовки / Е.В. Яковлева, А.В. Яковлев, А.И. Финаенов, Э.В. Финаенова // Журнал прикладной химии. - 2004. – N 11. - С. 1833-1835.

2. Анодный синтез терморасширяющихся соединений графита в азотной кислоте / А.В. Яковлев, А.И. Финаенов, Е.В. Яковлева, С.Л. Забудьков // Вестник СГТУ. - 2003. – N 1. - С. 113-120.

3. Яковлева, Е.В. Электрохимический синтез терморасширяющихся соединений графита в азотнокислом электролите / Е.В. Яковлева, А.В. Яковлев, А.И. Финаенов // Журнал прикладной химии. - 2002. - N10. - С. 1632-1638.

4. Яковлев, А.В. Электрохимический синтез соединений внедрения графита с азотной кислотой для получения пенографита / А.В. Яковлев, А.И. Финаенов // Журнал прикладной химии. - 1999. - N1. - С. 88-91.

МОНИТОРИНГ РИСКОВ ФИНАНСОВОЙ БЕЗОПАСНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аринина Д.В., студент
Научный руководитель: к. э. н., доцент Таратухина Н.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

На сегодняшний день кредитные организации являются важным сегментом развития экономики страны. Однако, несмотря на позитивные сдвиги в функционировании банков, сама их деятельность продолжает оставаться крайне рискованной и негативным образом влияет на экономическую безопасность страны в целом.

Актуальность темы исследования заключается в том, что финансовые риски, возникающие в деятельности кредитных организаций, оказывают определяющее влияние на результаты их деятельности, тем самым образую неустойчивость и нестабильность экономики страны.

Финансовая безопасность кредитных организаций – это состояние, при котором обеспечивается наиболее эффективное использование финансовых ресурсов кредитных организаций, направленное на предотвращение угроз и рисков, возникших в деятельности кредитных организаций, в целях обеспечения устойчивого развития и максимизации прибыли данного сегмента.

На сегодняшний день в деятельности кредитных организаций существует ряд финансовых рисков таких как:

-кредитный риск - риск неисполнения должником финансовых обязательств или неблагоприятное изменение стоимости вследствие ухудшения способности должника исполнять такие обязательства;

- рыночный риск – риск изменения рыночной стоимости финансовых активов и инструментов, связанный с изменением конъюнктуры финансового рынка;

- риск ликвидности – риск неспособности своевременно исполнять финансовые обязательства или своевременно реализовать финансовые активы или инструменты.

Проведем анализ финансовых рисков кредитных организаций.

Кредитный риск на сегодняшний день является ключевым фактором для финансовой стабильности кредитных организаций

Рассмотрим таблицу 1, где представлена динамика кредитных рисков кредитных организаций.

Показатель просроченной задолженности является ключевым фактором для оценки уровня кредитного риска кредитных организаций. За рассматриваемый период времени уровень просроченной задолженности по выданным кредитам вырос и на конец анализируемого периода составил 3134,6 млрд руб.

Таблица 1 – Динамика кредитных рисков кредитных организаций за 2015-2017 г.г., в млрд. руб.

Наименование показателя	01.01.2015 г.		01.01.2016		01.01.2017	
	Млрд руб.	Уд. вес %	Млрд руб.	Уд. вес %	Млрд руб.	Уд. вес %
Просроченная задолженность физ. лиц	667,5	33,7	863,9	28,4	900,9	28,7
Просроченная задолженность юр. лиц	1310,6	66,3	2182,7	71,6	2233,7	71,3
Всего	1978,1	100	3046,6	100	3134,6	100

Основной причинной нарастания кредитного риска являлись опережающие темпы роста просроченной задолженности по кредитам юридических лиц по сравнению с ростом объемов данных кредитов. Уровень просроченной задолженности по кредитам выданных юридическим лицам в динамике показал рост на 5% или на 923,1 млрд руб. Также в абсолютном выражении показатель просроченной задолженности физических лиц имеет тенденцию к росту и на 01.01.2017 г. составил 900,9 млрд. рублей. Данная динамика негативно сказывается на финансовой устойчивости банковского сектора экономики, что является негативной тенденцией и говорит о принятии мер, для решения данной проблемы.

На рисунке 1 представлены риски ликвидности активов кредитных организаций.

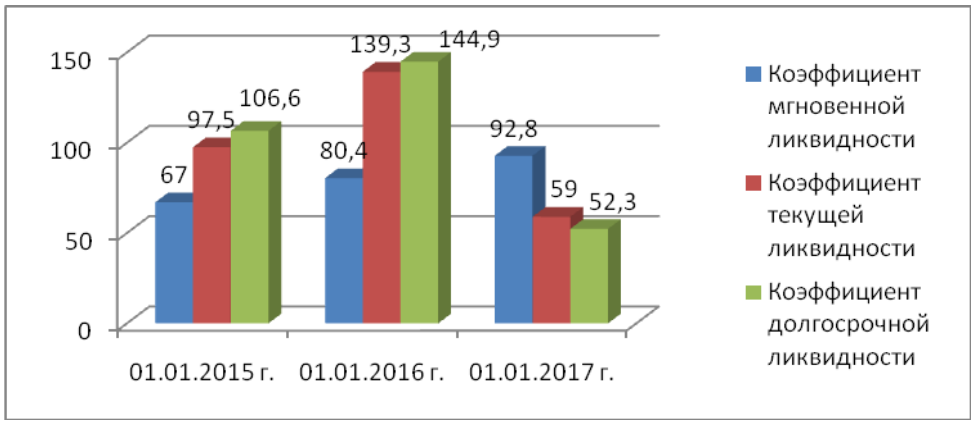

Рисунок 1 - Анализ динамики коэффициентов ликвидности банковского сектора за 2015-2017 г.г.

Анализ динамики коэффициентов ликвидности банковского сектора показал, что за анализируемый период заметна тенденция к росту у коэффициента мгновенной ликвидности и коэффициента текущей ликвидности, их значение выше нормативного значения и на конец анализируемого периода составило 106,6 и 144,9% соответственно.

В течение анализируемого периода коэффициент долгосрочной ликвидности напротив имеет значение ниже нормативного значения и имеет тенденцию к снижению значения данного показателя на 01.01.2015 г. составляет 92,8%, на 01.01.2017 г. составил 52,3%, что говорит о недостатке долгосрочных активов для покрытия обязательств банковского сектора сроком выше 1 года.

В таблице 2, представлена динамика показателей рыночного риска кредитных организаций.

Таблица 2 - Анализ динамики показателей рыночного риска, в процентах

Наименование показателя	01.01.2015 г.	01.01.2016 г.	01.01.2017 г.
Процентный риск	28,6	34,4	36,8
Фондовый риск	3,7	3,3	3,0
Валютный риск	3,7	6,3	3,2

Наибольшую долю в рыночных рисках кредитных организаций занимает процентный риск, его значение на 01.01.2015 г. составило 28,6%, на 01.01.2017 г. - 36,8% , к совокупному капиталу банковского сектора, это характеризует неустойчивое положение на денежном рынке, в связи с неблагоприятными изменениями по активам и пассивам и внебалансовым инструментам кредитных организаций.

Фондовый риск в течение анализируемого периода снижается с 3,7% до 3,0%, что говорит о благоприятном изменении цен на фондовые ценности и производные финансовые инструменты.

Резкое увеличение риска убытка вследствие неблагоприятного изменения курсов иностранной валюты заметно на 01.01.2016 г., доля риска составила 6,3%, но, наконец анализируемого периода сократилась до 3,2%, что является положительной тенденцией.

Таким образом, проанализировав финансовые риски кредитных организаций можно сделать вывод, что в современных условиях развития экономики, возникла необходимость в предложении новых мероприятий для обеспечения финансовой безопасности кредитных организаций, основанных на управлении финансовыми рисками. Среди важнейших мероприятий, снижающих финансовые риски в коммерческих банках, следует выделить следующие:

- усовершенствовать банковское законодательство;
- ужесточить надзор над банковским сектором, для уменьшения получения спекулятивной прибыли;
- создание единых комплексных мер к обнаружению рисков на начальных этапах их развития;
- разработка стратегий развития банков и контроль над ее исполнением.

В целом, для сокращения финансовых рисков кредитных организаций и формирования высокого уровня их финансовой безопасности, необходимо разработать четкий механизм мониторинга внешних и внутренних угроз банка. Причем функцию важнейшего регулятора пороговых значений финансовых рисков банков должен взять на себя Центральный банк Российской Федерации. Достижение высокого уровня финансовой безопасности кредитными организациями, безусловно, будет

оказывать позитивное влияние на национальную безопасность страны, усиливая конкурентные позиции Российской Федерации на внешнем рынке.

Библиографический список

1. Глазьев, С.Ю. Безопасность экономическая. Политическая энциклопедия / С.Ю. Глазьев. – М.: Мысль, 2015. - Т. 1.- 334 с. 46.

2. Глумов, А.Н. Формирование экономической безопасности предприятия / А.Н. Глумов, Е.П. Киселица // Академический вестник. - 2016. - № 4 (26). - С. 85-90.

3. Гончаренко, Л.П. Процесс обеспечения экономической безопасности предприятия / Л.П. Гончаренко // Справочник экономиста. – 2016. - №12. – С. 31-36.

4. Дзагаждова, Л.А. Планирование прибыли и рентабельности деятельности предприятий / Л.А. Дзагаждова, Т.К. Мирошникова // Экономика и управление в XXI веке: тенденции развития. - 2015. - №19-1. - С. 171-175.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ РЕГИОНА

Балыкин С.С., учащийся
Научный руководитель: учитель Карцева Т.Е.
ГБОУ СОШ № 7
г. Новокуйбышевск, Россия

Назначение *экономической безопасности региона* состоит в обеспечении охраны потребностей территориального образования и его населения от многообразия *внутренних*, возникающих в рамках региона, и *внешних* – со стороны проводимой экономической политики государства, администраций других регионов, иностранных государств – угроз при соблюдении равновесия с национальными интересами.

Под **угрозами экономической безопасности региона** подразумевается совокупность условий, препятствующих удовлетворению региональных потребностей или создающих опасность сокращения производственного потенциала хозяйствующих субъектов, нерационального и нецелевого использования природных, трудовых, материальных, финансовых ресурсов, усиления зависимости региона от межбюджетных трансфертов, углубления социальной дифференциации населения и обострения локальных межнациональных конфликтов.

Угрозы экономической безопасности региона являются следствием развивающихся противоречий как на внутреннем пространстве региона, так и за его пределами. Действие негативных активностей на локальные хозяйственные процессы провоцирует нарушение сбалансированного функционирования экономики региона, в результате которого аппарат управления региональной системы в силу различных факторов утрачивает контроль над стадиями воспроизводства совокупного общественного продукта.

Для обеспечения высокой степени *экономической безопасности региона* от кризисных явлений необходимо установить многообразие угроз, представляющих опасность полноценной жизнедеятельности экономических субъектов на региональном уровне.

Угрозы экономической безопасности региона подразделены на внутренние и внешние по отношению к региону.

Внутренние угрозы экономической безопасности региона обусловлены столкновением частных интересов субъектов региональной системы, что нарушает локальное социально-экономическое равновесие и вызывает обострение ситуации, выражающееся в стагнации воспроизводственных процессов, усилении социальной напряжённости и имущественного расслоения населения.

Возникновение *внешних угроз экономической безопасности региона* связано с негативным воздействием окружающей среды на регион.

В свою очередь, *внутренние угрозы экономической безопасности региона* представлены угрозами микро- и мезоэкономического уровней, *внешние угрозы экономической безопасности региона* – макро- и мегаэкономического.

Угрозы, носящие микроэкономический характер, связаны с деятельностью хозяйствующих субъектов, расположенных на территории региона. Угрозы мезоуровня возникают, как правило, в результате просчётов в области макроэкономической политики и охватывают в целом хозяйственный комплекс территории.

В макроэкономическом масштабе угрозы представлены отсутствием единой политики федерального центра в отношении регионов, что вызывает усиление региональной социально-экономической дифференциации.

Мегаэкономические угрозы обусловлены осложнением геополитической обстановки и нарастанием вероятности межгосударственных конфликтов, ростом государственного внешнего долга, оттоком капитала за рубеж, уменьшением золотовалютных резервов страны, вытеснением отечественных товаропроизводителей с национального и международного рынков, что влечёт утрату внешнеэкономических позиций Российской Федерации и негативно отражается на положении регионов и благополучии их населения.

Для обеспечения *экономической безопасности региона целесообразно проводить м***ониторинг экономической безопасности региона. . Мониторинг экономической безопасности региона** должен обеспечивать прогнозирование и своевременное выявление превышения пороговых значений с тем, чтобы своевременно принять адекватные меры для предотвращения и нейтрализации угроз *экономической безопасности*.

Главными целями **мониторинга экономической безопасности региона** являются:

– оперативное обеспечение органов государственной власти РФ информацией о состоянии *угроз экономической безопасности региона*, их характере, возможных последствиях, а также прогнозами в этой области;

– информационное взаимодействие всех органов власти;

– контроль за состоянием *угроз экономической безопасности региона*.

К задачам **мониторинга экономической безопасности региона** относятся:

– наблюдение за состоянием социально-экономической сферы региона и получение оперативной информации о ней;

– своевременное выявление изменений, происходящих в социально-экономической сфере региона, и причин, вызвавших их;

– предупреждение негативных тенденций, ведущих к формированию и развитию напряженности в социально-экономической сфере, угрожающих *экономической безопасности региона*;

– осуществление краткосрочного прогнозирования развития важнейших процессов в социально-экономической сфере региона;

– оценка эффективности методов, организационных структур и процессов управления обеспечением *экономической безопасности региона*.

К **мониторингу экономической безопасности региона** предъявляются следующие требования:

– достоверность мониторинга;

– оперативность;

– систематичность;

– комплексность;

Мониторинг экономической безопасности региона осуществляется по следующим стадиям:

– определение перечня показателей *экономической безопасности региона*;

– определение пороговых значений *показателей экономической безопасности региона*;

– расчет интегрального показателя *экономической безопасности региона*;

– при необходимости ранжирование районов, входящих в состав региона, по состоянию *экономической безопасности региона*.

Применение **мониторинга экономической безопасности региона** позволяет:

– проводить экспресс-анализ региональных кризисных ситуаций с ранжированием территорий внутри региона по уровню угроз экономической безопасности;

– проводить углубленный анализ кризисных ситуаций по сферам жизнедеятельности с целью обоснования комплекса мер по локализации и нейтрализации очагов кризисных ситуаций в регионе.

На основе итогов **мониторинга экономической безопасности региона** разрабатывается комплекс мер, направленных на преодоление кризисного состояния и устранение опасных отклонений пороговых значений показателей *экономической безопасности региона*.

Обеспечение экономической безопасности региона является непрерывным процессом защиты экономических интересов региона от внутренних и внешних угроз, обеспечиваемый путем осуществления комплекса мер, направленного на поддержание устойчивости и потенциала развития экономики региона.

В **обеспечении экономической безопасности региона** используются следующие ориентиры:

– укрепление экономической базы;

– активное участие в формировании общероссийского рынка;

– поддержание на высоком уровне и развитие научно-технического потенциала;

– создание нормальных условий жизнедеятельности людей в регионе;

– предотвращение либо локализация кризисных явлений в экономической и социальной сферах.

В рамках **обеспечения экономической безопасности региона** выделяют следующие этапы:

а) выявление угроз *экономической безопасности региона* и направленности их действий;

б) ранжирование угроз *экономической безопасности региона* по важности, времени наступления и т.д.;

в) оценки ожидаемого ущерба от действия угроз *экономической безопасности региона*;

г) формирование варианта стратегии *обеспечения экономической безопасности региона*;

д) определение и реализация конкретных мер по *обеспечению экономической безопасности региона*.

В качестве **критериев и показателей** используются: объем внутреннего регионального продукта; уровень инвестиций; уровень использования производственных мощностей; уровень износа основных производственных фондов; уровень технологического отставания производства; уровень конкурентоспособности; уровень безработицы; отношение средней заработной платы к прожиточному уровню в регионе; объем бюджетных доходов и т.д.

При **обеспечении экономической безопасности региона**, принимаются во внимание критерии, относящиеся как к государству в целом, так и к специфике *экономической безопасности* отдельных организации и предприятий, функционирующих в данном регионе. Также в рамках **обеспечения экономической безопасности региона** учитывается возможности взаимодействия с федеральными органами власти и их организациями, расположенными в регионах, гармонично сочетать интересы государства в целом, а также самого региона и расположенных в нем организаций.

В настоящее время **основными угрозами экономической безопасности региона** являются следующие:

1. **Спад производства и потеря внутреннего рынка**.
2. **Разрушение производственно-технического потенциала**.
3. **Потеря продовольственной независимости**.
4. **Криминализация экономики**.
5. **Ухудшения экологической обстановки в регионе**.
6. **Низкая степень бюджетной поддержки экономического развития регионов** (как из федерального бюджета, так и из средств региональных бюджетов).
7. **Потеря внешнего рынка**.

Данный перечень **основных угроз экономической безопасности региона** не является исчерпывающим и постоянным.

Также на выявление **основных угроз экономической безопасности региона** влияют:

– разные темпы экономических преобразований;

– предоставление отдельным регионам больших экономических и социальных льгот по сравнению с другими;

– недоучет региональных последствий проведения федеральной макроэкономической политики и т.п.

При этом важно подчеркнуть, что *угрозы экономической безопасности региона* это проекция угроз *экономической безопасности* государства.

Библиографический список

1. Экономическая безопасность России: Общий курс: Учебник /Под ред. В.К. Сенчагова. 2-е изд. - М.: Дело, 2005. - 896 с.
2. http://www.newsru.com/.
3. http://www.rbc.ru.

