Волжский университет имени В.Н. Татищева

ВЕСТНИК ПО БЕЗОПАСНОСТИ

№9 декабрь 2016

В НОМЕРЕ:

МАТЕРИАЛЫ ШКОЛЫ-КОНФЕРЕНЦИИ ПО БЕЗОПАСНОСТИ:

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск девятый

Тольятти 2016

ББК 004.00+33.00+34.00+57.00

Материалы Всероссийской научно-практической школы-конференции по безопасности. Вестник по безопасности. Выпуск девятый. – Тольятти: ВУиТ, 2016. - 112 с.

12-13 декабря 2016 года в Волжском университете имени В.Н. Татищева состоялась Всероссийская научно-практическая школа-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

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ЭКСТРЕМИЗМ КАК ОДНА ИЗ УГРОЗ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

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

Приверженность крайним взглядам, методам действий зачастую подрывает общественную и государственную безопасность, создавая реальную угрозу для сохранения существующих основ конституционного строя, межнационального, межконфессионального и межэтнического согласия.

Экстремизм является одной из наиболее острых и актуальных проблем современного общества и причиной тому служит многообразие его проявлений. Экстремизм, представляя глобальную угрозу безопасности для мирового сообщества, вышел за пределы отдельных государств и используется как инструмент для решения вопросов в сфере геополитики и экономического влияния.

По данным, опубликованным в журнале «Коммерсантъ Власть», становится очевидным, что за последние годы число внешних и внутренних экстремистских угроз заметно возросло. С 2015 года в Российской Федерации наметилась негативная тенденция в динамике преступности экстремистской и террористической направленности. За указанный период зарегистрировано 1329 преступлений экстремистской направленности, что на 28,5% больше, чем в 2014 году (1034). Особо следует обратить внимание на то, что рост числа этого вида преступлений отмечен в 56 субъектах Российской Федерации. Количество таких преступлений, как публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) и возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ), возросло почти на 40% в сравнении с 2014 годом[1].

Внешние угрозы обоснованы поддержкой экстремистских проявлений иностранными органами государственной власти и организациями с целью дестабилизации общественно-политической обстановки государства, а также деятельность приверженных идеологии экстремизма международных экстремистских и террористических организаций. К внутренним угрозам относится деятельность экстремистского характера религиозных, общественных неформальных объединений, отдельных лиц и некоммерческих организаций.

Чаще всего носителями экстремистских националистических взглядов становятся студенты средних профессиональных учебных заведений. Так, за истекший год к административной ответственности за публикацию в Интернете нацистской символики привлекли 46 человек, половина из которых – студенты техникумов и колледжей городов Оренбурга и Орска. В этом году еще восемь учащихся были привлечены за аналогичные правонарушения.

Так, приговором Ленинского районного суда г. Орска 22-летний житель г. Орска Владимир Аскаров и двое его друзей: ранее судимый 23-летний Игорь Рузманов и 29-летний Андрей Ходырев, жители г. Новотроицка, признаны виновными в совершении преступления, предусмотренного п. «а» ч. 2 ст. 282 УК РФ (возбуждение вражды, унижения достоинства группы лиц по признакам расы, национальности, происхождения, публично, с применением насилия). Аскарову также инкриминировано преступление, предусмотренное п. «е» ч. 2 ст. 111 УК РФ (умышленное причинение тяжкого вреда здоровью, опасного для жизни человека, по мотивам расовой, национальной вражды).

В суде установлено, что Аскаров, Рузманов и Ходырев на пр. Ленина в г. Орске с экстремистскими высказываниями напали на молодого человека неславянской национальности. Ему были нанесены удары деревянной битой по затылку и несколько ударов по телу руками и ногами. После этого Аскаров нанес потерпевшему удары ножом, причинив тяжкий вред здоровью.

Суд приговорил Ходырева к 10 месяцам, а Аскарова к 4 годам лишения свободы с отбыванием наказания в исправительной колонии общего режима. Рузманов осужден к 10 годам лишения свободы с отбыванием в исправительной колонии строгого режима.

Судебная коллегия по уголовным делам Оренбургского областного суда признала решение суда первой инстанции законным и обоснованным, а жалобы осужденных и их адвокатов – несостоятельными[2].

---

[1] Российский еженедельный общественно-политический и информационно-аналитический журнал «Коммерсантъ Власть». 2016. № 15 // Режим доступа: http://www.kommersant.ru/doc/2961578

[2] // Режим доступа: http://www.orenprok.ru/print?item=19245

Совершенно очевидно, что именно молодежь входит в группу риска и рассматривается террористическими группировками в качестве естественного резерва. Из этого следует, что необходимо сделать все, чтобы перехватить инициативу, включать молодых людей в разработку и реализацию программ противодействия вооруженному экстремизму.

Думается, что такая ситуация отчасти связана с тем, что органы власти не всегда уделяют должное внимание вопросам профилактики экстремизма среди молодежи. К примеру, в г. Оренбурге на протяжении 3 лет не принималась муниципальная программа по противодействию экстремизму и терроризму. Лишь благодаря настойчивости надзорного ведомства в этом году запланировано рассмотрение на заседании Оренбургского городского совета инициативы прокуратуры по принятию данной программы[3].

В целях противодействия экстремизму крайне важно создание концепции идеологической политики государства. Базовым элементом которой могла бы стать национальная идея, которая по-настоящему сплотила бы единый многонациональный российский народ. В концепции должны быть предусмотрены конкретные долгосрочные и среднесрочные меры, направленные на идеологическое воспитание и просвещение наиболее подверженной экстремизму социальной группы – подростков. Именно сознательная устойчивость к радикальной религиозной и иной идеологии подобного рода могла бы стать защитой от воздействия на население современных экстремистских идеологий. При наличии такой защиты даже самое щедрое финансирование дестабилизации обстановки в России извне окажется бесполезным.

Представляется целесообразным силами надзирающих и контролирующих органов организовать широкомасштабную и детальную проверку соответствия федеральному законодательству деятельности всех религиозных, национально-культурных и молодежных организаций, в отношении которых есть основания полагать, что они занимаются запрещенной экстремистской деятельностью.

Используя опыт работы на Северном Кавказе, организовать конкретную и предельно адресную профилактическую работу с представителями неформальных молодежных объединений в целях принятия мер, направленных на получение информации о негативных процессах, происходящих в молодежной среде, а также выявление идеологов и руководителей радикальных организаций, вовлекающих молодежь в экстремистскую деятельность.

Заслуживает также поддержки положительный опыт Республики Ингушетия, где создан военно-патриотический клуб, объединяющий детей сотрудников правоохранительных органов, погибших при исполнении служебного долга, и детей нейтрализованных членов бандподполья, что способствует их сближению и формированию между ними атмосферы взаимопонимания.

В предлагаемой концепции представляется целесообразным определиться и с пределами цензурирования в России глобальной сети интернет, так как эта проблема в настоящее время вызывает острые дискуссии в свете активизации защитников прав на свободу получения и распространения информации. Интересен в этом плане опыт зарубежных государств, противостоящих США и их союзникам. В связи с беспрецедентным информационным давлением они пошли на ограничения иностранных СМИ в целях защиты национального информационного пространства. Так, например, Министерство промышленности и информатизации Китая с 10 марта 2016 года ввело запрет на работу электронных СМИ, полностью или частично принадлежащих иностранным резидентам. Такие СМИ больше не смогут распространять информацию через интернет, а в лучшем случае – посредством печатных изданий. Китайские же СМИ будут сотрудничать с иностранными онлайн-СМИ только при наличии разрешения этого министерства. В руководстве национальных СМИ смогут работать только граждане Китая. Серверы онлайн-СМИ могут находиться только в КНР. Представляется, что в разумной мере этот опыт вполне мог бы быть взят на вооружение в России.

Для интернет-провайдеров необходимо разработать единые правила хранения личной информации их клиентов и пользователей в нужном объеме на тот случай, если подобные сведения будут затребованы при расследовании нарушений в сфере кибербезопасности.

В общественных местах доступа во «всемирную паутину» (библиотеки, школы, другие учебные заведения) установить фильтры, ограничивающие доступ к сайтам, содержащим экстремистские материалы.

Кроме того, представляется целесообразным предусмотреть внесудебный (административный) порядок включения информации в федеральный список экстремистских материалов, а также блокировки доменных имен сайтов, которые распространяют экстремистскую и радикал-националистическую информацию. При этом, если обладатели такой информации не считают ее экстремистской, пусть сами обжалуют соответствующие действия уполномоченных госорганов в суд и доказывают там свою правоту. Подобный порядок даст возможность более оперативно и эффективно

[3] // Режим доступа: http://ria56.ru/posts/8984456465445541.htm

реагировать на пропаганду экстремизма в интернете. Следует активизировать работу по внедрению современных технических средств для эффективного контроля радиоэфира и интернета.

Следующее, на наш взгляд, необходимо расширить спектр уголовно-правовых мер по пресечению противоправных действий террористических организаций, совершаемых в сети интернет, связанных с вербовкой. В этих целях рассмотреть вопрос о признании уголовно наказуемыми деяниями обладание такими материалами, их сбор или загрузку с компьютера. Современные технологии доказывания позволяют представить суду и подтвердить связанные с общением в социальных сетях технические элементы, свидетельствующие о наличии связей между обвиняемым и соответствующими электронными сообщениями.

Для разоблачения истинных целей и намерений исламских экстремистов, установления несостоятельности их теоретических подходов, противоречащих реалиям современного мира и коренным интересам исламских стран, видится полезным регулярно проводить на площадке Государственной думы специальные слушания с привлечением экспертов Федеральной службы безопасности, видных исламских ученых и авторитетов, ученых-исламоведов. Широко освещать в прессе материалы слушаний.

Особое внимание следует уделять миграционным процессам. Мигранты часто становятся объектом вербовки, радикализации. Многие из них находятся в России с превышением срока пребывания, выпадая из поля зрения правоохранительных органов. Необходимо проанализировать нормативные правовые акты, регулирующие вопросы нахождения иностранных граждан и лиц без гражданства на территории Российской Федерации. По результатам анализа принять дополнительные меры к совершенствованию законодательства.

В заключение следует указать на то, что не менее важным в борьбе с экстремизмом считаем необходимость совершенствования работы участковых уполномоченных полиции с иностранными гражданами в сфере контроля за соблюдением установленных правил проживания на территории России (контроль за лицами, сдающими жилье внаем, снимающими жилые помещения на обслуживаемом участке, получение сведений о характере занятости этих лиц). Службам собственной безопасности ведомств следует исключить возможные проявления коррупционной деятельности. В большей мере надлежит использовать помощь общественности[4].

«ПОТРЕБИТЕЛЬСКИЙ ЭКСТРЕМИЗМ» ИЛИ ЗЛОУПОТРЕБЛЕНИЕ ПРАВАМИ ПОТРЕБИТЕЛЯ

Подсеваткин В.С., студент
Научный руководитель: доцент Г.Р. Галеева
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Права потребителей в Российской Федерации защищаются достаточно хорошо, а иногда настолько хорошо, что от такой защиты страдают, несут серьёзные убытки добросовестные продавцы, изготовители, исполнители и другие субъекты гражданско-правовых отношений.

Основным инструментом защиты прав потребителей в РФ является Закон РФ от 07.02.1992 N 2300-1 "О защите прав потребителей" (далее - Закон о защите прав потребителей). Согласно указанному закону, потребителем признаётся гражданин, имеющий намерение заказать или приобрести, либо заказывающий, приобретающий или использующий товары (работы, услуги) исключительно для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности[5]. Принято считать, что потребитель является «слабой» стороной в гражданско-правовых отношениях, чем зачастую и руководствуются суды при принятии тех или иных решений.

В законе о защите прав потребителей предусмотрен ряд правовых механизмов, используемых как для защиты нарушенных прав граждан, так и для целенаправленного получения денежных средств или иной выгоды последними от продавцов, производителей, исполнителей. Например: Право потребителя возвратить товар надлежащего качества.