ДИНАМИКА ПОТРЕБЛЕНИЯ ИСКОПАЕМОГО ТОПЛИВА И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ АЛЬТЕРНАТИВНЫХ ИСТОЧНИКОВ ЭНЕРГИИ В МИРОВОМ ХОЗЯЙСТВЕ

Бурундукова Д.В., студент
Научный руководитель: д. э. н., профессор Щукина А.Я.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Наибольшее влияние на коэффициент антропогенной нагрузки (Ка) оказывает фактор потребления ископаемого топлива. Значительная доля антропогенного давления на территорию происходит из-за чрезмерного углеводородного потребления топлива. Покажем общее потребление топлива четырнадцатью странами мира за период 2012 — 2016 годы.

Таблица 1 - Динамика потребления топлива исследуемых стран[1][2][3]

Страны	2012	2013	2014	2015	2016
Швеция	16	15	13,92	13,89	17,89
Россия	952,3	1002,1	822	806	718
США	2253	2315	2335	2264	2196
Китай	4445	4622	4535	4422	3560
Германия	431	433	407	409	305
Франция	255,2	255,2	255,2	255,2	255,2
Великобритания	132	137	121	124	143
Бразилия	174	186	196	190	196
Италия	159	145	134	141	152
Нидерланды	83	83	77	78	72
Индия	998	1026	1136	1227	1189
Мексика	176	183	180	178	187
Норвегия	16	16	14	15	22
Япония	502	509	501	490	435
Всего:	10592,5	10927,3	10727,12	10613,09	9448,09

По данным таблицы 1 построим ряд графиков 1,2,3 и 4, которые более наглядно проиллюстрируют происходящие процессы в данной сфере мирового хозяйства.

Динамику общего потребления топлива основными странами мирового сообщества покажем графически (рисунок 1).

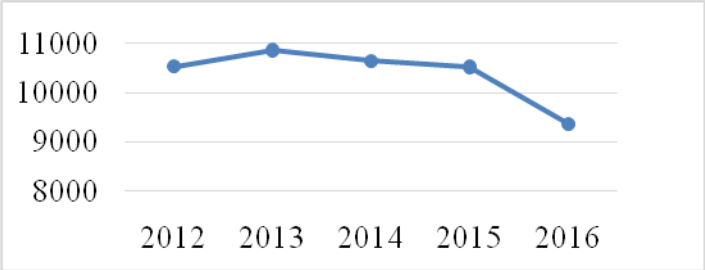

Рисунок 1 – Общая динамика потребления топлива 14 странами мира

На рисунке видно, что потребление топлива стремительно падает. США, Китай, Россия и Индия значительно превышают потребление топлива по сравнению с другими странами, более наглядно это просматривается на рисунке 2.

[1] Ножнин И.Н., Васильев А.Н., А.Я. Щукина. Сравнительный анализ степени реализации устойчивого развития стран мира и России. Научный журнал «Вестник Волжского университета имени В.Н. Татищева» №3 (34) 2015

[2] Васильев А.Н., Щукина А.Я. Оценка показателей эффективности использования природных ресурсов. Научный журнал «Вестник Волжского университета имени В.Н. Татищева» №3 (37) 2016 Том 2 сентябрь 2016г.

[3] Тенденции в энергобалансе крупнейших стран мира. URL: http://spydell.livejournal.com/547898.html (дата обращения: 29.10.2017)

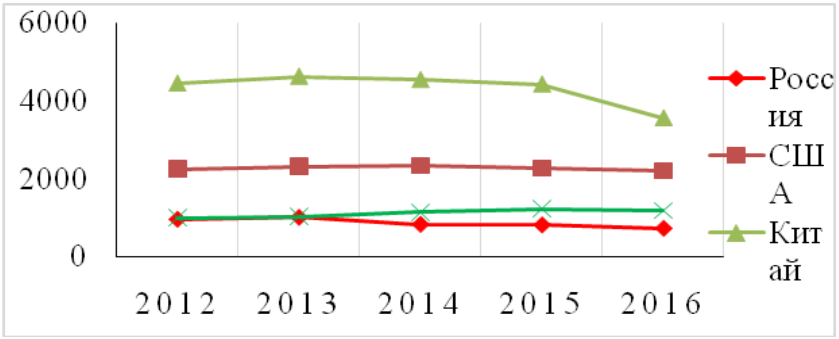

Рисунок 2 - Динамика потребления топлива странами-лидерами (млн. тонн н.э.)

Графики каждой исследуемой страны показывают тенденцию снижения потребления углеводородного топлива, отсюда наблюдается общее падение его потребления у основных стран мирового хозяйства (рисунок 1). В Индии наблюдается рост потребления топлива, но в 2015 году уже наметилось его снижение. Далее рассмотрим динамику потребления ископаемого топлива европейскими странами (рисунок 3).

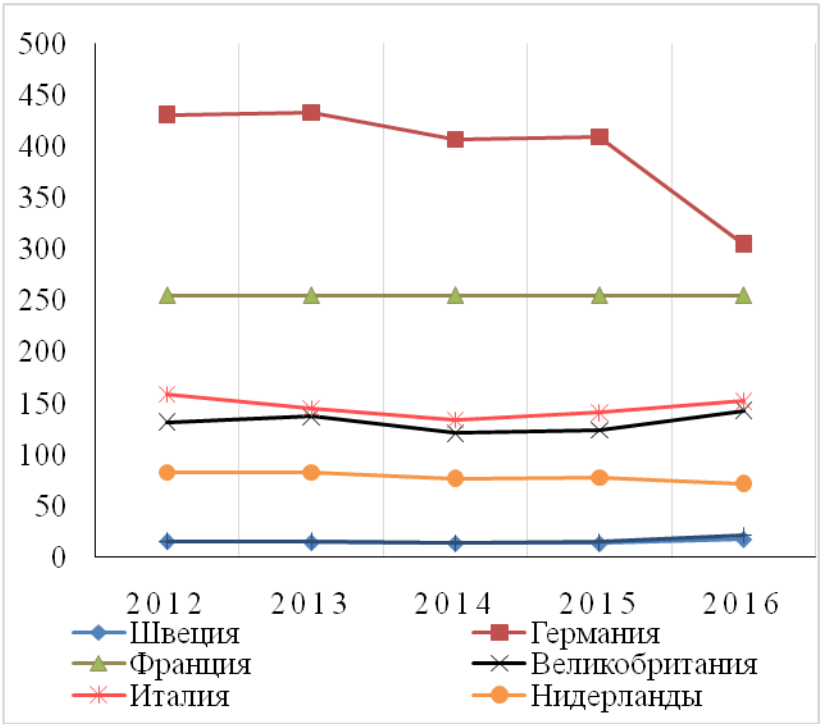

Рисунок 3 – Динамика потребления топлива европейскими странами (млн. тонн н. э.)

Несмотря на то, что Норвегия (графики Норвегии и Швеции практически сливаются), Великобритания, Швеция, Италия имеют небольшой рост показателя потребления к 2016 году, общей тенденцией является сокращение добычи и использования ископаемого углеводородного топлива. Рассчитаем темпы роста общего потребления топлива за период с 2012 по 2016 годы и покажем их динамику на графике.

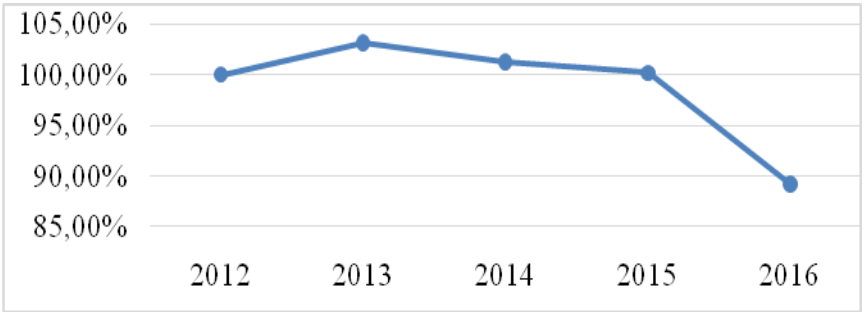

Рисунок 4 – Динамика темпов роста потребления топлива исследуемых стран

Анализ динамики темпов роста потребления ископаемого топлива позволяет сделать вывод, что по сравнению с 2012 годом в 2013 году оно выросло на 3,2 %; в 2014 году на 1,3%; в 2015 году на 0,2 %, а в 2016 году наблюдается снижение темпа роста по сравнению с 2012 годом на 10,8%, следовательно, антропогенная нагрузка на территории этих стран сокращается. Это чётко прослеживается на рисунках 10 и 12, особенно падение антропогенного давления проявляется в Германии, Японии, Нидерландах и Китае. В дальнейшем потребление ископаемых углеводородов будет снижаться, потому что многие развитые страны переходят на топливо, которое будет менее затратным и будет меньше вредить окружающей среде. Например, одним из лидеров по использованию возобновляемых источников энергии является Швеция. Приблизительно 40-60% всей энергетики страны приходится на гидроэнергетику, АЭС. Ветроэнергетика стремительно набирает обороты. На сегодняшний день 48% энергоснабжения страны приходится на возобновляемые источники энергии[1]. Также стоит отметить, что 21 мая 2017 года Швеция сделала официальное заявление о намерении к 2040 году полностью перейти на альтернативные источники энергии. 2016 год стал рекордным для этой страны – 57% всей производимой в регионе энергии пришлось на возобновляемые источники[2].

Великобритания ставит себе задачу к 2020 году увеличить долю получаемой энергии из возобновляемых источников до 15%. На данный момент этот показатель равен приблизительно до 10%. Общая доля возобновляемых источников энергии совместно с атомной энергетикой составляет 72,1%. Акцент делается на ветряные, солнечные, древесные источники. Последним рекордным показателем выработки энергии из возобновляемых источников был обозначен в отчёте на 7 июня 2017 года, где сообщалось о более чем половины произведенной энергии из альтернативных источников (50,7%)[3].

Германия имеет долю возобновляемых источников энергии в размере 32% и этот показатель только растёт. К 2020 году планируется иметь стабильно 35 %, что вполне ожидаемо, потому что темпы развития этой сферы только растут[4]. А к 2030 году 85% энергии от солнечных, ветряных (большая часть), биомассовых источников.

Нидерланды в наше время имеют возобновляемых источников энергии в размере 6-8% от всей энергетики. Страна обязалась повысить этот показатель до 14% к 2020 году[5]. Преобладающий источник – ветровые установки. В своих морских владениях страна построила самую мощную ветряную электростанцию в мире – Gemini. Планируется, что на эту станцию будет приходиться 13% производимой энергии от всех видов возобновляемых источников.

В Японии из альтернативных источников энергии преобладают солнечные батареи. Это связано с планом снижения доли АЭС в энергетике страны. Данный регион планирует к 2030 году повысить долю возобновляемых источников энергии до 22-24% (на данный момент показатель равен приблизительно 15%).

Норвегия всё чаще появляется в новостях как будущая зелёная батарейка Европы. Действительно, более 70% производимой в стране энергии приходится на гидроэнергетику (в основном энергия горных водопадов).

Китай является лидером по государственным инвестициям в сектор возобновляемых источников энергии. Главным источником альтернативной энергии является солнце. Потребление солнечной активности выросло до 12% от общего использования энергии. К 2020 году планируется повысить данный показатель до 15%.

Ведущим возобновляемым источником энергии (по скорости развития) в Индии является солнечный свет. В стране установлен рекорд дешевизны этого ресурса, который составил 2,62 рупии (4 цента) за 1 кВт•ч. Доля солнечной энергии составляет 16%. Страна поставила себе цель довести долю возобновляемых источников энергии до 40%.

---

[1] Швеция и возобновляемая энергетика.URL:http://delonovosti.ru/analitika/3966-shveciya-i-vozobnovlyaemaya-energetika.html (дата обращения: 01.11.2017)

[2] Швеция намерена полностью перейти на использование возобновляемых источников энергии к 2040 году. URL:https://privatemoney.org/blog/швеция-намерена-полностью-перейти-на/ (дата обращения: 01.11.2017)

[3] Альтернативная энергетика. URL:https://pronedra.ru/alternative/2017/06/10/vie-v-velikobritanii-rekord/ (дата обращения: 30.10.2017)

[4] Возобновляемые источники в Германии выработали 32% энергии. URL: http://csrjournal.com/21939-vozobnovlyaemye-istochniki-v-germanii-vyrabotali-32-energii.html (дата обращения: 01.11.2017)

[5] Ветроэнергетика в Нидерландах находится на грани рентабельности. URL:http:// neftegaz.ru/news/view/148366-Vetroenergetika-v-Niderlandah-nahoditsya-na-grani-rentabelnosti (дата обращения: 01.11.2017)

В Бразилии используются возобновляемые источники энергии, основу которых составляет почти 75% гидроэнергетика. Также стоит отметить частичное использование солнечной энергии, производство этанола из сахарного тростника.

В Италии преобладающим сектором возобновляемых источников энергии также является гидроэнергетика, на которую приходится 77%. Остальная часть энергии получается при сжигании отходов промышленности и всего лишь 1% от солнечных батарей.

Мексика идёт по пути увеличения возобновляемых источников энергии, львиную долю которых составляют ГЭС. Инвестиции различных фирм (по большей части из США) в размере 6,6 млрд. долларов пойдут на строительство 52 комплексов, работающих на солнечной и ветряной энергии

Франция постепенно увеличивает долю возобновляемых источников энергии. На данный момент эта доля приблизительно равняется 14%, к 2020 году планируется поднять этот показатель до 23% . Наиболее развиты ветряные и гидро- источники.

Более 70% альтернативной энергии в США относятся к ГЭС, также активно идёт развитие солнечных и ветряных источников.

В России к 2030 году показатели доли возобновляемых источников энергии могут превысить 11%. В 2017 году должно быть введено 120 МВт возобновляемых мощностей[1].

Однако следует отметить, что в настоящее время наиболее перспективным и безопасным альтернативным источником энергии является биогаз. Таким образом, анализ потребления углеводородного топлива показал, что происходит существенное падение в мире, что позволяет значительно снизить антропогенную нагрузку на территорию, а, следовательно, повысить как экономическую, так и национальную безопасность.

Библиографический список

1. Альтернативная энергетика. [Электронный ресурс]. Режим доступа: https://pronedra.ru/ alternative /2017/06/10/vie-v-velikobritanii-rekord/, свободный.

2. Васильев, А.Н., Щукина, А.Я. Оценка показателей эффективности использования природных ресурсов. [Текст]. Научный журнал «Вестник Волжского университета имени В.Н. Татищева» №3 (37) 2016 Том 2 сентябрь 2016г.

3. Ветроэнергетика в Нидерландах находится на грани рентабельности. [Электронный ресурс]. Режим доступа: http://neftegaz.ru/news/view/148366-Vetroenergetika-v-Niderlandah-nahoditsya-na-grani-rentabelnosti, свободный.

4. Возобновляемые источники в Германии выработали 32% энергии. [Электронный ресурс]. Режим доступа: http://csrjournal.com/21939-vozobnovlyaemye-istochniki-v-germanii-vyrabotali-32-energii.html, свободный.

5. Всемирный банк данных: Данные и исследования. [Электронный ресурс]. Режим доступа: http://www5.worldbank.org/eca/russian/data/., свободный.

6. Ножнин, И.Н., Васильев, А.Н., Щукина, А.Я. Сравнительный анализ степени реализации устойчивого развития стран мира и России. [Текст]. Научный журнал «Вестник Волжского университета имени В.Н. Татищева» №3 (34) 2015.

7. Тенденции в энергобалансе крупнейших стран мира. [Электронный ресурс]. Режим доступа: http://spydell.livejournal.com/547898.html, свободный.

8. Швеция и возобновляемая энергетика. [Электронный ресурс]. Режим доступа:http://delonovosti.ru/analitika/3966-shveciya-i-vozobnovlyaemaya-energetika.html., свободный.

9. Швеция намерена полностью перейти на использование возобновляемых источников энергии к 2040 году. [Электронный ресурс]. Режим доступа: https://privatemoney.org/blog/швеция-намерена-полностью-перейти-на/, свободный.

[1] Всемирный банк данных: Данные и исследования. URL: http://www5.worldbank.org/eca/russian/data/ (дата обращения: 02.11.2017)

ВЛИЯНИЕ ТЕНЕВОЙ ЭКОНОМИКИ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ СТРАНЫ

Голиков Г.О., учащийся
Научный руководитель: учитель Антонова И.Б.
МБОУ СОШ № 61
г. Тольятти, Россия

Проблемы теневой экономики стали одними из наиболее важных как для России, так и для зарубежных стран. Определенные виды теневой деятельности (наркобизнес, коррупция, финансирование терроризма) признаны угрозами национальной экономической безопасности, их справедливо включают в число глобальных проблем современности.

Ненаблюдаемая экономика представляет собой хозяйственную деятельность, которая осуществляется вне государственного учета и контроля и не получает отражения в официальной статистике. Последствия теневой экономической деятельности неоднозначны, однако ее негативное воздействие заключается в том, что она позволяет осуществлять антисоциальное распределение доходов в обществе в пользу относительно малочисленных привилегированных групп, сопровождающееся уменьшением благосостояния общества в целом. Кроме того, подобная деятельность фактически разрушает систему централизованного управления экономикой.