В соответствии со ст. 25 Закона о защите прав потребителей, потребитель вправе обменять непродовольственный товар надлежащего качества на аналогичный товар у продавца, у которого этот товар был приобретен, если указанный товар не подошел по форме, габаритам, фасону, расцветке,

[4] Российский еженедельный общественно-политический и информационно-аналитический журнал «Коммерсантъ Власть». 2016. № 15 // Режим доступа: http://www.kommersant.ru/doc/2961578

[5] Закон РФ от 07.02.1992 N 2300-1 "О защите прав потребителей".

размеру или комплектации. Если же аналогичный товар отсутствует в продаже (не нашёлся товар, соответствующий требованиям потребителя в отношении формы, габаритов, фасона, расцветки, размера или комплектации), потребитель вправе отказаться от исполнения договора купли-продажи и потребовать возврата уплаченной за указанный товар денежной суммы.

Таким образом, потребителем осуществляется возврат товара надлежащего качества, который мог быть в употреблении до 14 дней с момента покупки, по весьма субъективным причинам, которые никак нельзя ни подтвердить, ни опровергнуть;

Право потребителя на компенсацию морального вреда.

В соответствии со ст. 15 Закона о защите прав потребителей, Моральный вред, причиненный потребителю вследствие нарушения изготовителем (исполнителем, продавцом, уполномоченной организацией или уполномоченным индивидуальным предпринимателем, импортером) прав потребителя, предусмотренных законами и правовыми актами Российской Федерации, регулирующими отношения в области защиты прав потребителей, подлежит компенсации причинителем вреда при наличии его вины. Размер компенсации морального вреда определяется судом и не зависит от размера возмещения имущественного вреда.

Компенсация морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных потребителем убытков;

Освобождение потребителя от уплаты государственной пошлины и предоставляемое право выбора подсудности при обращении в суд.

Согласно п. 3 ст. 17 Закона о защите прав потребителей, Потребители, иные истцы по искам, связанным с нарушением прав потребителей, освобождаются от уплаты государственной пошлины в соответствии с законодательством Российской Федерации о налогах и сборах.

Под «иными истцами», согласно п. 16 Постановления Пленума Верховного Суда РФ от 28.06.2012 N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей", понимаются: иностранные граждане и лица без гражданства; прокурор; федеральный орган исполнительной власти, уполномоченный осуществлять федеральный государственный надзор в области защиты прав потребителей, и его территориальные органы, а также иные органы в случаях, установленных законом (далее - уполномоченные органы); органы местного самоуправления; общественные объединения потребителей (их ассоциации, союзы), имеющие статус юридического лица[6].

Согласно п. 2 ст. 17 Закона о защите прав потребителей, Иски о защите прав потребителей могут быть предъявлены по выбору истца в суд по месту:

- нахождения организации, а если ответчиком является индивидуальный предприниматель, - его жительства;
- жительства или пребывания истца;
- заключения или исполнения договора.

Если иск к организации вытекает из деятельности её филиала или представительства, он может быть предъявлен в суд по месту нахождения её филиала или представительства.

Таким образом, характерной чертой требований, предъявляемых потребителями в судебном порядке, обычно является неадекватное соотношение основной суммы иска и расходов, предъявляемых к возмещению.

Например, если потребитель обращается за помощью в общественную организацию, то сумма иска может складываться из стоимости приобретенного потребителем товара, расходов на проведение экспертизы, расходов на юридические услуги, моральный вред (какие либо границы вообще отсутствуют), штраф за добровольное неисполнение требований потребителя (50% от взысканной суммы). То есть при цене товара (работы, услуги) в 1000 рублей, цена иска будет составлять, допустим, 50000 рублей.

Деятельность некоторых субъектов «потребительского экстремизма» – общественных организаций по защите прав потребителей, выражается именно в взыскании с объекта «нападения» стоимости своих юридических расходов, оказываемых подставным потребителям;

Это основные механизмы воздействия потребителя на продавцов, изготовителей, исполнителей в рамках Закона о защите прав потребителей, что совсем не является пределом в данных правоотношениях. Указанные положения распространяются также на банковскую сферу, сферы страхования, строительства и многие другие, что приводит к подрыву существующих общеправовых принципов.

Вернёмся к названию настоящей статьи. Почему «потребительский экстремизм» и откуда это определение?

---

[6] Постановление Пленума Верховного Суда РФ от 28.06.2012 N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей".

Само понятие «экстремизм» исследователи, как правило, рассматривают в широком и специальном юридическом смысле. В широком смысле экстремизм (от лат. extremus – «крайний») определяется как «приверженность к крайним взглядам, мерам (обычно в политике)»[7].

Экстремизм – деятельность общественных объединений, иных организаций, должностных лиц и граждан, выраженная в крайних взглядах на существующую проблему и сопровождающаяся действиями противозаконного характера, направленная на удовлетворение, разрешение этой проблемы. Экстремизмом в правовом его смысле, как представляется, можно назвать действия, а также в публичной форме выраженные взгляды и намерения, преследующие своей целью нарушение или проявление неуважения к установленным законом правам и свободам граждан, общепринятым и справедливым нормам морали, общественному порядку и общему благосостоянию в демократическом обществе, при условии, что юридическая значимость этих действий доказана судом[8];

Термин «потребительский экстремизм» носит скорее литературный или научно-правовой характер и не находит официального закрепления в законодательстве.

Однако, исходя из смысла ст. 10 Гражданского Кодекса Российской Федерации[9], можно сформировать некое определение «потребительского экстремизма»:

«Потребительский экстремизм» – это недобросовестное поведение потребителей, направленное на получение выгоды, обращение в свою пользу имущества продавцов, изготовителей, исполнителей, выраженное в злоупотреблении своим правом «слабой стороны» и особым положением на рынке товаров, работ, услуг.

К главным причинам возникновения такого явления как потребительский экстремизм можно отнести несбалансированность законодательства в сфере защиты прав потребителей, презумпцию виновности продавца (изготовителя, исполнителя) при рассмотрении споров о защите прав потребителей в судах, отсутствие должного правового регулирования деятельности организаций, занимающихся защитой прав потребителей, правовой безграмотности продавцов (изготовителей, исполнителей).

Исходя из вышеизложенного, можно выделить некоторые меры борьбы со злоупотреблением потребителями своими правами:

- Не допускать конфликты с потребителем, с целью недопущения его обращения в общественные организации и судебные органы в целях защиты своих прав.
- Своевременно реагировать на претензии как письменные, так и устные, лишая тем самым потребителя возможности взыскания дополнительных расходов;
- Систематизировать и распространять информацию о явлении потребительского экстремизма;
- В случае возникновения спора не уступать и не допускать легкого взыскания денежных средств, а организовать максимально проблематичное судебное разбирательство, используя при этом все процессуальные права и механизмы.

На сегодняшний день явление «потребительского экстремизма» может быть и не так распространено, но с каждым днём оно проникает в новые сферы гражданско-правовых отношений, формирует благоприятную для себя судебную практику и подрывает основные правовые принципы. Таким образом, следует уделить серьёзное внимание злоупотреблению потребителями своими правами, а также разработать эффективные меры его противодействию.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СУРРОГАТНОГО МАТЕРИНСТВА В РФ

Сочнев А.В., студент
Научный руководитель: доцент Г.Р. Галеева
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

На современном этапе развития семейного законодательства РФ вопрос правового регулирования суррогатного материнства является одним из наименее урегулированных и наиболее спорных. Стоит отметить, что связывать данный факт исключительно с некомпетентностью законодателя было

[7] https://ru.m.wikipedia.org/wiki/Экстремизм.

[8] Анкета опроса экспертов по проблемам предупреждения преступлений, связанных с политическим и религиозным экстремизмом, разработанная НИИ проблем укрепления законности и правопорядка и Институтом международного права и экономики им. А.С. Грибоедова.

[9] "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ.

бы в корне неверно, поскольку сама природа данных отношений является достаточно спорной и неоднозначной.

В первую очередь стоит коснуться самой правовой природы договора суррогатного материнства. Фундаментальная проблема в данном случае состоит в том, что, исходя из существа правоотношений, лежащих в основе данного договора, достаточно сложно обозначить, является ли данный непоименованный договор сходным по правовому регулированию к договору купли-продажи, договору возмездного оказания услуг либо же суррогатное материнство представляет собой выполнение работы на основе договора.

Очевидно, что мы не можем в данном случае говорить о том, что данный договор близок по своей природе к договору купли-продажи. Пытаться уравнять данные договоры по своей природе не только абсолютно неэтично и аморально, но и чисто юридически невозможно, поскольку человек не может являться предметом договора купли-продажи.

Что касается возмездного оказания услуг, стоит отметить, что по своей правовой природе правоотношения, лежащие в основе договора суррогатного материнства, имеют много общего с отношениями, лежащими в основе договора возмездного оказания услуг. Это совокупность целенаправленных полезных действий, удовлетворяющих потребности человека (в данном случае, семейной пары), неразрывно связанная с личностью исполнителя. Однако, нельзя не обратить внимание на то, что услуга, как правило, не имеет вещественного воплощения, тогда как в случае договора суррогатного материнства по истечении девяти месяцев обнаруживается вполне материальный результат, который, однако, по причинам, обозначенным выше, мы не можем классифицировать как «вещь». На основании этого мы также не можем рассматривать суррогатное материнство как работу, поскольку «под работами понимаются действия, направленные на достижение материального результата, который может состоять в создании вещи, ее переработке, обработке или ином качественном изменении, например ремонте»[10].

На основе вышеизложенного следует заключить, что договор суррогатного материнства является уникальным непоименованным договором и требует конкретного законодательного регулирования. Более того, имеющиеся на данный момент нормы, регулирующие подобного рода правоотношения, вызывают определенные вопросы.

Речь в частности идет о абз. 2 п. 4 ст. 51 Семейного кодекса РФ, в котором сказано, что «лица, состоящие в браке между собой и давшие свое согласие в письменной форме на имплантацию эмбриона другой женщине в целях его вынашивания, могут быть записаны родителями ребенка только с согласия женщины, родившей ребенка (суррогатной матери)». Вполне очевидно, что данное положение направлено на защиту прав суррогатной матери как стороны соответствующего договора, однако нельзя не отметить, что данная норма сводит на нет права семейной пары как стороны договора.

Дело в том, что в случае отсутствия согласия суррогатной матери на запись семейной пары в качестве родителей ребенка уже после его рождения, закон становится на сторону суррогатной матери, лишая договор суррогатного материнства какого-либо правового смысла. Ведь при данных обстоятельствах не имеет никакого значения, насколько хорошо проработан упомянутый договор и насколько полно урегулированы лежащие в его основе правоотношения. В данном случае обозначенные в договоре условия передачи ребенка семейной паре вступают в конфликт с законодательством РФ, оставляя упомянутую сторону договора абсолютно незащищенной от подобного рода действий. Более того, закон никак не учитывает мотивационный аспект подобного рода действий, что может стать причиной различных случаев злоупотребления данным положением Семейного кодекса РФ.

Ярким примером может служить случай, произошедший в Санкт-Петербурге с Игорем и Светланой Петровыми (имена и фамилии изменены автором статьи, на которую делается ссылка). Пара долго оставалась бездетной. В качестве матери была выбрана 38-летняя женщина из Якутска, Преслава Воронова. Петровых поначалу смущал возраст будущей роженицы, однако пара оплатила Преславе перелет в Питер. Была проведена операция по искусственному оплодотворению. Через несколько дней стало ясно, что женщина беременна. УЗИ показало, что она ждет сразу двойню.

По контракту Петровы обязаны были каждый месяц выплачивать суррогатной матери по 30 тысяч рублей в месяц. Всего, включая эти деньги, Преслава должна была получить около 1 миллиона рублей. Но в какой-то момент ей этого показалось мало. И она поставила условие: либо еще 500 тысяч, либо «уеду домой и деток своих никогда не увидите»[11].

---

[10] Гражданское право России (часть 1): Курс лекций: Учебное пособие / Под ред. А.А. Мохова. - Волгоград, Издательство , 2003. – 114 с.

[11] «Суррогатная мать сбежала с новорожденными близнецами в секту». – «Комсомольская правда», интернет-ресурс - http://www.samara.kp.ru/daily/26591.4/3606355/

Подобный случай не является уникальным в своем роде и адекватно показывает несовершенство современного законодательства в области правового регулирования отношений, возникающих на основе договора суррогатного материнства.