Ненаблюдаемые виды деятельности подразделяются на:

- теневое производство, определяемое как те виды деятельности, которые являются в экономическом смысле производственными и вполне законными, но в то же время намеренно скрываются от органов государственной власти в целях уклонения от уплаты налогов, взносов на социальное страхование или уклонения от следования определенным предусмотренным законодательством стандартам, нормам и административным процедурам;
- незаконное производство, определяемое как:

а) запрещенное производство товаров и услуг, продажа или просто владение которыми также запрещены законом,

б) виды производственной деятельности, которые обычно являются разрешенными, но которые становятся незаконными, если они осуществляются производителями, не имеющими соответствующего разрешения;

- производство в неформальном секторе, определяемое как виды производственной деятельности, осуществляемые теми некорпорированными предприятиями в секторе домашних хозяйств, которые не зарегистрированы и (или) размер которых по количеству занятых меньше определенного порогового значения, и которые имеют какое-либо рыночное производство;
- производство домашних хозяйств, для собственного конечного использования, определяемое как те виды производственной деятельности, в результате которых домашние хозяйства потребляют или капитализируют произведенные ими же товары и услуги;
- виды деятельности, неучтенные вследствие недостатков в программе сбора основных статистических данных.

Причины разрастания теневой экономики многообразны:

- финансовые;
- социальные;
- правовые;
- социокультурные;
- политические и др.

При этом неверная оценка масштабов теневой экономики служит причиной недостоверной и неполной оценки как чистого экономического благосостояния в целом, так и влияния теневой экономики на характер экономического роста в частности. Это дезориентирует деятельность государственных управленческих органов в оценках результатов национального производства и, следовательно, в определении содержания экономической политики в перспективе.

По данным отчета Экспертов Ассоциации дипломированных сертифицированных бухгалтеров (АССА) объем теневой экономики в России составляет 33,6 трлн. рублей, или 39% от размера ВВП РФ в 2016 году. По этому показателю Россия занимает четвертое место в мире. На рисунке 1 приведены страны с крупнейшей теневой экономикой.

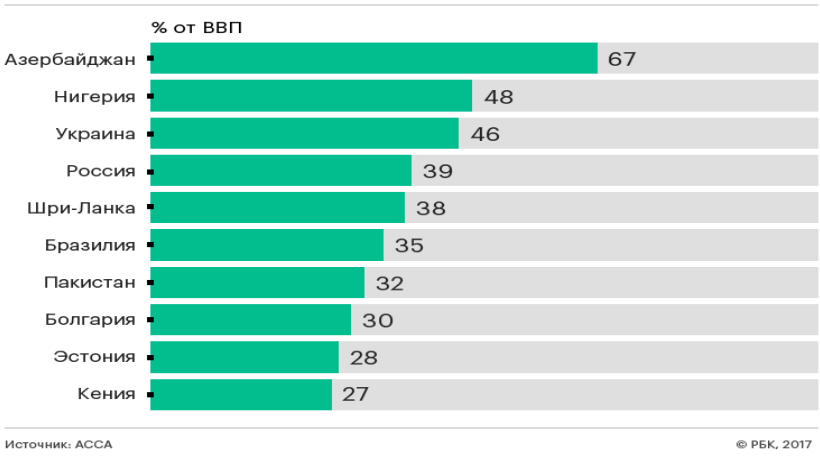

Рисунок 1 – Страны с крупнейшей теневой экономикой

По подсчетам экспертов, самый большой объем теневой экономики по соотношению к ВВП страны - в Азербайджане (66,12%). За ним следуют Нигерия (46,99%) и Украина (46,1%). На пятом месте расположилась Шри-Ланка с показателем 36,46%.

Доля теневой экономики в глобальном ВВП составила в 2016 году 22,66%, подсчитала АССА. В перспективе доля ненаблюдаемой экономики будет сокращаться: до 22,5% в 2017 году, 22,1% в 2020-м и 21,4% в 2025 году, прогнозируют эксперты.

Необходимо отметить, что в России показатель остается практически неизменным: в 2011 году он составлял 39,33%, а к 2025 году останется на том же уровне — 39,3%, ожидает АССА.

Оценки ненаблюдаемой экономики в России колеблются от 10% валового внутреннего продукта согласно данным Росстата и, до 45 - 50% по оценкам правоохранительных органов. По оценкам же социологического центра Российской академии государственной службы при Президенте Российской Федерации за последние десять лет теневой сектор вырос в 5 раз и сейчас достигает 50% ВВП России (в странах объединенной Европы значение этого показателя находится в интервале от 6 до 10%)

В России к ненаблюдаемым видам деятельности, где на теневую экономику приходится от 10 до 50% ВВП, можно отнести следующие:

- сельское хозяйство - до 50% ВВП, так как здесь присутствует личное подсобное хозяйство;

- операции с недвижимым имуществом – до 50% ВВП, так как физические лица, имеющие в собственности жилую недвижимость, получают не декларируемый «теневой» доход от сдачи недвижимости в аренду.

- торговля - до 11% ВВП, так как цена является договорной;

- *строительство - до 18% ВВП, так как всегда находятся строители, которые нелегально оказывают услуги по ремонту и отделке квартир;*

- образование - до 10% ВВП, так как широкое применение находят репетиторы-нелегалы.

Наименьшие показатели объема теневого сектора в мире по итогам 2016 года были зафиксированы в США (7,8% ВВП), Японии (10%) и Китае (10,2%). Доля теневой экономики в глобальном ВВП составила по итогам прошлого года 22,66%. По прогнозу специалистов, в ближайшие годы ее доля будет сокращаться: до 22,5% в 2017 году, до 22,1% в 2020 году и до 21,4% в 2025 году.

В мае 2017 года президент России Владимир Путин утвердил Стратегию экономической безопасности Российской Федерации на период до 2030 года.

Исходя из стратегии, российские власти планируют повысить эффективность государственного управления государственными корпорациями, государственными компаниями и акционерными обществами с государственным участием. Государство также намерено продолжить борьбу с нецелевым использованием и хищением государственных средств, коррупцией, теневой и криминальной экономикой, говорится в документе.

Для обеспечения экономической безопасности основные усилия направлены на устранение дисбалансов в экономике, территориальном развитии, развитии рынка труда, транспортной, информационной, социальной и образовательной инфраструктурах, формирование новой географии экономического роста, новых отраслей экономики, центров промышленности, науки и образования, активизацию фундаментальных и прикладных научных исследований, повышение качества общего, профессионального и высшего образования, совершенствование национальных инвестиционных и финансовых институтов, стимулирование миграции производства из других стран в Россию.

Библиографический список

1. Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. 2-е. изд. - М.: Дело, 2005. – 896 с.
2. http://www.newsru.com/.
3. http://www.rbc.ru.

ИСТОЧНИКИ ВОЗНИКНОВЕНИЯ И КЛАССИФИКАЦИЯ НАЛОГОВЫХ РИСКОВ

Гундров Н.А., студент
Научный руководитель: к. э. н., доцент Голикова О.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Выявление сущности налоговых рисков должно проводиться в контексте исследования признаков, наследуемых от родового понятия «риск». Само слово «риск» в переводе с многих иностранных языков означает «угроза», «опасность» (лат. resekum — опасность, скала; итал. risiko - опасность; франц. riscue - угроза, рисковать). Негативный характер данного понятия нашел отражение и в современных определениях. Для раскрытия природы налоговых рисков исследователи чаще всего используют признак наличия отрицательных последствий [2, 63]. При этом, несмотря на многообразие разных суждений о налоговых рисках, практически все исследователи говорят о финансовом характере налоговых рисков и, соответственно, их отрицательных последствиях как единственном либо одном из нескольких аспектах, описывающих их природу. Действительно, налоговые платежи, имея денежное выражение, обусловливают финансовый характер рисков, связанных с их оплатой. Рассматривая неблагоприятные финансовые последствия налоговых рисков, ряд ученых [6, 224] выделяют в качестве носителей налоговых рисков субъектов налоговых правоотношений. Под участниками налоговых отношений исследователи понимают плательщиков налогов и государство в лице органов государственной власти, уполномоченных в области обложения налогом [4, 87], т.е. всех субъектов, принимающих решения в области обложения налогом. Они считают, что налоговые риски несут как плательщики налогов, так и уполномоченные органы государственной власти. К примеру, Ф.Н. Филина определяет налоговые риски как опасность для субъектов налоговых правоотношений понести финансовые и иные потери, связанные с процессом обложения налогом, вследствие негативных отклонений для данного субъекта от предполагаемых им, основанных на действующих нормах права, состояний будущего, из расчета каких им принимаются решения в настоящем [3, 94]. В отношении плательщиков налогов налоговые риски рассматриваются с позиций вероятности увеличения их расходов, связанных с оплатой налогов. Под такими расходами понимаются как сами совокупности налогов, так и иные платежи, нужность оплаты каких может возникнуть в процессе обложения налогом (К примеру, штрафные санкции за нарушение налогового закона).

Налогоплательщик несет риск в виде вероятности возрастания налоговой нагрузки из-за нежелательной для него переквалификации налоговыми органами хозяйственных сделок и признания «незаконным начисление налогов, которое сам налогоплательщик рассматривал как законное» [5, 56]. Государство здесь несет риск в виде вероятности налоговых недопоступлений, вызванных применением плательщиками налогов схем минимизации налоговых платежей, основанных на противоречиях налогового закона [7, 71].

Несомненно, неопределенность, связанная с трактовкой налогового закона и обусловленная отдельными его недоработками, вызывает налоговые риски, как у государства, так и у плательщиков налогов. Но такой подход представляется узким и не охватывает полный спектр возможных источников налоговых рисков.

В этих целях представляется нужным рассмотреть все возможные источники неопределенности, способной вызвать налоговые риски. В работах отечественных авторов, посвященных вопросам анализа, оценки и управления рисками, в качестве основных источников неопределенности рассматриваются следующие:

− недостаточность информации об объекте, процессе, в отношении какого принимается решение, а также постоянная изменчивость данной информации;

− случайность, непредвиденность, неожиданность ряда событий, процессов, учесть какие при принятии решений не представляется возможным в силу их вероятностного характера;

− наличие противодействующих тенденций, спровоцированных конфликтом либо несовпадением интересов субъектов.

В дополнение к вышеназванным источникам, ряд ученых также выделяют в качестве источника неопределенности вероятностный характер научно-технического прогресса [1, 218].

Так, с учетом того, что плательщики налогов осуществляют свою деятельность согласно с утвержденным законом, их налоговые риски обусловлены неопределенностью, вызванной неполнотой и изменчивостью информации о действующем налоговом законе.

Проведенный анализ сущности налоговых рисков дает возможность сформулировать следующее определение налоговых рисков. Под налоговыми рисками следует понимать вероятность наступления отрицательных последствий финансово-правового характера для государства и плательщиков налогов, возникающую при принятии управленческих решений в требованиях неопределенности, связанной с поведением участников налоговых отношений.

Дальнейшие исследования природы налоговых рисков, разработка способов управления ими обязаны осуществляться с учетом особенностей деятельности носителей налоговых рисков в области обложения налогом. При этом особую важность имеет анализ и систематизация видов управленческих решений, принимаемых носителями налоговых рисков, и возможных негативных последствий.

Виды налоговых рисков возможно классифицировать по разным признакам:

− По субъектам, несущим налоговые риски: налоговые риски государства, плательщиков налогов, налоговых агентов, взаимозависимых лиц.

В дальнейшем возможно осуществлять детализацию рисков плательщиков налогов – для юридических и физических лиц, а государства – для разных законодательных и исполнительных органов власти, участвующих в процессе.

− Исходя из факторов, определяющих налоговые риски: внешние и внутренние (либо систематические и несистематические). Для организации - плательщика налогового платежа могут существовать обе группы рисков: внешние могут возникать по причинам, вызванными изменениями в требованиях обложения налогом, внутренние – по причине неэффективной налоговой политики самого хозяйствующего субъекта.

Систематический риск обусловлен действием многообразных, общих для всех хозяйствующих субъектов факторов.

Несистематический риск обусловлен действием факторов, полностью зависящих от деятельности самого хозяйствующего субъекта.

− По объекту связи с иными видами рисков: риском упущенной выгоды, риском потерь материальных и нематериальных ценностей, риском неплатежеспособности, инвестиционным риском и др. Так как содержание налогового риска раскрывается применительно к конкретным ситуациям, содержащим риск, и объектам их проявления, можно сказать, что для организации-плательщика налогового платежа налоговые издержки представляются одним из таких объектов, тесно взаимосвязанным с иными объектами рисков.

− Юридические лица, как правило, оценивают и прогнозируют налоговые риски. Результативность организации оценки во многом определяется классификацией риска. По виду последствий: риски налогового контроля, риски укрепления налогового бремени, риски уголовного преследования налогового характера.

Риски налогового контроля представляют собой потери, возникающие вследствие применения отрицательных санкций, предусмотренных законом. В РФ подобные санкции определяются главами 16-18 НК РФ (ст.ст. 116—135), (ст.ст. 15.2—15.11) Кодекса об административных правонарушениях РФ. В частности, к ним относятся штрафы (за неуплату либо неполную оплату сумм налогового платежа, за непредставление налоговой декларации и т.д.), а также риски аннулирования лицензий и ликвидации организации по искам налоговых органов.

НК РФ определяются три вида санкций, применяющихся совместно либо по отдельности:

− оплата совокупности налоговой недоимки;

− оплата штрафа в процентном отношении от налоговой недоимки (от 20 до 40%);

− оплата пени либо процентов за просрочку выплаты.

К рискам укрепления налогового бремени, возможно, было бы отнести рост налоговых баз как вследствие изменения методологии их исчисления, так и в связи с их динамикой, связанной с расширением объемов хозяйственной деятельности. Риск укрепления налогового бремени — риск появления новых налогов, роста ставок действующих налогов, отмены налоговых льгот, увеличения штрафов за невыполнение и иные мероприятия, увеличивающие налоговое давление на плательщика налога.

Налоговое бремя или, по-иному, налоговую нагрузку, можно рассчитать как отношение сумм всех налоговых платежей, подлежащих оплате в бюджет, к совокупности выручки от реализации и внереализа-

ционных доходов. Подобные риски свойственны финансовым проектам длительного характера, таким, как новые экономические субъекты, инвестиции в недвижимость и оборудование, долгосрочные кредиты.

Риски уголовного преследования обусловлены тем, что для руководителей организаций-плательщиков налогов, нарушающих налоговое законодательство, существует вероятность возбуждения уголовного дела и привлечения к уголовной ответственности.

Помимо уголовной ответственности, у плательщиков налогов могут возникнуть существенные финансовые потери за совершение нарушений закона, предусмотренных перечисленными выше статьями УК РФ.

− по величине возможных потерь: допустимые, критические и катастрофические риски. Так, примером критического налогового риска для хозяйствующего субъекта представляется предъявление штрафных санкций в совокупности с главной совокупности налогового платежа, представляющих угрозу платежеспособности организации-плательщика налогового платежа, примером катастрофического риска — само существование данной организации.

Существует несколько разных причин возникновения неопределенности (категорий рисков): информационные риски, риски процесса, риски окружения и репутационные риски.

Информационный риск - риск неоднозначного толкования закона плательщиком налогового платежа и налоговым органом. Степень риска, возможно, оценить на базе сложившейся судебной практики, а в отсутствие таковой нужно заранее инициировать судебный спор самостоятельно, чтобы создать нужный прецедент.

Группа рисков, связанных с неверным выполнением налоговых обязательств, ошибками в налоговом учете либо налоговом планировании называется рисками процесса.

Итак, налоговый риск — это объективная реальность, с какой сталкивается каждый субъект финансовых и правовых отношений. Этот риск несет вполне осязаемый и материальный финансовый результат в виде доходного поступления либо убытка, какой нужно оценивать. Понимание сути риска и причин его возникновения даст возможность выработать методологию управления рисками.

Библиографический список

1. Международное налогообложение: размывание налоговой базы с применением офшоров: Монография / Пинская М.Р. - М.: НИЦ ИНФРА-М, 2017. - 192 с.
2. Механизм формирования финансового потенциала малого бизнеса / Морозко Н.И. - М.:НИЦ ИНФРА-М, 2017. - 314 с.
3. Налоги и налогообложение: Теория и практика: Уч. пос. / Погорелова М.Я. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 205 с.
4. Налоговое регулирование трансфертного ценообразования в РФ: Учебник/Л.П. Грундел, Н.И. Малис - М.: Магистр, НИЦ ИНФРА-М, 2016. - 256 с.
5. Налоговый менеджмент и налоговое планирование в РФ: Монография / Евстигнеев Е.Н., Викторова Н.Г. - М.: НИЦ ИНФРА-М, 2017. - 270 с.
6. Налоговый учет: Учебное пособие / Н.И. Малис, А.В. Толкушкин. - М.: Магистр: НИЦ ИНФРА-М, 2016. - 576 с.
7. Споры с налоговыми органами при осуществлении налогового контроля и взыскании налогов и сборов: практические рекомендации / Борисов А. - М.: Юстицинформ, 2016. - 264 с.

ИНСТРУМЕНТЫ МЕНЕДЖМЕНТА РИСКА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ УДАЛЕННОЙ РАБОТЫ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Димакис М.А., студент
Научный руководитель: д. э. н., профессор Глухова Л.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Актуальность статьи заключается в том, что информация, бесспорно, выступает основой всего процесса управления в организации, труд управленца и заключается в ее сборе, изучении, обработке и грамотном толковании. От уровня организации сбора, обработки и передачи информации в целом зависит эффективность управления, а также качество принимаемых управленческих решений в частности. И тут возникает проблема обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации.

На сегодняшний день информатизация общества вместе с автоматизацией процессов развиваются столь стремительно, что игнорирование возрастающих рисков в области информационных технологий становится недопустимым.

В последние годы в России возникает концепция распределенных систем управления различными процессами, где предусматривается локальная обработка информации. В результате чего были созданы автоматизированные рабочие места (АРМ) на базе профессиональных ЭВМ для каждого уровня управления и каждой предметной области. В следствии возникает необходимость защиты информационных потоков от всевозможных рисков. Для этого используются инструменты менеджмента риска, которые помогают нам обезопасить и контролировать потоки информации.