Разумеется, существуют и обратные ситуации. В качестве примера можно упомянуть историю Нины Дмитрушковой, родившей девочку на основе заключенного ей договора суррогатного материнства. Сообщалось, что заказчик - известный адвокат - за девочкой не пришел. Вероятно, это произошло потому, что он хотел внука (для рождения ребенка был использован биоматериал его умершего сына), а родилась девочка. После того, как Нине не были выплачены деньги и ребенка у нее не забрали, она обратилась в суд и выиграла его. Однако деньги получить не удалось, так как судебный процесс проходил без ответчика. Женщине пришлось нанять частного детектива, чтобы разыскать человека, с которым она заключала договор. Вот тогда и выяснилось, что договор она якобы подписала не с ним, а с вымышленным человеком[12].

Как можно заметить, в данном случае суррогатная мать как сторона договора несколько легкомысленно отнеслась к его заключению, не удостоверив личность обратившегося к ней человека, или столкнулась с работой очень умелого мошенника, обезопасившего себя на случай рождения ребенка женского пола.

Приведенные примеры объективно указывают на необходимость более детального правового регулирования правоотношений, возникающих в связи с заключением договора суррогатного материнства. Из них также следует, что, учитывая современное законодательство и, в частности, упомянутую ст. 51 Семейного кодекса РФ, права семейной пары как стороны договора являются абсолютно незащищенными, поскольку изменившаяся воля суррогатной матери является достаточным и законным основанием невыполнения данного договора, не влекущим за собой каких-либо негативных правовых последствий. И хотя не исключено, что суд может обязать суррогатную мать в этом случае вернуть выплаченные ей по договору средства, едва ли можно говорить о какой-либо иной компенсации, поскольку представить столь длительный срок напрасного ожидания семейной парой ребенка в материальной форме представляется весьма трудным. К тому же, суррогатная мать поступает в полном соответствии с законодательством, что ставит под сомнение возможность получения подобной компенсации в принципе. Исходя из этого, единственным способом решения данной проблемы на сегодняшний день является включение в договор о суррогатном материнстве пункта, предусматривающего выплату суррогатной матерью компенсации в случае отказа от исполнения условий договора. Однако все в данном случае будет зависеть от решения суда, поскольку, вероятнее всего, требовать выплаты подобной компенсации семейной паре придется в судебном порядке.

В заключение следует отметить, что суррогатное материнство – закономерный результат научно-технического прогресса, который дает семейным парам, не способным самостоятельно родить ребенка, возможность продолжить свой род и познать радости отцовства и материнства. И законодатель должен приложить все усилия, чтобы с правовой точки зрения данная возможность не вызывала недоверия, поскольку здоровая и полноценная семья – главная структурная единица развитого правового государства.

СТ. 205.6 УК РФ КАК ГАРАНТИЯ БЕЗОПАСНОСТИ ГРАЖДАН РОССИИ: ЕЕ ПЛЮСЫ И МИНУСЫ

Учкин Т.А., студент
Научный руководитель: старший преподаватель Ю.А. Веретина
ФГБОУ ВО «Оренбургский государственный аграрный университет»
г. Оренбург, Россия

6 июля 2016 года в Уголовный кодекс Российской Федерации Федеральным законом № 375-ФЗ[13] была введена ст. 205[6], которая установила ответственность за несообщение органам власти «о лице (лицах), которое по достоверно известным сведениям готовит, совершает или совершило» одно из шестнадцати преступлений, предусмотренных данной статьей. В обозначенный перечень вошли

[12] «Суррогатная мать, у которой не стали забирать ребенка, требует алименты» - «Вести.Ru», интернет-ресурс - http://www.vesti.ru/doc.html?id=2828431

[13] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности. Федеральный закон от 6 июля 2016 года № 375-ФЗ // Российская газета. 2016. 11 июля.

не только преступления террористической направленности, но и отдельные преступления, посягающие на основы конституционного строя и безопасность государства, мир и безопасность человечества.

Думается, что намерения при этом были самыми благими. Введение данной статьи должно было усилить гарантию безопасности населения. Гражданин, осведомлённый о существовании ответственности за несообщение об указанных преступлениях, обязательно сообщит в органы власти. Тем более существуют гарантии его безопасности, так как об этом можно сообщить анонимно.

Вместе с тем, введение в УК РФ указанной статьи вызывало и справедливый поток критики[14]. Многими авторами негативно оценивается само недоносительство. Не случайно еще более ста лет назад Н.С. Таганцев указывал на то, что в современных условиях государственной жизни нет необходимости привлечения всех граждан к участию в преследовании преступников. Специальные органы могут вести дело открытия преступников и с несравненно большим успехом, и с меньшей затратой сил[15].

Возникает вопрос: не возвращает ли нас введение обсуждаемой статьи назад в советское время? Есть мнение о том, что обязать каждого совершать доносы – это как вернуться в сталинскую эпоху, где граждане активно пользовались доносительством, были шпионами друг другу и могли так устранять всякого, даже самого добропорядочного гражданина, стоило только сообщить куда следует. Статью использовали для запугивания друзей и родственников «политических» преступников, которым предлагали выбрать: либо даешь показания против своего товарища, либо садишься в соседнюю камеру.

У нас также возник ряд замечаний и вопросов относительно данной нормы. Во-первых, из названия статьи следует, что лицо подлежит ответственности за несообщение о любом преступлении. Однако из ее содержания следует иное: на лицо не возлагается обязанность сообщать о факте совершения преступления (независимо от стадии преступной деятельности), а требуется сообщать о лице (лицах), его совершающем. Кроме того, сообщать о лице (лица) следует только в том случае, если его (их) деяние предусмотрено одной из указанных статей. Таким образом, наблюдается противоречие между наименованием статьи и ее содержанием.

Вопросы по применению указанной нормы: следует ли сообщать в соответствующие органы власти информацию о совершении преступления (на любой его стадии) в случае, если о лице (лицах) информации нет? Возлагает ли законодатель обязанность на лиц знать указанные в перечне статьи Уголовного кодекса и иметь навыки квалификации преступлений? Еще одним из наиболее часто задаваемых вопросов будет вопрос о том, как установить достоверно ли человек знал о преступлении или нет? С учетом того, что следствие не всегда утруждает себя доказыванием наличия умысла, велика вероятность того, что для привлечения к уголовной ответственности по ст. 205^6 УК РФ будет достаточным доказать тот факт, что гражданин был знаком с лицом, обвиняемым в терроризме, а значит, не мог не знать о готовящемся преступлении.

Недостаток ст. 205^6 УК РФ, в первую очередь, заключается в том, что она порождает в обществе сомнения в презумпции невиновности окружающих. По результатам проведенного социологического опроса, касаемо внесения данной статьи и принятия «Пакета Яровой», люди очень бояться того, что будут иметь место ложные доносы, а потому, ввиду социальных противоречий между гражданами, под действие данной статьи будут попадать абсолютно невиновные граждане.

Следующий момент, вызывающий недоумение. Введение указанной статьи породило вопросы о том, почему она размещена именно в разделе IX «Преступления против общественной безопасности и общественного порядка», в главе 24 «Преступления против общественной безопасности»? Получается, что существовавшая ранее (до вступления в силу Уголовного кодекса Российской Федерации 1996 года) статья, предусматривающая ответственность за недонесение имела своим объектом интересы государственной власти, а точнее интересы правосудия, а вновь введенная статья посягает на общественную безопасность.

Вообще, обращаясь к истории России, не трудно заметить, что наказание за недоносительство практиковалось много веков. Наказание за недоносительство впервые было предусмотрено Соборным уложением 1649 года, а затем она перемещалась из одних законов в другие вплоть до 1996-го, когда недоносительство было декриминализовано в связи с принятием Уголовного кодекса РФ.

---

[14] Кириенко М.С. Несообщение о преступлении: старый состав в новых условиях // Адвокат. 2016. № 7. С. 9-14.

[15] Таганцев Н.С. Русское уголовное право. Часть общая. СПб, 1902. Т. 1. С. 541.

Самая главная неприязнь обществом ст. 205^6 УК РФ заключается в том, что она является одной из составляющих Пакета антитеррористических законов, который в СМИ прозвали «Пакет Яровой». В данном пакете законов обнаружено огромное количество противоречий с ныне действующим законодательством, а самое главное – прямое противоречие Конституции РФ. Граждане РФ категорически против такого вторжения в их частную жизнь, поэтому никаких плюсов от принятия данного Пакета законов не видят.

Безусловно, преступления против общественной безопасности в последнее время ужесточились и под угрозой терроризма находится огромное количество людей, но для того, чтобы их предотвращать нужно принимать иные меры, поскольку граждане знакомы со всеми изменениями в законодательстве и вряд ли будут рисковать сообщая о преступниках посредствам мобильной связи, интернета и так далее. Для реализации «Пакета Яровой» требуется колоссальная затрата средств из бюджета страны, что является очень негативным явлением, ввиду кризиса.

Мобильным операторам придётся приобретать дополнительное оборудование стоимостью в миллиарды рублей для хранения информации в течение полугода, что повлечет подорожание услуг связи. Куда проще, к примеру, оснащать места большого скопления людей более качественной системой безопасности. Позаботиться о дополнительных средствах безопасности воздушного транспорта, но никак не полной реализацией пакета антитеррористических законов.

Следует отметить и тот факт, что действующим Уголовным кодексом предусмотрена ст. 316 «Укрывательство преступлений», которая, как и 205^6 УК РФ является видом прикосновенности к преступлению, но максимальное наказание в виде лишения свободы за совершение данного преступления предусмотрено до двух лет. Почему тогда законодатель в ст. 205^6 УК РФ установил максимальное наказание в один год?

ТЕРРОРИЗМ КАК ГЛОБАЛЬНАЯ ПРОБЛЕМА ЧЕЛОВЕЧЕСТВА

Щеколдина О.А., студент
Научный руководитель: старший преподаватель Ю.А. Веретина
ФГБОУ ВО «Оренбургский государственный аграрный университет»
г. Оренбург, Россия

Терроризм является опасным явлением, приобретающий в настоящее время разнообразные формы угрозы человечеству. Террористические акты влекут человеческие жертвы, разрушение духовных и материальных ценностей, сеют вражду между различными государствами, ненависть между национальными группами.

Понятие терроризма раскрывается в ст.3 Федерального Закона Российской Федерации «О противодействии терроризму» от 06 марта 2006 года № 35, согласно которой «терроризм – это политика которая основана на применении террора и идеологии насилия против мирного населения, воздействуя на принятие решения органами государственной власти и местного самоуправления»[16]. В Уголовном кодексе Российской Федерации ответственность за совершение террористического акта предусмотрена статьей 205.

Следует отметить, что терроризм появился не вчера. Террористы были всегда. Самая ранняя террористическая группировка – секта сикариев, которая действовала в Палестине в I веке новой эры и истребляла представителей еврейской знати, выступавших за мир с римлянами. В качестве оружия сикарии использовали кинжал или короткий меч – сику. Это были экстремистски настроенные националисты, возглавлявшие движение социального протеста и настраивавшие низы против верхов. В действиях сикариев прослеживается сочетание религиозного фанатизма и политического терроризма: в мученичестве они видели нечто приносящее радость и верили, что после свержения ненавистного режима Господь явится своему народу и избавит их от мук и страданий[17].

Той же идеологии придерживались и представители мусульманской секты ассасинов, убивавшие халифов, префектов, губернаторов и даже правителей: ими был уничтожен Иерусалимский король

[16] О противодействие терроризму. Федеральный Закон от 6 марта 2006 г. № 35 - ФЗ // Российская газета. 2006. 25 марта. В редакции Федерального закона от 31 декабря 2014 г. № 505-ФЗ // Российская газета. 2015. 16 января.

[17] Ветров Н.Д. Терроризм как преступление против человечества. М.: Издательство «Спарк», 2014. С. 186.

Конрад Монферратский. Убийство являлось для сектантов ритуалом, они приветствовали мученичество и смерть во имя идеи и твердо верили в наступление нового миропорядка.

В настоящее время терроризм порождается определенными причинами: нерешенность социальных, религиозных, а также национальных проблем, имеющей значение для национальной или иной группы, связанной с ее ценностями, обычаями, традициями. Террористические акты стали частью военных действий в Чечне, Афганистане, Сирии.