Для начала мы рассмотрим стандарт, управления рисками ISO 31000:2009, который дает определение риска как результата неопределенности в отношении целей, где результат – это отклонение от предполагаемого исхода (положительного или отрицательного), а неопределенность – состояние недостаточности информации, связанное с пониманием события или знаниями о нем, его последствиями или вероятностью. Учитывая, что большинство рисков невозможно свести к нулевым значениям, на первое место, как в глобальном, так и в локальном масштабе выходит управление ими.

Но прежде чем браться за управление рисками ИБ, следует разобраться с существующим стандартом в этой области.

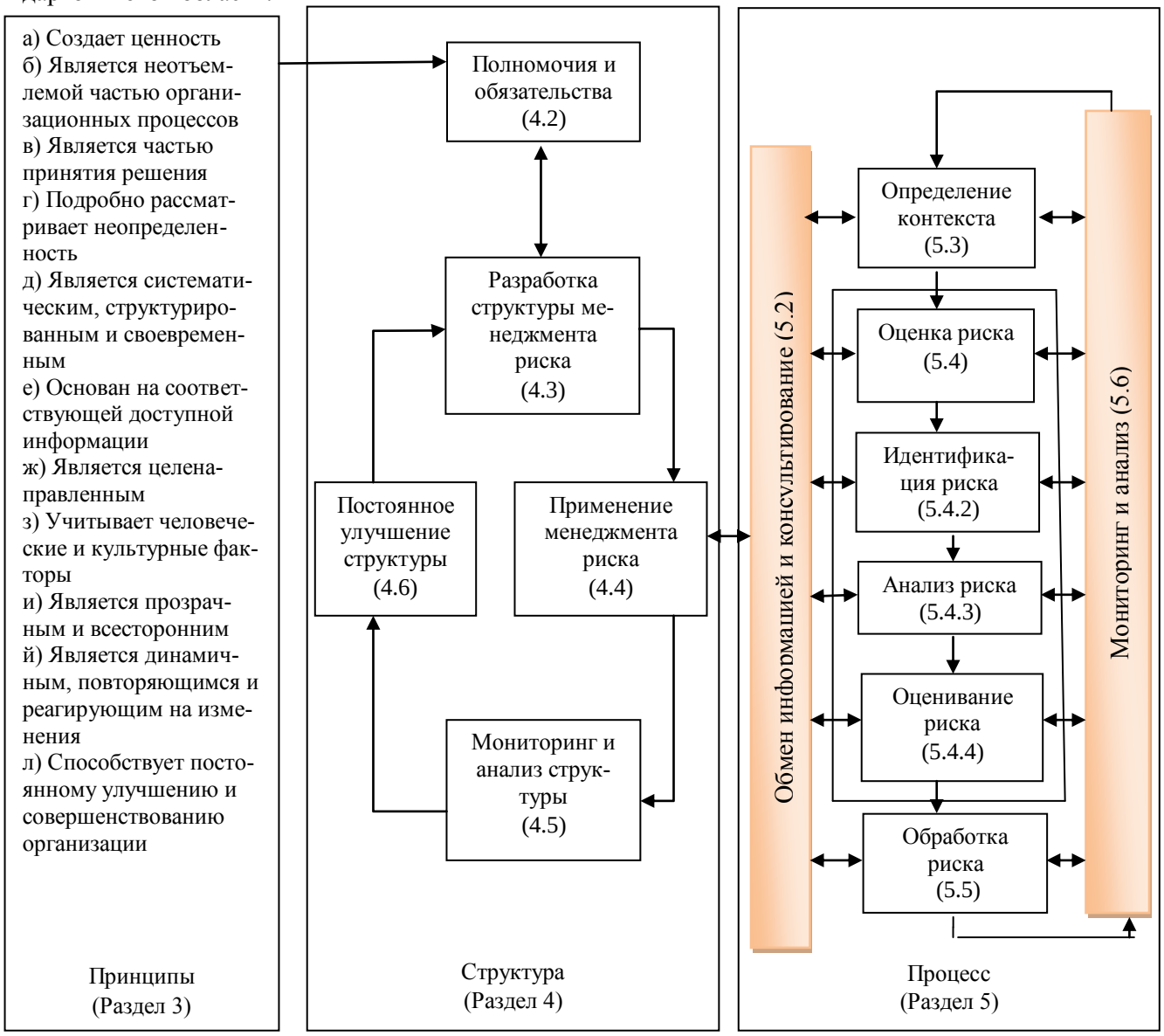

Рисунок 1 - Взаимосвязь между принципами, структурой и процессом менеджмента риска (ISO 31000)

ISO 31000:2009 является основным международным стандартом по управлению рисками для организаций и дает основные определения и принципы, которыми должна руководствоваться организация после принятия решения о внедрении системы управления рисками.

Как следствие, в организациях начинают создаваться отдельные подразделения по информационной безопасности и IT-рискам, которые занимаются выявлением и управлением рисками в данной сфере. Так, международной организацией ISO был выпущен стандарт по управлению рисками информационной безопасности в организации – ISO 27005:2008 "Информационные технологии – техники безопасности – управление рисками информационной безопасности".

В стандарте ISO 27005:2008 дается определение риска информационной безопасности – вероятность того, что заданная угроза использует уязвимости актива или группы активов и таким образом нанесет вред организации.

В соответствии со стандартом процесс управления рисками информационной безопасности позволяет организовать следующее:

-идентификацию рисков;

-оценку рисков в терминах последствий для бизнеса и вероятности их появления;

-сообщение и осознание вероятности и последствий рисков;

-выстраивание порядка приоритетов для обработки рисков;

-выстраивание приоритета для действий по уменьшению вероятности возникновения рисков;

-вовлечение заинтересованных лиц в процесс принятия решений по управлению рисками и информирование о статусе процесса управления рисками;

-мониторинг эффективности обработки рисков;

-регулярное отслеживание и пересмотр рисков и процесса управления рисками;

-выявление информации для улучшения подхода к управлению рисками;

-обучение менеджеров и сотрудников рискам и действиям для их снижения.

В области управления рисками информационной безопасности существует определенный прогресс, позволяющий заинтересованным специалистам переходить от теоретических описаний к практическим действиям. Так, международный стандарт ISO 27005:2008 служит отправной теоретической точкой, дальнейший практический путь от которой, несмотря на индивидуальный подход для каждой организации, может быть эффективно реализован.

Инструменты менеджмента риска уже показывают свою эффективность в тех компаниях, в которых они уже внедрены и обеспечивают безопасную удаленную работу конечных пользователей. В связи с кризисным состоянием Российской экономики на данный момент можно предполагать распространение в будущем подобных систем и в государственном секторе. Это возможно даже сегодня, так как уже существуют стандарты и другие документы по системе управления рисками, позволяющие внедрить данную систему качественно и в относительно короткие сроки. Однако, учитывая специфику российской экономики, многие организации больше рассчитывают на поддержку государства или так называемый административный ресурс, недостаточно уделяя внимания системе корпоративного управления и управления рисками в частности.

Библиографический список

1. ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. [Электронный ресурс] URL: http://files.stroyinf.ru/Data2/1/4293804/4293804268.pdf (Дата обращения 27.10.2017).

2. ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство. [Электронный ресурс] URL: http://files.stroyinf.ru/Data2/1/4293795/4293795643.pdf (Дата обращения 27.10.2017).

3. Макарычев, А. Управление рисками информационной безопасности в России. [Электронный ресурс] URL: http://www.itsec.ru/ articles2/pravo/upravlenie-riskami-informatsionnoy-bezopasnosti-v-rossii (Дата обращения 27.10.2017).

4. Дорофеева, А. Менеджмент информационной безопасности: управление рисками. [Электронный ресурс] URL:http://cyberrus.com/wp-content/uploads/2014/07/vkb_03_10.pdf (Дата обращения 27.10.2017).

5. Шаповалов, В. Система управления рисками компании. [Электронный ресурс] URL: https://fd.ru/articles/4365-red-sistema-upravleniya-riskami-kompanii (Дата обращения 27.10.2017).

УПРАВЛЕНИЕ ПСИХОЛОГИЧЕСКИМИ ГРАНИЦАМИ В ДИАДЕ «РУКОВОДИТЕЛЬ-ПОДЧИНЕННЫЙ»

Захаров И.В., студент
Научный руководитель: к. псх. н., доцент Семова А.А.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Каждому руководителю и рядовому сотруднику в организации приходится сталкиваться с такими ситуациями, когда кто-то опаздывает или не приходит на деловую встречу, дает советы, которых мы не спрашиваем, или когда «форс-мажорная» ситуация заставляет нас задерживаться на работе, а у вас на вечер были совсем другие планы.

Варианты реагирования на выше предложенные ситуации могут быть у разных людей различными. Кто-то начинает через силу улыбаться, боясь показать раздражение и злость. У кого-то возникает смущение и тревога, не позволяющая с возмущением проявиться к «советчику». Боязнь и страх перед руководством также является сопротивлением проявиться «другим», «отличным».

Цель данной статьи – исследование вопроса о влиянии психологических границ на деловые отношения «руководитель-подчиненный».

В статье рассмотрены основные понятия, формы нарушения и границы установления безопасных психологических границ между руководителем и подчиненным для эффективного взаимодействия в организации.

Примерами нарушения психологических границ между руководителем и подчиненным могут быть такие ситуации как: «Ваш руководитель регулярно нарушает договоренности между вами и опаздывает на планерки, совещания не предупреждая; не выплачивает вовремя заработную плату; авторитарно заставляет вас доделывать работу за тех, кто не справился в сроки.

В организации можно выделить два вида границ взаимодействия между сотрудниками: внешние и внутренние границы. К внутренним границам относятся чувства и эмоции человека. А внешние границы обозначаются социальным статусом, уровнем мышления, уровнем интеллекта. Оба вида границ позволяют очерчивать пространство влияния и ответственности менеджера и подчиненных.

Рассмотрим понятия границ в организации в процессе построения взаимоотношений между руководителями и подчиненными.

Внешние границы описываются и закрепляются в должностных инструкциях, трудовых договорах, правилах внутреннего распорядка, уставах, положениях и других документах организации. Такие формальные документы позволяют четко определять персоналу свои границы, которые выражаются в правах и обязанностях, а так жене нарушать границ других сотрудников. Тем самым, это облегчает выстраивания между руководителем и подчиненным формальных бесконфликтных коммуникаций. Это также способствует определению степени ответственности, прав и обязанностей персонала.

В своей статье автор рассматривает внутренние психологические границы, как способ разделения пространства между персоналом.

Понятие «психологические границы» рассматривалось в научных трудах зарубежных исследователей К. Левина, А. Маслоу, К. Роджерса, В. Франкла, Ф. Перлза.

Согласно идеи К. Левина, психологическими границами является полем реализации возможностей индивида в определенном жизненном пространстве. По мнению А. Маслоу, в границах выделяются наиболее значимые моменты, которые изменяют отношение человека к самому себе и к миру, моменты, которые стимулируют личностный рост и стремление к самоактуализации. В работах К. Роджерса граница предстает как «снимаемый в ходе развития личности предел, стимулирующий мотивацию личности к изменению». Для В. Франкла граница понимается как ограничение обстоятельствами. Она может быть преодолена путем нахождения смысла, своих высших ценностей. В зарубежной литературе по проблемам психологических границ интересны исследования Ф. Перлза. Автор под психологической границей подразумевает контактную границу, которая является необходимым условием процесса контакта, т.е. взаимодействие между субъектом и внешней средой (внешний мир, части организма, психика субъекта), воспринимаемой им в данный момент как не Я.

В данной статье, проанализировав научные точки зрения исследователей по проблеме психологической границы, мы определили психологическую границу как то, что определяет нашу отдельность и наши индивидуальные отличия от других людей.

Психологические границы обозначают и охраняют внутреннее пространство, собственную психологическую территорию, включающую в себя:

– систему представлений о себе (какой Я, что во мне хорошо и что плохо, какими качествами Я обладаю, оценку своей внешности);

– потребности, желания, стремления, цели и представление о способах их достижения;

– систему экзистенциальных установок, касающихся смысла жизни и смысла происходящих событий, ответственности и вины, любви и одиночества, зависимости и свободы, собственной возможности (или невозможности) принимать решения и делать выбор, творчества и ограничивающих долженствований;

– представления о собственных возможностях;

– способы и стиль взаимодействия с другими людьми;

– право создавать идеи и выбирать способ их реализации;

– представления о своем месте в мире, социуме;

– систему правил и принципов, по которым строится взаимодействие с социальной средой;

– обладание некоторой физической территорией, то есть вещами, предметами, объектами, которые именуются словом «мой» (например, стол, диван, комната, дом, одежда, рабочее место).

Почему многим людям, работающим в организации, бывает трудно сказать руководителю «нет», не удается высказать и отстоять свою идею, выразить свое не согласие с позицией и взглядами руководителя, которые отличны от ваших.

Дело в том, что психологические границы формируются в детстве при общении ребенка с родителями. Если желания, потребности, стремления ребенка игнорируются или навязываются родителями, то границы ребенка становятся нечеткими, «выпуклыми» или «вогнутыми». Но в любом случае эти границы носят «нездоровый» характер.

«Размытые» границы разрушают личность. Будучи взрослым человеком, такая личность не умеет определить границы собственного «Я», свои приоритеты, желания. В его поведении присутствует раздражение, ложное смирение, подавленность, злость, которые он скрывает под маской «послушности». Накопившееся напряжение от подавления этих чувств, в какой - то момент может неожиданно «вспыхнуть» и выразиться как ярость, гнев на незначительную ситуацию.

Персональное восприятие психологических границ может быть различным. От «здоровых», сбалансированных границ, чётко простроенных и подвижных, в зависимости от ситуаций, до полного отсутствия или только намёка на их наличие.

К «незрелым» можно отнести не только личностей «без границ», но и тех, которые построили *непроницаемые* разделительные линии. Такие люди выстраивают свое общение с другими людьми таким образом, что проявляют высокомерие, недоверие, безэмоциональность, много критикуют, иронизируют.

Люди с нарушением границ ведут себя по-разному. Можно выделить три варианта реакций.

1) В случае, когда *границы* порушены, *открыты*, человек не чувствителен к потребностям как собственной личности, так и личностей других людей. Он беспрепятственно становится объектом использования, манипуляций, лёгкой добычей для насилия. Часто такие люди не представляют различий между интимностью и публичностью, женщины могут быть не разборчивы в сексуальных связях.

2) Второй тип реакции связан с *закрытыми границами*. Человек, травмированный болезненным опытом деструктивных отношений, детскими травмами, может «сооружать» вокруг себя непреодолимые преграды, фактически изолируясь от отношений, предполагающих необходимость раскрытия. Такие люди, словно всю жизнь обороняются, становясь полностью закрытой системой. Постоянно защищая свою территорию, они никому не доверяют и обречены жить в состоянии войны со всеми окружающими. Им везде видится угроза, даже там, где её нет. Негативные детские решения вынуждают их воспринимать мир как плохой и крайне враждебный, а невраждебные действия интерпретировать как враждебные. Внутренняя агрессия легко обращается и вовне, и вслед за обороной они часто предпринимают наступление, нарушая границы других людей. Сформировавшись в ситуациях, требовавших прочной защиты, со временем, даже когда угрозы личности отсутствуют, они продолжают неизменно выполнять свою роль, не допуская подлинной близости, самораскрытия в отношениях.

3) Третья реакция – промежуточная между двумя первыми. Это – поведение человека с *размытыми, зыбким границами*. Он дезориентирован и может вести себя либо как при первом типе реакций, с открытыми границами, либо как при втором, с закрытыми. Причём, колебания в его поведении – от полной открытости до возведения непроницаемых защит, как правило, не соответствуют си-

туациям. У него есть представления о границах, но нет чётких принципов их пространивания и отстаивания.

Итак, каждому человеку жизненно важно понимать, что обретение подлинной свободы в любой сфере бытия, невозможно без установления «здоровых» границ. Если отсутствуют или рушатся границы, то неизбежно рушатся и отношения, работа становится рабской обязанностью, прекращается духовный рост. Границы воздействуют на нас во всех сферах – физической, психологической, духовной, в области межличностных отношений.

Если нет границ, их необходимо сооружать, если они зыбкие, то стоит укрепить. Границы служат нашей защите, возводя необходимый буфер между людьми, предотвращая любые покушения на психологическое пространство личности.

В чем причина нарушения здорового функционирования границ?

1. Человек не полностью осознает свои цели и желания в этой ситуации или, вообще, по жизни, а то есть не понимает, где, именно, находится его граница.
2. Человек осознает свою границу, но не может ею управлять.

Способность к осознанию и управлению своими границами определяется следующими чувствами:

- Злость;
- Отвращение;
- Сочувствие (жалость) к себе.

Следовательно, если человеком по какой-либо причине блокируется переживание этих чувств сознательным или бессознательным образом, то у него будут возникать проблемы с формированием и управлением психологическими границами личности.

Работа по выстраиванию здоровых, сбалансированных границ личности носит комплексный, системный характер и связана напрямую с достижением зрелости системы «Я».