В Чечне пик терроризма связывают с господством ваххабизма. На его поддержание и распространение тратились очень большие деньги. В то время на территории республики действовали лагеря для подготовки террористов и боевиков, инструкторами наемников были наемники из арабских стран, в том числе гражданин Саудовской Аравии Хаттаб. Хаттаб получал деньги для поддержания терроризма от международных террористических организаций (Аль-Каида). Что касается террористических актов в Сирии, то они продолжаются и по настоящее время. Есть версия о том, что Сирийцы совершают террористические акты и на территории РФ, но они пока не имеют юридического подтверждения.

Одним из самых масштабных, за последнее время, террористических актов, в котором пострадали граждане Российской Федерации является теракт в небе над Синайским полуостровом. По данным российских СМИ, взрыв произошел в отсеке негабаритного багажа в хвостовой части самолета, в результате которого 31 октября 2015 года погибло 224 человека, большинство из которых были гражданами Российской Федерации. Вскоре эта версия была подтверждена сотрудниками ФСБ. Расследование этой трагедии продолжается до сих пор. Самое сложное – это изобличить преступников. Сейчас о них существуют различные версии как в СМИ, так и в следственных органах. Стоит также отметить, что вскоре после крушения одна из группировок, подконтрольных «ИГИЛ», взяла на себя ответственность за катастрофу российского лайнера в Египте.

Делая вывод, хотелось бы отметить что, терроризму присуще преднамеренное создание страха, напряженности, подавленности. Терроризм порождает страх преступлений, ради достижения определенных целей, воздействуя на органы государственной власти или органов местного самоуправления, а также причинение смерти лицам, которые захватываются в качестве заложников.

ОЦЕНКА СОЦИАЛЬНОЙ ТЕРПИМОСТИ (НЕТЕРПИМОСТИ) В ВУЗЕ (ОТЧЕТ ПО РЕЗУЛЬТАТАМ НИРС ЮРИДИЧЕСКОГО ФАКУЛЬТЕТА ВОЛЖСКОГО УНИВЕРСИТЕТА ИМЕНИ В.Н. ТАТИЩЕВА)

Алексеева А.М., Белова М.В., Ванькина И.А., Вдовкина Ю.С., Горбунова Т.А., Григорян Г.Г., Диасамидзе Л.Т., Дунин К.Ю., Иванов Г.Ю., Козубова Н.С., Коробкина Е.А., Краснобаев Н.И., Малолеткова Ю.В., Маркушина К.И., Медведев С.Е., Подсеваткин В.С., Пономарева Т.В., Савельева Е.А., Салейкин Н.Ю., Серебрянников В.И., Сочнев А.В., Строган О.А., Сутковой Г.О., Томшивер А.Я., Ульянов А.О., Федорова О.Ю., Ясакова Ю.В., Яшина Е.П., студенты
Научный руководитель: к.ю.н., доцент С.В. Дубовиченко
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Актуальность темы исследования. В современном мире не существует однозначного подхода к определению термина "экстремизм". В нормативно-правовых актах различных стран, соглашениях и конвенциях международных организаций, а также в многочисленных научных исследованиях понятие "экстремизм" разнится в зависимости от подхода и методов исследования данного определения.

В основе настоящего исследования лежит определение экстремизма, сформулированное Я.И. Гилинским: "Экстремизм обозначает приверженность крайним взглядам и радикальным мерам, а также реализацию этих мер, проявляющиеся в отрицании существующих политических и правовых норм, ценностей, процедур, основополагающих принципов организации политических систем, стремлении к подрыву политической стабильности, низвержению существующей власти и действующих порядков". Именно это определение наиболее полно отражает сущность данного явления.

Исходя из вышесказанного можно сделать вывод, что экстремизм неразрывно связан с личностью человека и её структурой, причём, чем сложнее и разнообразнее состав общества (что особо актуально для России), тем чаще мы будем сталкиваться с подобным явлением.

Как известно, наиболее уязвимой и внушаемой группой населения является молодежь.

Актуальность проблемы экстремизма в молодежной среде определяется не только его опасностью для общественного порядка, но и тем, что данное преступное явление имеет свойство перерастать в более серьезные преступления, такие как терроризм, убийство, причинение тяжких телесных

повреждений, массовые беспорядки. Молодежь рассматривается как большая социальная группа, имеющая специфические социальные и психологические черты, наличие которых определяется возрастными особенностями молодых людей и тем, что их социально-экономическое и общественно-политическое положение, их духовный мир находится в состоянии становления.

В современной научной литературе к этой группе обычно относят (в статистике и социологии) людей в возрасте от 15 до 30 лет.

Элементы экстремистского поведения молодежи формируются на фоне деформации социальной и культурной жизни общества. В перечень основных причин роста экстремистского поведения молодежи исследователи склонны включать следующие: социальное неравенство, желание самоутвердиться в мире взрослых, недостаточную социальную зрелость, а также недостаточный профессиональный и жизненный опыт.

Молодежи свойственна психология максимализма и подражания, что в условиях острого социального кризиса является почвой для агрессивности и молодежного экстремизма. Большинство преступлений экстремистского характера совершается несовершеннолетними в составе группы.

Общеизвестно, что подростки особенно восприимчивы к влиянию сверстников. Стремясь быть признанными в этой среде, они часто ищут компании других подростков, которые могли бы их оценить[18]. Так, Самарским областным судом рассматривалось уголовное дело в отношении двух лиц, совершавших в течение длительного времени преступления по мотивам национальной ненависти и вражды к лицам неславянской внешности. Согласно материалам дела, для облегчения совершения преступления, подсудимые решили обратиться за помощью к несовершеннолетнему, предложив ему поучаствовать в избиении лиц неславянской внешности. В результате такого нападения, уроженцу Азербайджана были причинены повреждения различной степени тяжести, от которых он скончался в больнице[19].

По информации правоохранительных органов, большинство преступлений экстремистской направленности, в том числе с участием несовершеннолетних, совершаются посредством использования Интернета. С его помощью вербуются новые сторонники из молодежной среды, а также распространяется негативная информация. В данном контексте, опасность заключается в том, что правоохранительным органам сложно контролировать информацию, которая имеется в Сети.