Вот несколько, из множества возможных, направлений по установлению «здоровых» границ. Этот труд необходимо включает в себя:

- повышение самооценки, чувства собственного достоинства, укрепление веры в свою ценность, значимость;
- обучение доверию собственным чувствам. Раскрытие своей истинной сущности возможно лишь в принятии и демонстрации того, что происходит во внутреннем мире в каждый конкретный момент, без подавления и осуждения себя. Этому может помочь освоение навыков «Я-высказывания», как умения открыто говорить о своих переживаниях, потребностях и подлинных желаниях;
- обучение способности говорить «да» и особенно «нет», в зависимости от своих истинных предпочтений и желаний. Способность сказать «нет» подобна подаваемому всему миру знаку: «Я – личность. У меня есть потребности, вкусы, предпочтения, которые столь же важны, как и ваши. И я могу за себя постоять». Сказав «нет», вы тем самым обозначаете границы своего суверенитета;
- развитие навыков ассертивного поведения. Они предполагают умения выразительно и отчётливо заявлять о желаемом; принимать возможные неприятности; открыто и откровенно выражать свои чувства; конструктивно решать возникающие конфликты; распознавать и противодействовать манипулятивным приёмам.

В данной статье автор попытался рассмотреть конкретные ситуации завуалированных посягательств на психологические границы личности в организации. А также высказал свою точку зрения на основе существующего общего подхода к данному вопросу о расстановке психологических границ в диаде «руководитель - подчиненный».

Невозможно дать единого рецепта на все случаи жизни, как вести себя при взаимодействии с другим человеком в организации, не нарушая его границ и не позволяя вторгаться в свое пространство. То, насколько комфортно мы чувствуем себя, ответственны, в первую очередь, мы сами. Можно обвинять руководство, окружающих, можно критиковать себя, а можно самому устанавливать необходимые границы и отвечать за последствия своих выборов.

Библиографический список

1 «Психологические границы личности» http://psychology-s.ru/psihologicheskie-granicy-lichnosti/(дата обращения: 16.10.2017).

http://banki-uchebnik.ru/menedzhment/113-podchinennye-v-organizatsii

2. «Подчиненные в организации»http://banki-uchebnik.ru/menedzhment/113-podchinennye-v-organizatsii(дата обращения: 16.10.2017).

3. Володина, Ю.А. 2010 год. Журнал «Вестник Брянского государственного университета» на тему «Проблема определения границ психологического пространства личности» https://cyberleninka.ru/article/n/problema-opredeleniya-granits-psihologicheskogo-prostranstva-lichnosti(дата обращения: 16.10.2017).
4. Бешига, А. № 9 (1164) «СП» от 08.03.2017 года. http://esp.md/kaleydoskop/2017/03/18/lichnye-granicy-kak-ne-poteryat-sebya-na-rabote (дата обращения: 17.10.2017).
5. Сахарова, О. 04.08.2017 год. Психологические границы. Управление психологическими границами. https://www.psysovet.ru/threads/7200/(дата обращения: 17.10.2017).
6. Князев, И.В. 12.02.2015 год. Психологические границы https://upsihologa.com.ua/ Psihologicheskie_granicy-yuiop.html (дата обращения: 15.10.2017).
7. Уласевич, Т. 19.12.2016 год. Личные границы человека. http://psychologytoday.ru/ public/lichnye-granitsy-cheloveka/ (дата обращения: 15.10.2017).

ИНФОРМАЦИОННАЯ ЭКОНОМИКА КАК ОСНОВНОЙ ЭТАП ФОРМИРОВАНИЯ ЭКОНОМИКИ УСТОЙЧИВОГО РАЗВИТИЯ

Захарова Т.А., студент
Научный руководитель: д. э. н., профессор Щукина А.Я.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Человек на протяжении многих тысячелетий использовал окружающую природную среду в качестве источника ресурсов. В течении длительного периода его деятельность не оказывала значительное воздействие на биосферу Земли. 20 век изменил ситуацию в сторону лавинонарастающих негативных изменений в окружающей природной среде. Стремясь к комфортному проживанию и удовлетворению своих материальных потребностей, общество постоянно наращивало производственные мощности, не учитывая законов природы и не задумываясь о последствиях. При таком подходе огромная часть изъятых из недр Земли ресурсов возвращались к ней в качестве отходов, состоящих зачастую из синтезированных и ядовитых веществ.

В связи с чем, возникает объективная необходимость смены деятельности парадигмы хозяйствования на новую. Все более очевидным становился тот факт, что приход экономики устойчивого развития неизбежен. Стремительная деградация окружающей природной среды ведет к угрозе безопасности существования человечества и неотвратимо приближает его к вымиранию. Эта близость определяется лишь временным периодом способности человека осуществлять свою деятельность в условиях, хищнически израсходованных, ограниченных природных ресурсов. Необходимы масштабные исследования путей минимизации скоростей деградации окружающей природной среды, требуется разработка приемлемых систем ее дальнейшего развития. На смену старому технологическому укладу должна прийти экономика, двигаемая информационными знаниями и технологиями. Новая экономика должна быть динамичной, наукоёмкой и чутко реагирующей на изменения, происходящие в окружающей природной среде.

Знания, полученные в какой-либо сфере, могут кардинально поменять уклад целого государства. В связи с этим, сегодня большое внимание уделяется информационной экономике.

Главное направление в экономике информация задаёт в системе производительных сил, а также производства и потребления. Направления её действия наглядно представлены на рисунке 1.

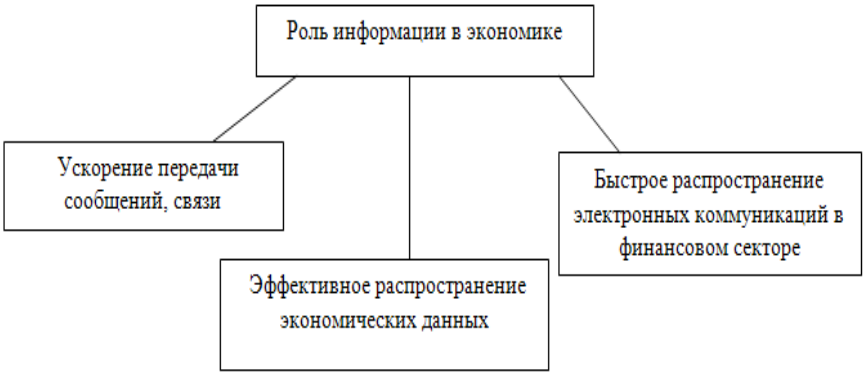

Рисунок 1 – Роль информации в экономике

Развитие информационной экономики ведет не только к изменению устройства определённой системы, но и к совершенствованию основных экономических законов. Основная идея заключается в том, что информационный продукт не подчиняется закону об убывающем доходе. Напротив, затраты на информационный продукт сравнительно не высоки и постоянны. Происходит это из-за того, что эффект масштаба осуществляется нетрадиционно. А именно со стороны спроса (внешние сетевые эффекты), то есть за счет повышения спроса повышается и объем производства. К примеру, возьмем такую крупную, известную компанию как Microsoft Windows. Потребительская полезность данной операционной системы прямо пропорциональна количеству её потребителей. Примером развития инноваций могут служить облачные технологии.

Облачные технологии – технологии, не требующие использования локального сервера или компьютера, то есть команда выполняется удалённо, зачастую через интернет.

Облачные технологии состоят из большого количества серверов, расположенных в центре обработки данных (ЦОД). Предприятия активно используют «облако» для экономии ресурсов, так как данная технология позволяет экономить на размещении собственных систем планирования ресурсов предприятия (ERP-система). Динамика развития облачных технологий представлена на диаграмме (рисунок 2).

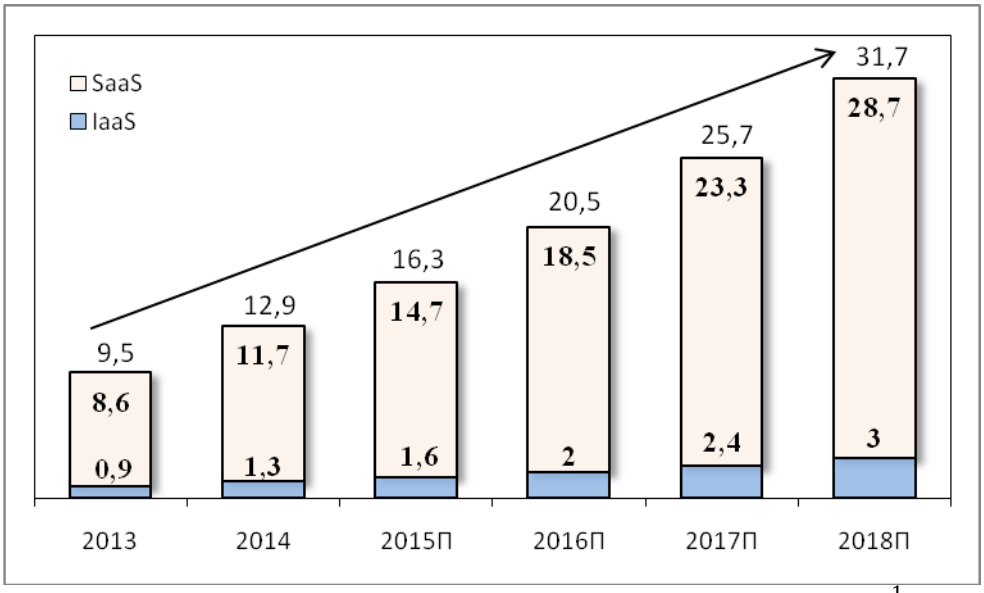

Рисунок 2 - Динамика развития облачных технологий в млрд руб.[1]

Представленная перспектива развития информационных технологий до 2018 года свидетельствует о том, что облачные технологии не останавливаются в своём развитии, в связи с чем получают надёжную поддержку со стороны государства, а также от частных инвесторов для дальнейшего развития.

Стоит отметить, что наряду с облачными технологиями важными сторонами в развитии информационной экономики является развитие технологий в области аналитики больших объёмов данных, а также интеграция мобильных устройств и технологий социальных сетей в корпоративную среду. Все эти направления были объединены в общий термин «Третья платформа». Предполагается, что третья платформа уже в ближайшем будущем кардинально поменяет бизнес-модель в различных отраслях рынка информационных технологий. Процесс поэтапного формирования и развития ИТ-рынка можно представить в таблице 1.

Примером социальных технологий на 3 платформе может служить широкое применение ИТ-технологий в сфере образования, а именно: ведение школьных электронных дневников, специальные форумы для обмена научной информацией и многое другое.

Основываясь на информационной и инновационной экономике, в России разрабатывается проект «цифровой экономики». Формирование цифровой экономики стало зарождаться еще в 2000-х годах. В 2016 году президент В.В. Путин обратился к Федеральному собранию, уделив особое внимание ИТ-сфере и цифровой экономики.

[1] Рынок телекоммуникаций. URL:http://www.iks-consulting.ru (дата обращения: 28.10.2017)

Таблица 1 –Три платформы в эволюции ИТ-рынка

Этап эволюции	Основа	Количество пользователей
1 платформа	Мейнфреймы и терминалы – основа работы тысяч приложений и программ	Тысячи пользователей
2 платформа	– Традиционные персональные компьютеры; – Интернет и веб-технологии; – Клиент-серверная архитектура программного обеспечения; – Сотни тысяч приложений.	Миллионы пользователей
3 платформа	– Большие объемы информации; – Мобильные устройства; – Облачные вычисления; – Социальные технологии.	Миллиарды пользователей

В.В. Путин призвал к продолжению наращивания уровня информатизации. В ходе реализации данного проекта уже в июне 2017 года была разработана и утверждена программа «Цифровая экономика», которая предусматривает меры по созданию правовых, технических, организационных и финансовых условий для развития цифровой экономики в РФ и ее интеграции в пространство цифровой экономики государств – членов Евразийского экономического союза (ЕАЭС)[1]. Помимо этого, программа “Цифровая экономика Российской Федерации” направлена на формирование в России благоприятной регуляторной среды для применения цифровых технологий в экономике, наращивание компетенций в области цифровых технологий российских предприятий, развитие инфраструктуры обработки данных, обеспечение киберустойчивости, подготовку достаточного количества качественных кадров и многое другое. По словам Андрея Белоусова, помощника президента по экономическим вопросам, важным моментом в формировании программы цифровой экономики выступает формирование реестра технологий или компетенций, которые нужны нам в стране, к 2020 и 2025 годов. Одновременно необходимо определить, кто сможет создать и контролировать эти компетенции[2].

Не стоит забывать о том, что фундаментом в развитии инновационной и новой, цифровой экономики является экономика, основанная на знаниях, то есть информационная экономика. Именно она позволяет разрабатывать и совершенствовать инновационную инфраструктуру, создавать аддитивные технологии, которые, в свою очередь, привели к формированию цифровой экономики.

Государство со своей стороны оказывает мощную поддержку информационной экономике. Согласно приведенной ниже таблице 2, большое количество инвестиций направленно в эту область.

Таблица 2 –Государственное инвестирование по секторам экономики за 2017год

Сектор экономики	Кол-во инвестиций (%)
Финансовые услуги	0,17
Биотехнологии	19,57
Транспорт	0,19
Строительство	1,34
Промышленное производство	1,20
Медицина	2,19
Консалтинг и образование	1,78
Химические материалы	7,69
Телекоммуникации	7,74
Информационные технологии	26,02
Промышленное оборудование	5,74
Электроника	13,94
Энергетика	8,80
Потребительский рынок	3,64

Для наглядности построим диаграмму по приведённым данным таблицы и проанализируем их.

Из диаграммы видно, что государство уделяет особое внимание развитию информационных технологий, и как следствие, выделяет больше инвестиций в эту сферу. Второе место, как показано на

[1] Правительство России. URL:http://government.ru (дата обращения: 28.10.2017)

[2] Российская ассоциация электронных коммуникаций. URL: raec.ru (дата обращения: 01.11.2017)

диаграмме, занимают биотехнологии или аддитивные технологии, значимость которых невозможно переоценить.

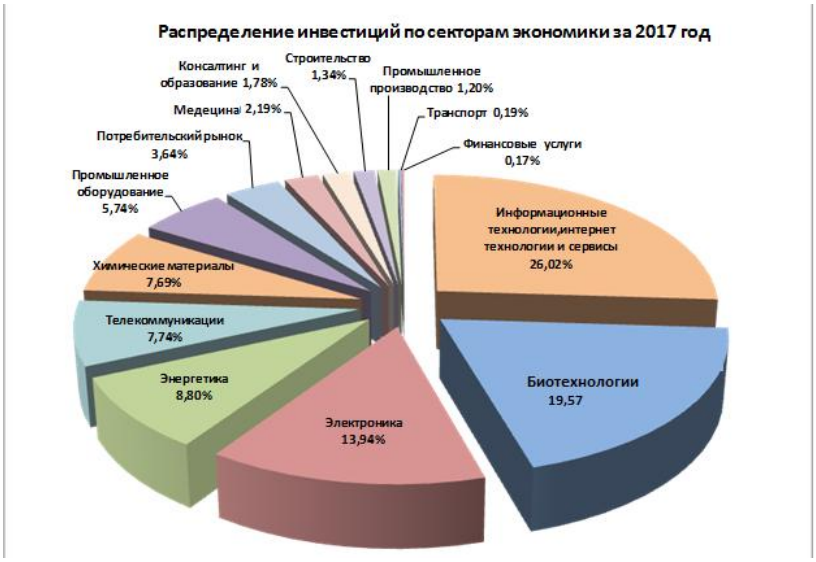

Рисунок 3 – Распределение инвестиций по секторам экономики за 2017 год

Аддитивные технологии являются ярким примером развития инноваций. Помимо увеличения доходности предприятий, за счёт внешних сетевых эффектов, информация даёт нам возможность развивать инновационные проекты, которые, в свою очередь, так же играют важнейшую роль в становлении экономики устойчивого развития. Эти инновационные технологии основаны на создании деталей природным путём или по-другому путём взращивания. Фактически, появляется возможность делать биологические вещи. Например, создавать протезы, заменять кости, выращивать детали человеческого организма. Уже сегодня аддитивные технологии являются передовыми во всем мире. Страны вкладывают средства в эту отрасль, осознавая то, что инвестируют в своё будущее. Объем производства с помощью аддитивных технологий будет только расти. Это так же подтверждают данные мировой статистики (рисунок 4).

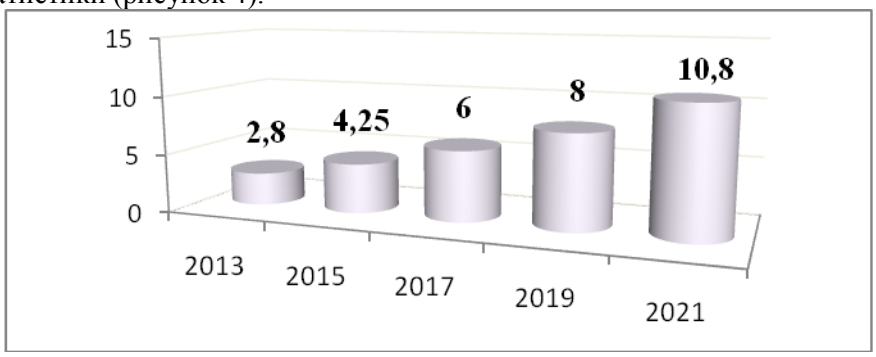

Рисунок 4 - Прогноз роста объёма аддитивного производства в мире за период 2013-2021 годы

На сегодняшний день в России уже имеются возможности создавать детали любого назначения аддитивным путем, не отрезая лишнее, а наращивая необходимые размеры. Это и есть природоподобные технологии, которые уже практикуются в Российской производственной сфере.

Значение информации в современном мире очень велико. Помимо того, что основанная на ней информационная экономика определяет производительность всех основных факторов производства, эта система позволяет создавать новейшие технологии, а также служит базой для появления и развития программ и проектов, позволяющих в дальнейшем сформировать экономику устойчивого развития.

Библиографический список

1. Багрова, Н.А. Развитие инновационной экономики в современных условиях. [Текст] / Н.А. Багрова. ФБГОУ ВО «Российский государственный университет». – Москва, 2016.

2. Киреева, Н.Г. Экономика и природная среда. [Текст] / Н.Г. Киреева, Н.В. Киреева. Рандеву - АМ, Агар. 2016. – 176 с.

3. Марин, С. Рынок аутсорсинговых контактных центров в России 2015-2020 годы. [Текст] / С. Марин, С. Патрикеева. – Москва, 2016. – 118 с.

4. Правительство Российской Федерации. Распоряжение от 28 июля 2017 года № 1632-р. [Электронный ресурс]. Режим доступа: http://government.ru., свободный.

5. Российская ассоциация электронных коммуникаций. [Электронный ресурс]. Режим доступа: raec.ru., свободный.

6. Рынок телекоммуникаций. [Электронный ресурс]. Режим доступа: http://www.iks-consulting.ru., свободный.

БЕЗРАБОТИЦА КАК УГРОЗА СОЦИАЛЬНОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ

Ирицян А., студент
Научный руководитель: к. п. н., доцент Исакова Т.Б.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Наличие безработицы в тех или иных формах и того или иного уровня признается практически во всех странах. При этом можно установить взаимосвязь между степенью изученности этой проблемы в определенной стране и ее положением в мировом сообществе. Наиболее экономически развитые страны тратят большие средства на анализ, прогнозирование безработицы и разработку путей ее стабилизации, а, по возможности, и снижения.

Этот вывод нашел свое юридическое закрепление в 1948 году во «Всеобщей декларации прав человека», где подчеркивается, что каждый человек имеет право на труд, на свободный выбор работы, на справедливые и благоприятные условия труда и на защиту от безработицы[1].

Актуальность данной статьи состоит в том, что проблема занятости населения стала одной из острейших социальных проблем, с которыми столкнулось человечество в XXI веке. Безработица несет с собой не только бедность значительным слоям населения, но и духовную, моральную, нравственную деградацию людей. Поэтому решение проблемы занятости населения и, прежде всего, молодежи, стоит в числе наиважнейших, первоочередных задач обеспечения социальной безопасности в любой цивилизованной стране.

В первую очередь это связано с тем, что молодежь – это будущее общества, а ее трудовая деятельность является средством социального обеспечения населения страны.

Рынок труда молодежи является насыщенным в силу того, что каждый год школы, колледжи, вузы выпускают огромное количество молодых людей нуждающихся в трудоустройстве. Однако, из-за невысокой квалификации и отсутствия опыта трудовой деятельности, работодатели слабо заинтересованы в приеме на работу выпускников, несмотря на то, что молодежь наиболее адаптирована к постоянной смене вида деятельности и обладает наибольшим потенциалом профессионального роста, что обостряет проблему безработицы среди молодежи.

Авторы пособий по экономике трактуют безработицу как положение экономически активной части населения, характеризуемое отсутствием у людей наемной работы или законного прибыльного занятия при наличии стремления иметь такое занятие и его поиска[2].

Безработными в Федеральном Законе «О занятости населения» признаются трудоспособные граждане, которые не имеют официальной работы и заработка, зарегистрированы в органах службы занятости населения в целях поиска подходящей работы, ищут работу и готовы приступить к ней. При этом в качестве заработка не принимаются к сведению выплаты выходного пособия и сохраняемого среднего заработка гражданам, уволенным в связи с ликвидацией организации либо прекращением деятельности индивидуальным предпринимателем, сокращением численности или штата работников организации, индивидуального предпринимателя[3].

Но, если учитывать то, что молодые люди не всегда встают на учёт в центры занятости, они по факту так же являются безработными. В связи с этим в статистических данных цифры указаны меньше, чем реальное значение числа неработающей молодёжи.

---

[1] Всеобщая декларация прав человека - М.: Книга по Требованию, 2012. - 461 с.

[2] Рофе, А.И. Экономика труда. Учебник / А.И. Рофе. - 3-е изд. доп. и перераб. - М.: КНОРУС, 2015. − 376 с.

[3] Закон РФ от 19.04.1991 №1032-1 (ред. От 28.12.2016) «О занятости населения в РФ», статья 3 «Порядок и условия признания граждан безработным», [Электронный ресурс] режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_60/e8db22bb3d2f8269f06f80a9749a8ff61bcf8bf5/

Приведём эти статистические данные за прошедший 2016 год: самый высокий уровень безработицы в России наблюдался среди недавних выпускников школ — городской молодежи в возрасте 15–19 лет (29,2%) и молодежи сельской (25,6%). Почти вдвое меньше — среди молодых людей в возрасте 20–24 лет (12,5 и 15% соответственно). Специалисты Росстата отмечают, что в среднем среди молодежи в возрасте до 25 лет процент безработных составляет 13,6%[1]. Этот показатель является довольно высоким. На данное время существует тенденция к увеличению этого числа, по крайней мере, в 2017 его снижения не ожидается.

К основным причинам безработицы среди молодых людей относят:

– отсутствие опыта работы у молодежи;

– несоответствие уровня квалификации и профессиональной подготовки работника требованиям работодателя;

– рост общей численности безработных;

– низкая конкурентоспособность;

– недостаток информации о наличии вакантных рабочих мест;

– недоверие работодателей к качеству исполнения работы молодежью.

На сегодняшний день в России не созданы необходимые условия, которые способствовали бы в реализации права на труд для молодых граждан страны. По мнению Н.И. Чернышевой молодёжная политика на федеральном и региональном уровнях не имеет стабильной и гибкой базы. Это не смотря на то, что молодёжь считают будущим нации[2].

На наш взгляд, необходимо принять следующие меры в области регулировании трудоустройства молодёжи:

– создавать для молодёжи атмосферу стабильности и защищённости;

– совершенствовать нормативно-правовую базу;

– перестроить образовательную деятельность высших и средних профессиональных учебных заведений, сократив число невостребованных программы, и расширить спектр программ по подготовке к профессиям, которые востребованы в современных условиях;

– так же, в образовании увеличить объем практической подготовки, возможно, с накоплением профессионального опыта, введя стажировки, большее количество часов практик;

– создавать рабочие места для молодых специалистов, ввести квоты на рабочие места для молодежи.

Таким образом, можно отметить то, что сегодняшняя молодёжь оказывается в положении между возможностями и желаниями осуществления своей профессиональной деятельности. Сложности в поиске работы без опыта, но с достойным образованием ставят под сомнение заинтересованность государства в будущем страны, так как безработица молодёжи ведёт за собой ряды социальных проблем, таких, как, например, снижение рождаемости, разводы ввиду недостатка средств у молодых людей для обеспечения семьи, и многих других последствий.

Библиографический список

1. Всеобщая декларация прав человека - М.: Книга по Требованию, 2012. − 461 с.

2. Рофе, А.И. Экономика труда. Учебник / А.И. Рофе. — М.: КНОРУС, 2015. − 376 с.

3. Чернышева, Н.И. Пути решения проблемы молодежной безработицы в современном обществе // Известия Тульского государственного университета, 2015. − 155-160 с.

4. Закон РФ от 19.04.1991 №1032-1 (ред. От 28.12.2016) «О занятости населения в РФ», статья 3 «Порядок и условия признания граждан безработным», [Электронный ресурс] режим доступа: URL: http://www.consultant.ru/document/cons_doc.

5. «Росстат: Безработица среди молодежи в России достигает 30%» [Электронный ресурс] режим доступа: URL: http://www.examen.ru/news-and-articles.

[1] Статья: «Росстат: Безработица среди молодежи в России достигает 30%» [Электронный ресурс] - режим доступа: URL: http://www.examen.ru/news-and-articles/articles/rosstat-bezraboticza-sredi-molodezhi-v-rossii-dostigaet-30

[2] Чернышева Н.И. Пути решения проблемы молодежной безработицы в современном обществе // Известия Тульского государственного университета. 2015. №2-1. С. 155-160.

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ПЛАТЕЖЕСПОСОБНОСТИ ПРЕДПРИЯТИЙ НА СОВРЕМЕННОМ ЭТАПЕ

Кичаева Е., студент
Научный руководитель: к. э. н., доцент Журова Л.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Финансовая безопасность государства – основное условие его способности осуществлять самостоятельную финансово-экономическую политику в соответствии с национальными интересами. Уровень финансовой безопасности государства во многом определяется уровнем финансовой безопасности предприятий, работающих в реальном секторе экономики.

Одним из условий обеспечения финансовой безопасности предприятия является его платежеспособность. В экономической литературе существуют различные подходы к определению понятия платежеспособности, ряд из которых представлен в таблице 1.

Таблица 1 – Подходы к определению понятия «платежеспособность предприятия»

Автор	Определение
Бердникова Т.Б. [1]	Способность предприятия своевременно и в полном объеме произвести расчеты по краткосрочным обязательствам перед контрагентами
Ковалев В.В. [5]	Способность предприятия возместить кредиторскую задолженность при наступлении сроков платежа текущими поступлениями денежных средств
Петрова Л.В. [7]	Способность предприятия рассчитываться по своим долгосрочным обязательствам
Ухов И.Н. [9]	Способность предприятия к своевременному выполнению денежных обязательств, обусловленных законом или договором, за счет имеющихся в его распоряжении денежных ресурсов
Шеремет А.Д. [10]	Способность предприятия вовремя удовлетворять платежные требования поставщиков в соответствии с хозяйственными договорами, возвращать кредиты, производить оплату труда персонала, вносить платежи в бюджет и во внебюджетные фонды

Таким образом, платежеспособным является предприятие, способное вовремя и без нарушений договорных условий выполнять график погашения задолженности перед своими контрагентами.

Для оценки уровня платежеспособности используются различные показатели (таблица 2).

Таблица 2 – Показатели оценки платежеспособности предприятия

Автор	Показатели
Бланк И.А. [2]	Коэффициент абсолютной платежеспособности, коэффициент промежуточной платежеспособности, коэффициент текущей платежеспособности, общий коэффициент соотношения дебиторской и кредиторской задолженности, коэффициент соотношения дебиторской и кредиторской задолженности по коммерческим операциям
Ковалев В.В. [5]	Коэффициент текущей ликвидности, коэффициент быстрой ликвидности, коэффициент абсолютной ликвидности, коэффициент обеспеченности собственными оборотными средствами, доля собственных оборотных средств в покрытии запасов, коэффициент покрытия запасов, маневренность собственного капитала, маневренность собственных оборотных средств
Коваленко О.Г. [6]	Коэффициент текущей ликвидности, коэффициент критической ликвидности, коэффициент абсолютной ликвидности, коэффициент срочной ликвидности, коэффициент обеспеченности собственными средствами, коэффициент маневренности собственных оборотных средств
Шеремет А.Д. [10]	Коэффициент текущей ликвидности, коэффициент быстрой ликвидности, коэффициент абсолютной ликвидности, коэффициент общей платежеспособности

Как видно из таблицы, чаще всего для оценки платежеспособности используются коэффициенты ликвидности.

Уровень платежеспособности предприятия определяется различными факторами, в числе важнейших из которых – размер и динамикой дебиторской и кредиторской задолженности [4].

В таблице 3 представлена динамика дебиторской задолженности организаций Российской Федерации.

Таблица 3 – Динамика дебиторской задолженности организаций (без субъектов малого предпринимательства) Российской Федерации (на конец года, млрд руб.)

Год	Дебиторская задолженность	Из нее:	Из общего объема дебиторской задолженности	
		Просроченная	Задолженность покупателей и заказчиков	Из нее: Просроченная
2000	2451	916	1721	735
2001	3211	1007	2045	837
2002	3663	911	2263	715
2003	4139	877	2540	624
2004	5174	839	3010	607
2005	6331	856	3484	572
2006	7871	1040	4324	588
2007	11061	887	5807	627
2008	13783	1051	6966	797
2009	15442	1011	7505	756
2010	18004	1048	8589	805
2011	20797	1167	10121	925
2012	22867	1225	11824	946
2013	26264	1483	13420	1199
2014	31014	2016	16074	1635
2015	35736	2276	17259	1731
2016	37053	2241	18388	1544

Источник: Росстат. URL: http://www.gks.ru/free_doc/new_site/finans/dindz.htm

По данным таблицы 3 можно заметить, что в течение всего анализируемого периода дебиторская задолженность имеет тенденцию к росту. Резкое увеличение происходит в 2007 г. и 2013 г. как следствие начала финансовых кризисов в стране. Просроченная дебиторская задолженность резко увеличилась в 2014 г. поскольку вследствие финансового кризиса дебиторы не смогли вовремя погашать свои обязательства.

В таблице 4 представлена динамика кредиторской задолженности организаций Российской Федерации.

Таблица 4 – Динамика кредиторской задолженности организаций (без субъектов малого предпринимательства) Российской Федерации) (на конец года, млрд руб.)

Год	Кредиторская задолженность	Из нее: Просроченная
2000	3515	1571
2001	4231	1560
2002	4832	1433
2003	5283	1306
2004	5944	1122
2005	6389	956
2006	7697	821
2007	10653	833
2008	13353	994
2009	14882	958
2010	17683	1006
2011	20954	1208
2012	23632	1188
2013	27532	1470
2014	33174	1881
2015	38925	2429
2016	42280	2656

Источник: Росстат. URL: http://www.gks.ru/free_doc/new_site/finans/dinkz.htm

Данные таблицы 4 показывают резкое увеличение кредиторской задолженности в 2007 г. и 2014 г. (как следствие начала финансового кризиса). Снижение денежных поступлений от покупателей за реализованную продукцию (товары, работы, услуги) не позволили организациям вовремя отвечать по обязательствам перед государством и контрагентами.

Уровень платежеспособности предприятий во многом определяется их отраслевой спецификой. В таблице 5 представлены показатели платежеспособности предприятий химической отрасли (ПАО «КуйбышевАзот»), нефтегазовой отрасли (ПАО НК «РОСНЕФТЬ»), отрасли автомобилестроения (ПАО «АВТОВАЗ»).

Таблица 5 – Показатели платежеспособности предприятий за 2015-2017 гг. (источник: данные финансовой отчетности предприятий)

Предприятие	31.12.2015 г.			31.12.2016 г.			30.09.2017 г.		
	Ктл	Кал	Косос	Ктл	Кал	Косос	Ктл	Кал	Косос
ПАО «КуйбышевАзот»	1,7	0,2	0,41	1,57	0,13	0,36	1,78	0,16	0,44
ПАО НК«РОСНЕФТЬ»	1,32	0,31	0,26	0,83	0,28	-0,39	0,52	0,06	-0,91
ПАО «АВТОВАЗ»	0,41	0,05	-1,43	0,52	0,15	-0,92	0,53	0,05	-0,99

Обозначения, используемые в таблице: Ктл – коэффициент текущей ликвидности, Кал – коэффициент абсолютной ликвидности, Косос – коэффициент обеспеченности собственными оборотными средствами.

Как видно из данных таблицы 5, коэффициент текущей ликвидности ни одного предприятия не достиг нормативного значения (≥ 2). ПАО «КуйбышевАзот» имеет наибольшие значения данного коэффициента на протяжении всего анализируемого периода, однако рост показателя в 2017 г. во многом обусловлен ростом дебиторской задолженности.

Коэффициент абсолютной ликвидности имеет норматив $\geq 0{,}25$. В 2015 г. предприятия химической и нефтегазовой отраслей достигли этого значения, на 30.09.2017 г. значения данного коэффициента у всех предприятий ниже нормативного.

Снижение показателей текущей и абсолютной ликвидности ПАО НК «РОСНЕФТЬ» на конец анализируемого периода обусловлено значительным ростом кредиторской задолженности.

Значения показателей текущей и абсолютной ликвидности ПАО «АВТОВАЗ» за весь период значительно ниже нормативных, что свидетельствует о невозможности покрытия краткосрочных обязательств за счет оборотных активов.

Коэффициент обеспеченности собственными оборотными средствами является показателем, свидетельствующим о возможности предприятия осуществлять финансирование текущей деятельности собственными средствами. Нормативом является значение $\geq 0{,}1$. На протяжении всего анализируемого периода значения данного показателя у ПАО «АВТОВАЗ» имеют отрицательные значения, что является следствием дефицита собственных оборотных средств – оборотные активы формируются за счет заемных средств. У ПАО НК «РОСНЕФТЬ» данный показатель имеет отрицательные значения на 31.12.2016 г. и 30.09.2017 г. Ухудшение платежеспособности нефтяной компании обусловлено сокращением денежных поступлений от реализации продукции (за счет снижения продаж нефти, а также снижения мировых цен на нефть).

Механизмы обеспечения платежеспособности предприятия включают в себя механизмы по управлению дебиторской задолженностью и кредиторской задолженностью.

Управление дебиторской задолженностью на предприятии связано, в первую очередь, с оптимизацией размера и обеспечением инкассации задолженности покупателей по расчетам за реализованную продукцию. В целях эффективного управления этой дебиторской задолженностью на предприятиях должна разрабатываться и осуществляться особая финансовая политика управления дебиторской задолженностью (или его кредитная политика по отношению к покупателям продукции). Политика управления дебиторской задолженностью представляет собой часть общей политики управления оборотными активами и маркетинговой политики предприятия, направленной на расширение объема реализации продукции и заключающейся в оптимизации общего размера этой задолженности и обеспечении своевременной ее инкассации (погашения) [8].

Управление кредиторской задолженностью представляет собой часть общей политики управления оборотными активами и маркетинговой политики предприятия, которая направлена на расширение объема реализации продукции с целью оптимизации общего размера этой задолженности [3]. Важнейшим направлением сокращения расходов является определение оптимальной структуры оплаты товаров и услуг для каждого конкретного случая, включающей в себя: составление бюджета и схемы кредиторской задолженности; оценку финансовых возможностей, вероятных рисков и степени доверия в отношениях с кредиторами.

Таким образом, платежеспособность является одним из важнейших условий финансовой безопасности предприятий, обеспечивающих защиту приоритетных финансовых интересов предприятия от внешних и внутренних угроз.

Библиографический список

1. Бердникова, Т.Б. Анализ и диагностика финансово-хозяйственной деятельности предприятия: учебное пособие // – М.: ИНФРА-М, 2016. – 224 с.
2. Бланк, И.А. Управление финансовой безопасностью предприятия. – 3-е изд., стер. – К.: Эльга, 2013. – 776 с.
3. Емелин, В.Н., Пивкина, Е.И. Управление кредиторской задолженностью организации // Молодой ученый. — 2016. — №14. — С. 465-467. URL: https://moluch.ru/archive/67/11238/
4. Каранина, Е.В. Финансовая безопасность (на уровне государства, региона, организации, личности). Монография. – Киров: ФГБОУ ВО«ВятГУ», 2015. – 239 с.
5. Ковалев, В.В. Финансовый анализ: методы и процедуры: учебное пособие.– М.: Финансы и статистика, 2015. – 260 с.
6. Коваленко, О.Г. Анализ и оценка платежеспособности организации // Современные научные исследования и инновации. 2016. № 11 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2016/11/74037
7. Петрова, Л.В., Игнатущенко, Н.А., Фролова, Т.П. Анализ и диагностика финансово-хозяйственной деятельности: учебное пособие для вузов. – М.: Издательство Московского государственного открытого университета, 2015. – 179 с.
8. Макрушина, Л.С. Управление дебиторской и кредиторской задолженностью предприятия // Студенческий: электронный научный журнал. – 2017. – № 18 (18).
9. Ухов, И.Н. Виды платежеспособности и способы ее оценки // Менеджмент в России и за рубежом. – 2016. – № 5. – С. 8–18.
10. Шеремет, А.Д., Негашев, Е.В. Методика финансового анализа деятельности коммерческих организаций: практическое пособие //– 2-е изд., перераб.и доп. – М.: ИНФРА-М, 2012. – 208 с.
11. [Электронный ресурс]. URL: http://info.avtovaz.ru/ Официальный сайт ПАО «АВТОВАЗ».
12. [Электронный ресурс]. URL: http://www.kuazot.ru/ Официальный сайт ПАО «КуйбышевАзот».
13. [Электронный ресурс]. URL: https://www.rosneft.ru/ Официальный сайт ПАО «НК «РОСНЕФТЬ».
14. [Электронный ресурс]. URL: http://www.uacrussia.ru/ Официальный сайт ПАО «ОАК».

ФОРМИРОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ДЛЯ ПРЕДПРИЯТИЯ

Мелёхин Д.М., студент
Научный руководитель: д. э. н., профессор Глухова Л.В.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Обеспечение экономической безопасности предприятия, её способность противодействовать как внешним, так и внутренним угрозам является одним из основных условий перехода предприятия к устойчивому развитию. Под угрозой безопасности предприятия следует понимать потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности. Угрозу можно классифицировать по различным показателям и измерить их в количественных параметрах. Например, возможный ущерб оценивается числом погибших людей, потерявших (ухудшивших) здоровье, денежной сумме экономических потерь и т.д. По степени вероятности угроза оценивается как невероятная, маловероятная, вероятная, весьма вероятная и вполне вероятная. По степени развития угроза проходит четыре этапа: возникновение (зарождение), экспансия, стабилизация и ликвидация. Отдаленность угрозы во времени определяется как непосредственная, близкая (до 1 года) и далекая (свыше 1 года), а отдаленность в пространстве — территория предприятия, прилегающая к предприятию территория, территория региона, территория страны, зарубежная территория. Темпы нарастания угрозы измеряются по месяцам, кварталам, годам.

Под объектом безопасности предприятия следует понимать степень устойчивости и развития предприятия, его способность противостоять угрозам. В объекты безопасности предприятия можно выделить: различные структурные подразделения или группы сотрудников, либо владельцы акций

предприятия; ресурсы предприятия (информационные, кадровые, материально-технические, информационные, интеллектуальные и финансовые); различные виды деятельности (управленческая, производственная, снабженческая и т.д.).

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Достижение этой цели требует реализации следующих задач:

выявление угроз для стабильности и развития предприятия и выработка мер по их противодействию; обеспечение защиты технологических процессов; реализация мер противодействия всех видов шпионажа (промышленного, научно-технического, экономического и т.д.); всестороннее изучение деловых партнеров; разработка и совершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия; реализация мер по защите коммерческой и иной информации; реализация мер по защите интеллектуальной собственности.

Обеспечением безопасности предприятия занимаются две группы субъектов. Первая группа занимается этой деятельностью непосредственно на предприятии и подчинена его руководству. Среди этой группы можно выделить специализированные субъекты (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, спасательная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетенции). Другую часть субъектов этой группы условно можно назвать полуспециализированной, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.). К третьей части этой группы субъектов относится весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности. Следует иметь в виду, что эффективно обеспечивать безопасность предприятия эти субъекты могут только в том случае, если цели, задачи, функции, права и обязанности будут распределены между ними таким образом, чтобы они не пересекались друг с другом.

Среди существующих средств обеспечения безопасности можно выделить следующие:

1. Технические средства. К ним относятся охранно-пожарные системы, видео-радиоаппаратура, средства обнаружения взрывных устройств, заграждения и т.д.

2. Организационные средства. Создание специализированных организационно-структурных формирований, обеспечивающих безопасность предприятия.

3. Информационные средства. Прежде всего, это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Кроме этого, важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах.

4.Финансовые средства. Без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей.

5. Правовые средства. Использование не только изданных вышестоящими органами власти законов и подзаконных актов, но также разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности.

6. Кадровые средства. Достаточное количество кадров, занимающихся вопросами обеспечения безопасности. Одновременно с этим решают задачи повышения их профессионального мастерства в этой сфере деятельности.

7. Интеллектуальные средства. Привлечение к работе квалифицированных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

Следует заметить, что применение каждого из вышеуказанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе.

Необходимо иметь в виду, что наиболее полное представление о системе безопасности предприятия можно получить после изучения официально принятых документов по концепции безопасности предприятия, комплексной программы обеспечения безопасности предприятия и планов подразделений предприятия по реализации этой программы. Сформированная на научной основе система безопасности предприятия является организационной основой создания ее структурного подразделения — службы безопасности.

Библиографический список

1. Александрова, А.И. Инновационная диверсификация бизнеса в системе управления экономической безопасностью предприятия // Науч. журн. НИУ ИТМО. Сер.: Экономика и экол. менеджмент. - 2014. - № 1. - С. 186.

2. [Электронный ресурс] - Режим доступа: [http://economics.ihbt.ifmo.ru/ru/article/8816/innovacionnaya_diversifikaciya_biznesa_v_sisteme_upravleniya_ekonomicheskoy_bezopasnostyu_predpriyatiya.htm]

3. Короткова, А.В. Инструменты контроля и их роль в экономической безопасности бизнеса // Инновац. развитие экономики. - 2014. - № 2. С. 252.

4. Собин, О.А. Вопросы обеспечения государством экономической безопасности малого бизнеса // Экономика и упр. в XXI веке: тенденции развития. - 2012. - № 5. - С. 236.

5. Байдина, М.Б. Производственные показатели для оценки и анализа экономической безопасности / М.Н. Волкова, М.Б. Байдина // Концепт. Спецвыпук «Актуальные вопросы экономики и менеджмента». – 2014. - №12.

ИНДЕКС ЧЕЛОВЕЧЕСКОГО РАЗВИТИЯ КАК ВАЖНЕЙШИЙ ПОКАЗАТЕЛЬ ХАРАКТЕРИСТИКИ НАЦИОНАЛЬНОЙ ЭКОНОМИКИ

Руденко А.С., студент
Научный руководитель: д. э. н., профессор Щукина А.Я.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Показателем, играющим важную роль в анализе реализации устойчивого развития, является творческий фактор (интеллектуальная деятельность человека). В этом факторе солидную долю занимает индекс человеческого развития.

Индекс человеческого развития — это совокупный показатель уровня развития человека в стране, поэтому иногда его используют в качестве синонима таких понятий как «качество жизни» или «уровень жизни». Индекс измеряет достижения страны с точки зрения состояния здоровья, получения образования и фактического дохода ее граждан, по трем основным направлениям:

1. Здоровье и долголетие, измеряемые показателем ожидаемой продолжительности жизни при рождении;
2. Доступ к образованию, измеряемый уровнем грамотности взрослого населения и совокупным валовым коэффициентом охвата образованием;
3. Достойный уровень жизни, измеряемый величиной валового внутреннего продукта (ВВП) на душу населения в долларах США по паритету покупательной способности (ППС).

Эти три измерения стандартизируются в виде числовых значений от 0 до 1, среднее геометрическое которых представляет собой совокупный показатель ИЧР в диапазоне от 0 до 1. Затем государства ранжируются на основе этого показателя. Все страны в рейтинге классифицируются четырьмя категориями:

1. Страны с очень высоким уровнем ИЧР;
2. Страны с высоким уровнем ИЧР;
3. Страны со средним уровнем ИЧР;
4. Страны с низким уровнем ИЧР.

ИЧР состоит из трех равнозначных компонентов:

1) дохода, определяемого показателем валового внутреннего продукта (валового регионального продукта) по паритету покупательной способности (ППС) в долларах США;

2) образования, определяемого показателями грамотности (с весом в 2/3) и доли учащихся среди детей и молодежи в возрасте от 6 до 23 лет (с весом в 1/3);

3) долголетия, определяемого через продолжительность предстоящей жизни при рождении (ожидаемую продолжительность жизни)[1].

Частные индексы рассчитываются по следующей формуле:

$$I_i = X_i – X_{i\,min} / X_{i\,max} - X_{min} \quad (1)$$

где, X_i – это фактическое значение показателя;

[1] Программа развития ООН: Индекс человеческого развития в странах мира в 2015 году. URL:http://gtmarket.ru/news/2015/12/16/7285 (дата обращения: 23.10.2017)

$X_{i\,min}$ – минимальное значение показателя;

$X_{i\,max}$ – максимальное значение показателя.

Индекс продолжительности жизни определяется по формуле:

$I_e = e_0^0 - 25 / 85 - 25$ (2)

где, e_0^0 – фактическая средняя продолжительность предстоящей жизни при рождении.

При расчете индекса валового регионального продукта (ВРП) в формулу подставляются не сами значения, а их логарифмы:

$I_{ВРП} = \ln X_{ВРП} - \ln 100 / \ln 40000 - \ln 100$ (3)

где, $X_{ВРП}$ – величина реального ВРП на душу населения в долл. США по паритету покупательной способности (ППС).

Индекс достигнутого уровня образования (образованности) определяется по формуле:

$I_{обр} = (2/3 * I_{грамм}) + (1/3 * I_{уч})$ (4)

где, $I_{грам}$ – индекс грамотности взрослого населения;

$I_{уч}$ – индекс совокупной доли учащихся;

2/3, 1/3 – весовые коэффициенты.

Индексы грамотности взрослого населения и совокупной доли учащихся определяются по формулам:

$I_{грамм} = X_{грамм} - 0 / 100 - 0$ (5)

$I_{уч} = X_{уч} - 0 / 100 - 0$ (6)

где, $X_{грам}$ – фактическая грамотность взрослого населения;

$X_{уч}$ – фактическая совокупная доля учащихся.

ИЧР представляет собой среднее арифметическое индекса продолжительности жизни I_e, индекса достигнутого уровня образования $I_{обр}$ и индекса ВРП $I_{ВРП}$:

$ИЧР = I_e + I_{обр} + I_{ВРП} / 3$ (7)

где, I_e – индекс ожидаемой продолжительности жизни при рождении;

$I_{обр}$ – индекс достигнутого уровня образования;

$I_{ВРП}$ – индекс реального ВВП в расчете на душу населения.

Рассчитаем ИЧР для населения России за 2016 год. Некоторые фактические значения показателей, такие как, величина реального ВВП на душу населения, фактическая грамотность взрослого населения, средняя продолжительность жизни и т.д., можно взять в статистических справочниках.

Основные показатели России таковы: средняя ожидаемая продолжительность жизни при рождении — 70,93 лет; средняя продолжительность получения образования — 14,7 лет; валовой национальный доход на душу населения — 11 400$ в год.

Для расчета ИЧР необходимо вывести три индекса: индекс продолжительности жизни, индекс ВВП и индекс образованности взрослого населения.

1. Индекс продолжительности жизни. В формулу подставляет значение фактической средней продолжительности жизни:

$I_e = 70{,}93 - 25 / 85 - 25 = 0{,}766$ (8)

2. Индекс достигнутого уровня образования (образованности). Для выведения индекса образованности нужно получить еще два дополнительных индекса: Индекс грамотности и Индекс совокупной доли учащихся.

Индекс грамотности составляет 0,994

Индекс совокупной доли учащихся равен 0,71

Отсюда выводится индекс образованности, по формуле:

$I_{обр} = (2/3 * 0{,}994) + (1/3 * 0{,}71) = 0{,}9$ (9)

3. Индекс ВВП (ВРП). Вычисляется по формуле.

$I_{ВРП} = \ln 11\,400 - \ln 100 / \ln 40\,000 - \ln 100 = 0{,}790$ (10)

Индекс ВРП составил 0,790

И, наконец, индекс человеческого развития. Он представляет собой среднее арифметическое этих трех индексов и составляет для России:

$ИЧР = (0{,}766 + 0{,}9 + 0{,}790) / 3 = 0{,}819$ (11)

Из этого следует, что Россия по этому показателю занимает позицию немного выше стран с высоким уровнем ИЧР в рейтинге за 2015 год[1].

[1] Доклад о человеческом развитии 2016. URL:http://hdr.undp.org/sites/default/files/HDR2016_RU_Overview_Web.pdf (дата обращения: 27.10.2017)

Таблица 1 – Рейтинг стран с очень высоким уровнем человеческого развития

Страны с очень высоким уровнем человеческого развития		
Место	Страна	Индекс
1	Норвегия	0,949
2	Австралия	0,939
3	Швейцария	0,939
4	Германия	0,926
5	Дания	0,925
…	…	…
49	Российская Федерация	0,804
51	Кувейт	0,800

В таблице видно, что Россия находится внизу рейтинга, индекс страны составил 0,804 в 2015 году, а по результатам расчётов выше ИЧР РФ составил 0,819, что говорит о повышении человеческого развития.

Индекс человеческого развития ценен, на данный момент, в связи с мировой потребностью в инновациях. Чем выше уровень человеческого развития в какой-либо стране, тем больше потенциал создания инновационных технологий.

Например, первое место в рейтинге Глобального индекса инновационного развития занимает Швейцария[1]. В данной стране постоянно повышается качество товаров и услуг с помощью разработок, в которые инвестирует государство или частный сектор. Также имеются ВУЗы мирового уровня, в которых проводятся исследования в данном направлении. Правовая система имеет либеральный характер и обеспечивает полную защиту интеллектуальной собственности.

В Швеции большинство предприятий постоянно внедряют какие-либо инновационные разработки, повышая тем самым эффективность производства и снижая потребление не возобновляемого топлива.

И в многих других развитых странах процветает инновационная деятельность, происходит финансирование и стимулирование бизнеса в сфере передовых технологий.

В развивающихся странах положение дел немного меняется. Регионы так же стремятся к внедрению новейших технологий в производство, но инновации не несут в них повсеместный характер. Для примера рассмотрим Россию.

В Российской Федерации инновационная деятельность носит региональный характер. Это связано с неравномерным развитием субъектов страны. Рассмотрим выборку из рейтинга социально-экономического положения субъектов РФ по итогам 2016 года.

Таблица 2 – Регионы из рейтинга социально-экономического положения субъектов РФ по итогам 2016 года[2]

Субъекты	Место	Рейтинг
г. Москва	1	80,891
г. Санкт-Петербург	2	74,541
Самарская область	12	57,388
Воронежская область	17	54,946
Республика Тыва	84	15,439
Еврейская автономная область	85	13,139

Благодаря выборке видно, что субъекты Российской Федерации сильно различаются между собой по уровню социально-экономического развития.

Рассмотрим данные регионы в инновационной направленности.

В Москве находится примерно 300 тысяч исследователей, работающих на инновационных предприятиях, в ведущих университетах. Увеличивается число сегментов экономики в инновационной промышленности. Стоит отметить Курчатовский институт, являющийся «Системообразующим элементом инновационного комплекса России». В нём сформирован научно-технический комплекс с

[1] Эксперты ООН назвали самые инновационные страны мира. URL:https://www.rbc.ru/economics/16/08/2016/57b3082f9a7947a29e68c136http://www.rbc.ru/economics/16/08/2016/57b3082f9a7947a29e68c136 (дата обращения: 27.10.2017)

[2] Рейтинг социально-экономического положения субъектов РФ по итогам 2016 года. URL: http://riarating.ru/infografika/20170530/630063754.html (дата обращения: 28.10.2017)

уникальной исследовательско - технологической базой, состоящей из: ускорительных комплексов, исследовательских реакторов, плазменных установок, установок для развития ядерных технологий[1].

В Санкт-Петербурге осуществляется деятельность больше 50 организаций, входящих в инновационную инфраструктуру (технопарки, инжиниринговые центры, инвестиционные фонды, федеральные институты развития и т.д.). В городе сконцентрировано более 10% потенциала страны в научной сфере, который состоит из свыше 350 научных организаций.

Самарская область отличается инновационной деятельностью, направленной на полное аэрокосмическое производство. Также в данном регионе происходит модернизация оборудования, направленного на производство автомобилей. Что же касается научной сферы деятельности, то в области находятся 29 вузов, 61 научно-исследовательская организация, которые составляют основу научного потенциала региона[2].

В Воронежской области инновационная инфраструктура состоит из 5 технопарков, 4 индустриальных парков, 6 бизнес – инкубаторов, 1 технологической платформы, 5 территориальных кластеров, 7 инжиниринговых центров и т.д. Деятельность в сфере инноваций в данной области очень разнообразна, начиная от пищевой промышленности, заканчивая авиационными разработками[3].

В Республике Тыва инновационная деятельность имеет ослабленный характер. Это обусловлено тем, что в данном регионе только планируется внедрение современных достижений науки и создание необходимых правовых и инфраструктурных условий для развития инновационной деятельности[4].

В Еврейской автономной области существует программа по улучшению качества образования. На 2016 год доля, приходящаяся на обучающихся в образовательных организациях по новым государственным стандартам, составила 64,1%, в 2021 году планируется повышение доли обучающихся до 96%, что способствует развитию инновационной деятельности региона.

В связи с тем, что инновационная экономика является завещающим этапом переходной экономики России, то приоритетной задачей экологоориентированного экономического развития должно стать выравнивание уровня социально- экономического положения регионов РФ.

Библиографический список

1. Доклад о человеческом развитии 2016.[Электронный ресурс]. Режим доступа: http://hdr.undp.org/sites/default/files/HDR2016_RU_Overview_Web.pdf ., свободный.

2. Инфраструктура инновационной деятельности. [Электронный ресурс]. Режим доступа: http://econom.govvrn.ru/its/infrastruktura-innovatsionnoy-deyatelnosti., свободный.

3. Национальный исследовательский центр "Курчатовский институт". [Электронный ресурс]. Режим доступа: http://nrcki.ru/., свободный.

4. Обрабатывающие производства и инновации. [Электронный ресурс]. Режим доступа: http://www.mert.tuva.ru/directions/innovation/., свободный.

5. Программа развития ООН: Индекс человеческого развития в странах мира в 2015 году. [Электронный ресурс]. Режим доступа: http://gtmarket.ru/news/2015/12/16/7285., свободный.

6. Рейтинг социально-экономического положения субъектов РФ по итогам 2016 года. [Электронный ресурс]. Режим доступа: http://riarating.ru/infografika/20170530/630063754.html., свободный.

7. Самара: Инновационная активность в регионе. [Электронный ресурс]. Режим доступа: http://ingriastartup.ru/novosti/lenta_novostej/samara/., свободный.

8. Эксперты ООН назвали самые инновационные страны мира. [Электронный ресурс]. Режим доступа:https://www.rbc.ru/economics/16/08/2016/57b3082f9a7947a29e68c136http://www.rbc.ru/economics/16/08/2016/57b3082f9a7947a29e68c136., свободный.

[1] Национальный исследовательский центр "Курчатовский институт". URL: http://nrcki.ru/ (дата обращения: 29.10.2017)

[2] Самара: Инновационная активность в регионе. URL: http://ingria-startup.ru/novosti/lenta_novostej/samara/ (дата обращения: 01.11.2017)

[3] Инфраструктура инновационной деятельности. URL:http://econom.govvrn.ru/its/infrastruktura-innovatsionnoy-deyatelnosti (дата обращения: 01.11.2017)

[4] Обрабатывающие производства и инновации. URL: http://www.mert.tuva.ru/directions/innovation/ (дата обращения: 01.11.2017)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

Елкина В., студент
Научный руководитель: к. п. н., доцент Исакова Т.Б.
ОАНО ВО «Волжский университет имени В.Н. Татищева» (институт)
г. Тольятти, Россия

Термин «информационная война» появился в середине 80-х гг. XX в. в работах американских военных теоретиков и начал широко применяться после проведения операции «Буря в пустыне» в 1991 г. Считалось, что войны XXI в. будут по преимуществу информационными, а основными средствами их ведения станут средства массовой информации.

Существует множество определений понятия информационной войны. Так, Г.Г. Почепцов подразумевает под информационной войной «коммуникативную технологию по воздействию на массовое сознание с кратковременными и долговременными целями». В новом армейском уставе США информационная война определяется как «действия, предпринятые для достижения информационного превосходства в интересах национальной стратегии и осуществляемые путем влияния на информационные системы противника при одновременной защите собственной информации и своих информационных сетей».

Две принципиально различные сферы функционирования информации – техническая и гуманитарная – задают соответствующие направления, где формируются возможности информационного оружия. В результате создаются два варианта информационных технологий: технические и гуманитарные (социальные).

Основными формами ведения технической информационной войны являются радиоэлектронная борьба, война с использованием средств электронной разведки и наведения, борьба с хакерами, кибернетическая война.

Гуманитарные технологии информационной войны – это любые средства, сознательно используемые для воздействия на разум противника с минимальной физической силой и таким образом, чтобы иметь высокую вероятность заставить противника выполнить чужое желание. Таким образом, принципиальное отличие информационного оружия от обычного в том, что оно воздействует на разум, а не на тело человека. В результате применения информационного оружия объект воздействия (человек, социальная группа, народ) начинает совершать действия, идущие в разрез с его собственными интересами и отвечающими интересам противника.

Информационное оружие применялось с давних пор. Например, орды Чингиз-Хана стимулировали распространение слухов, что если город не сдается – пощады не будет никому.

Но на современном этапе использование информационного оружия приобрело особую актуальность. Его возможности совпали с возможностями нового этапа развития цивилизации – информационного общества, который характеризуется тем, что информация играет важнейшую роль практически во всех сферах жизни.

Кроме того, информационная война обладает для ведущей ее стороны целым рядом преимуществ по сравнению с обычной войной, в частности:

- война ведется в «белых перчатках». Агрессора, как правило, невозможно обвинить в уничтожении людей;
- информационная война не регламентирована международным правом;
- ведение информационной войны стоит дешевле, чем ведение обычной войны;
- развязывание информационной войны гораздо менее опасно для страны-агрессора и ее граждан, чем развязывание традиционной войны. Люди обычно не в состоянии реагировать на невидимое воздействие. Более того, это воздействие может облекаться в доброжелательную форму, на которую даже чисто биологически человек не готов отвечать агрессивно. Факт и последствия ведения информационной войны не всегда являются очевидными для тех, против кого она ведется. Таким образом, отсутствие видимых разрушений, характерных для войн обычных, можно признать главной опасностью информационной войны. Население даже не ощущает, что подвергается воздействию. В результате общество не приводит в действие имеющиеся в его распоряжении защитные механизмы;
- эффект зачастую достигается гораздо больший, чем с помощью обычного оружия. Применение технологий информационной войны может вызвать нарушение социально-экономических про-

цессов и привести к гибели государства. При этом народ оказывается деморализованным и неспособным к сопротивлению. Например, развал сверхдержавы СССР произошел в результате поражения в «холодной войне», которая была в значительной мере информационной войной. Государственный переворот в современной Украине.

Вследствие осознания возможностей информационного оружия, появился термин Strategic Information Warfare - «стратегическое информационное противоборство». Такое противоборство представляет собой «использование государствами глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и уменьшения воздействия на собственный информационный ресурс».

Проведенные исследования позволили выделить следующие ключевые особенности информационного противоборства (ИП): сравнительно низкая стоимость создания средств ИП; крушение статуса традиционных государственных границ при подготовке и проведении информационных операций; изменение приоритетов в деятельности стратегической разведки, которые смещаются в область завоевания и удержания информационного превосходства; усложнение проблем обнаружения начала информационной операции; сложность создания коалиции против агрессора, развязавшего информационную войну.

По мнению специалистов ИП направлено на решение следующих задач:

- создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию противника;
- манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания недоверия, подозрительности, обострения политической борьбы, провоцирование репрессий против оппозиции и даже гражданской войны;
- снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений;
- инициирование забастовок, массовых беспорядков и других акций экономического протеста;
- затруднение принятия органами управления важных решений;
- подрыв международного авторитета государства, его сотрудничества с другими странами;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

У современного человека есть возможность оперативно получать огромный объем информации со всего света. Но, как правило, это та информация, которая поступает через средства массовой информации. Человек видит мир глазами СМИ, в его голове формируется такая картина действительности, которую предлагают ему СМИ. В таких условиях появляются огромные возможности по манипулированию массовым сознанием, созданию мифов. Находясь часто в мире оторванных от реальности символов, люди могут идти даже против своих собственных интересов.

Актуальной становится необходимость разработки систем и способов психологической защиты от патогенных информационных технологий. Е.Е. Пронина считает, что функцию психологической защиты призвана выполнить медиапсихология, включающая три взаимосвязанных направления: медиааналитика, медиатерапия, медиаобразование.

В задачи медиатерапии входит:

- профилактика и реабилитации информационных травм аудитории;
- психологическое восстановление посредством массовой коммуникации;
- стабилизация психических состояний;
- формирование адекватных контролируемых реакций;
- содействие национальной самоиденфикации и личностному самоопределению индивидов.

Расширение знаний аудитории об основных приемах воздействия СМИ и современных коммуникативных технологиях повышает информационно-психологическую защищенность участников массовой коммуникации, а это задача медиаобразования.

Если говорить о журналистах – очевидно, в условиях информационной войны для них важнее всего не стать слепыми исполнителями чужой воли, стараться, чтобы деятельность СМИ отвечала интересам своей страны.

Библиографический список

1. Вартанова, Е.Л. Глобализация информационных потоков как фактор антитерроризма // Журналистика и СМИ против террора. – М., 2009. – С. 144 – 167.
2. Исакова, Т.Б. Международное гуманитарное право и средства массовой информации: учебно-методическое пособие. – Тольятти, 2011. – 154с.
3. Пронина, Е.Е. Медиапсихологический подход к анализу угрозы терроризма // Журналистика и СМИ против террора. – М., 2009. – С. 168 – 192.
4. Пронина, Е.Е. Психологические особенности творческой работы репортеры. – М., 2001.

НАСКОЛЬКО СОЦИУМ ГОТОВ К ОСМЫСЛЕНИЮ ПОНЯТИЯ МОРАЛЬНО-НРАВСТВЕННОЙ ЦЕНЗУРЫ?

Сердюкова А.С., соискатель
Научный руководитель: д-р пед. наук, доцент Ронжина Н.В.
Российский государственный профессионально-педагогический университет
г. Екатеринбург, Россия

Если не противиться привычке –
она становится необходимостью…
Августин Блаженный

В статье осуществлен анализ понятия «цензура», его использование в современной политической лексике, а также в Конституции Российской Федерации, которое сегодня не воспринимается как научное. Это предопределяет наличие целого ряда противоречий в социокультурных практиках. Актуальность обращения к сущности сложившихся противоречий связана с расширением спектра нравственно-этических девиаций, постепенно захватывающих наше общество. Это касается принимаемой многими гражданами (особенно молодежью) и средствами массовой информации допустимости балансирования на грани цинизма и допустимостью в презентации интимных сторон жизни людей, норм русского языка и их извращением, а также навязыванием под лозунгом толерантности образцов поведения, предопределяющих вырождение социума. Анализ структур, занимающихся информационной безопасностью в пространстве Интернета, показал активную работу общественных и государственных структур предотвращающих преступные действия правонарушителей. Автор убежден, что возникающие трудности разрешимы в условиях возврата «генетической памяти» нашего народа к традиционным нравственно-этическим ценностям, которые существовали в тесной взаимосвязи православной культуры с многовековой историей русского народа.

Ключевые слова: морально-нравственная цензура; право; совесть.

Анализируя понятие «цензура», был выявлен с ряд важных противоречивых моментов. С одной стороны, мы имеем известную формулировку о запрете цензуры в Конституции Российской Федерации [3]. С другой стороны, мы видим, что в сфере информационной безопасности в обществе действуют структуры, имеющие право на запрет той или иной информации, которая доносится до потребителей услуг системы Интернет. Так, по данным Роскомнадзора с 2012 по 2016 гг. проанализированы 273500 жалоб граждан и организаций, проанализированы 13500 судебных решений о признании той или иной информации запрещенной [2]. Оказывается, имеется более 20 категорий, которые позволяют отнести тот или иной вид информации к несущему угрозу обществу (экстремистские, пропагандирующие проституцию и наркотики, способствующие совершению экономических преступлений, популяризирующие способы изготовления взрывчатых веществ и прочие материалы).

Глава Роскомнадзора А.А. Жаров, описывая роль Единого реестра запрещенной информации (ЕРЗИ), действующего в рамках Роспотребнадзора, констатирует, что «на основании решения суда в ЕРЗИ было внесено более 114000 интернет страниц и доменных имён с противоправным контентом». Сегодня блокируется «около 24000 интернет – страниц. Доля блокировок, т.е. тех ресурсов, которые не удаляют противоправную информацию, стабильно располагается в районе 20% от всех сайтов, на которых выявлен противоправный контент» [2].

Сегодня параллельно с Роспотребнадзором действует Лига безопасного интернета (ЛБИ). Эта структура, как отмечает К.В. Малофеев, активно обращается к услугам так называемых «кибердружинников», с помощью которых за последние 5 лет «заблокировано более 10000 сайтов и страниц с детской порнографией и ее пропагандой (возбуждено более 800 уголовных дел, раскрыто 30 дел, связанных с производителями детской порнографии)», более 3000 – с пропагандой и рекламой продажи

наркотиков, более 1000 – с популяризацией самоубийств). «За время существования экспертного центра ЛБИ проведено около 1000 исследований; возбуждено более 300 дел; вынесено более 3 000 решений о внесении URL в Реестр запрещенных сайтов; проведено около 250 судебных экспертиз» [4].

Таким образом, государством осуществляются определенные меры безопасности информационного интернет – пространства по предотвращению преступных действий социумом. А вот вопрос по обеспечению информационной безопасности на уровне сохранности национального языка, духовной-нравственной культуры остается открытым.

Так, ученые-юристы из СПбГУ (С.А. Белов, М.Н. Кропачев, М.А. Ревазов и др.) провели исследование, связанное с проблемами выявления контроля за соблюдением норм современного русского языка в процессе судебного контроля, и пришли к выводу о том, что это поле нуждается в серьезной корректировке: отсутствуют источники, на основании которых суды могли бы выносить объективные решения о нарушениях языковых норм. Те базы, к которым рекомендовано обращаться, не содержат перечня отклонений от нормы. В то же время норма, казалось бы, представлена в словарях и справочниках, рекомендованных Министерством образования РФ. В то же время рекламная, аудиовизуальная и даже представленная в официальных документах ненормативная, жаргонная лексика, противоречащая нормам русского языка, не всегда может получить нормативно-правовую оценку, так как отсутствуют разъяснение по «антинормам» [1].

В связи с этим считаем целесообразным предложение о создании общественных и официальных структур, исполняющих экспертные функции при оценке допустимости и недопустимости использования национального языка, а также при оценке нарушений нравственно-этического базиса современного российского общества. Для правового регулирования предлагаем обратиться к недостаточно освоенному в актуальных научных дискурсах понятию «каноническое право»[6], так как оно не ограничивается регламентом внутрицерковной организации, а обращаясь к правоотношениям (вытекающим из частного гражданского, судебного, уголовного и процессуального права), большое внимание уделяет именно бережному, внимательному отношению к «слову» и духовно-нравственному воспитанию людей.

Выбранная исследователем тема была с давних времен известна обществу в связи с постоянно изменяющимися условиями развития общества, актуальна эта тема и сегодня. Так, Аристотель писал: *«Разумно отстранить от ушей и глаз детей…все то, что не соответствует достоинству…законодатель должен удалить из государства сквернословие…потому что из привычки сквернословить развивается и склонность к совершению дурных поступков…в особенности у молодых…раз мы не допускаем в государстве подобных слов, то, очевидно, не дозволяем также смотреть непристойные картины или представления»* [5].

Библиографический список

1. Белов, С.А., Кропачев, М.Н., Ревазов, М.А. Судебный контроль за соблюдением норм современного русского литературного языка // Закон. 2017. № 3. С.103 - 115.

2. Жаров, А.А. Технологическая инфраструктура – «кровеносная система» современного мира // Материалы VII Международного форума безопасного интернета ФБИ-2016, 27 апреля 2016 г. Москва. МИА «РОССИЯ СЕГОДНЯ». Организатор Лига безопасного интернета. [Электронный ресурс]. URL: http://www.ligainternet.ru/encyclopedia-of-security/materialy-fbi/] (дата обращения 02.05.2017).

3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (в ред. от 21.07.2014 N 11-ФКЗ) // Российская газета. 1993. 25 декабря.

4. Малофеев, К.В. Доклад на Пленарном заседании // Материалы VII Международного форума безопасного интернета ФБИ-2016, 27 апреля 2016г. Москва. МИА «РОССИЯ СЕГОДНЯ». Организатор Лига безопасного интернета. [Электронный ресурс] URL: http://www.ligainternet.ru/encyclopedia-of-security/materialy-fbi/ (дата обращения 02.05.2017).

5. Политика / Аристотель; [пер. с древнегреч. С.А. Жебелева]. М.: Изд-во АТС, 2017. - 384 с.

6. Протоиерей Владислав Цыпин. Каноническое право. М.: Изд-во Сретенского монастыря, 2009. 864 с.

Содержание

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ В СМИ

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск десятый

Компьютерная верстка и дизайн О.Ю. Федосеева, И.А. Чиргадзе

Сдано в набор 14.12.2017.
Подписано к печати 16.12.2017.
Формат 60х84/16. Бумага офсетная.
Гарнитура Times ET.
Печать оперативная. Усл. п.л. 9,6. Уч.-изд. л. 8,9.
Тираж 500 экз. Заказ № ???.