Несмотря на недавние результаты исследования, проведенные Левада-Центром, в котором отмечается, что в целом среди населения страны наблюдается постепенный спад ксенофобских и этнофобских настроений и «индикатор этнофобных установок среди населения в целом вернулся к уровню 2011 года, уходя от «аномальных» перекосов»[20], тем не менее, согласно статистике, приведённой МВД, за период с 2003 года по 2015 год в России наблюдается рост преступлений экстремистской направленности[21], что также характерно для большинства современных государств (рисунок 1).

Рисунок 1 – График преступлений экстремистской направленности

[18] Л. Агрессия: причины, последствия, контроль. М., Олма-пресс. 2009. с. 207.
[19] Приговор Самарского областного суда № 02-62/2010 от 1 ноября 2010 г. по делу № 02-62/2010
[20] http://www.levada.ru/2016/10/11/intolerantnost-i-ksenofobiya/
[21] https://мвд.рф

Таким образом, экстремизм (во всех его проявлениях) представляет угрозу национальной безопасности, посягает на основополагающие принципы правового государства, нарушает интересы общества и личности.

Предметом настоящего исследования являются результаты анкетирования студентов 1-5 курсов юридического факультета и фокус-группы, в состав которой входили респонденты в возрасте от 25 лет. Выбор указанных респондентов обусловлен необходимостью сравнения правосознания студентов, формируемое в условиях современного мира, с уже сложившимися представлениями лиц, входящих в фокус-группу, об экстремизме. Опрос проводился в период с 3 по 14 октября 2016 г.

Объектом исследования является субъективное восприятие экстремизма: отношение к экстремизму, оценка эффективности мер борьбы с экстремизмом и уровня преступлений экстремистской деятельности.

Вопросы, включённые в опрос, были условно разделены на три группы:

1. Уровень экстремизма, т.е. субъективное мнение о распространённости экстремизма;

2. Состояние защищенности от проявлений экстремизма, т.е. отсутствие какого-либо риска, в случае реализации которого возникают негативные последствия экстремистской направленности;

3. Готовность к проявлению/непротивлению социальной терпимости, т.е. установка личности на совершение определенных действий, направленных на проявление/непротивление социальной терпимости.

Методы исследования: опрос (анкетирование), диалектический метод, математический метод, сравнительный метод, в также общенаучные методы исследования (индукция, дедукция, обобщение, анализ, синтез).

Цель исследования состояла в выявлении и анализе основных социальных представлений отдельной социальной группы (студентов юридического факультета) и фокус-группы об экстремизме, его основных причинах, способов предупреждения и масштабов распространения.

Исходя из этого, необходимо выделить следующие **задачи:**

1. Выяснить какое значение опрошенные респонденты вкладывают в понятие "экстремизм";

2. Определить отношение студентов и фокус-группы к экстремистской деятельности;

3. Провести ряд сравнительных анализов по полученным данным студентов различных курсов, а также фокус-группы;

4. Анализ предложенных респондентами рекомендаций по решению проблем экстремизма и социальной нетерпимости;

5. Подготовить рекомендации по формированию ценностной антиэкстремистской установки обучающихся юридического факультета Волжского университета имени В.Н. Татищева

Категориальный аппарат исследования

Само понятие «экстремизм» исследователи, как правило, рассматривают в широком и специальном юридическом смысле. В широком смысле экстремизм (от лат. extremus – «крайний») определяется как «приверженность к крайним взглядам, мерам (обычно в политике)».

Выше мы уже приводили определение Я.И. Гилинского: «Экстремизм обозначает приверженность к крайним взглядам и радикальным мерам, а также реализацию этих мер, проявляющуюся в отрицании существующих политических, правовых норм, ценностей, процедур, основополагающих принципов организации политических систем, стремлении к подрыву политической стабильности, низвержению существующей власти и действующих порядков».

Резолюция Парламентской Ассамблеи Совета Европы, принятая в 2003 г., содержит следующее определение: «экстремизм представляет собой форму политической деятельности, явно или исподволь отрицающую принципы парламентской демократии и основанную на идеологии и практике нетерпимости, отчуждения, ксенофобии, антисемитизма и ультра-национализма».

«Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом» от 15 июня 2001 г. даёт следующее определение понятия «экстремизм» (п. 3 ч. 1 ст. 1): «Экстремизм — какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них, и преследуемые в уголовном порядке в соответствии с национальным законодательством Сторон».

Если обратиться к конкретным доктринальным дефинициям экстремизма[22], то здесь можно выделить его определения:

[22] Сигарев А.В. Правовое регулирование противодействия экстремизму: курс лекций: - Новосибирск: СибАГС, 2015. – С. 13-14.

1**) как общественно опасной «деятельности»:**

а) экстремизм – деятельность общественных объединений, иных организаций, должностных лиц и граждан, выраженная в крайних взглядах на существующую проблему и сопровождающаяся действиями противозаконного характера, направленная на удовлетворение, разрешение этой проблемы;

б) экстремизмом в правовом его смысле, как представляется, можно назвать действия, а также в публичной форме выраженные взгляды и намерения, преследующие своей целью нарушение или проявление неуважения к установленным законом правам и свободам граждан, общепринятым и справедливым нормам морали, общественному порядку и общему благосостоянию в демократическом обществе, при условии, что юридическая значимость этих действий доказана судом;

2) как социально негативного явления:

а) экстремизм – социально-негативное явление, проявляющееся в совокупности общественно опасных уголовно наказуемых деяний, совершаемых в соответствии с определенной системой взглядов, воззрений, убеждений, возведенных в культ, в целях достижения определенного результата, предусмотренного этой системой взглядов, в какой-либо области общественных отношений, существующий порядок в которой отрицается экстремистами;

б) экстремизм – антиобщественное социально-политическое явление, представляющее собой социально и психологически обусловленное, идеологически мотивированное использование крайних форм и методов в социально-политических отношениях;

в) экстремизм – это общественное явление, заключающее борьбу за власть субъектов социальных отношений в политической, национальной, экономической, религиозной и иных сферах общественной жизни, использующих для достижения цели крайние (агрессивные) способы и формы деятельности;

г) экстремизм – негативное явление, исходящее из крайних политических, националистических взглядов, проявляющееся в преднамеренно реализуемых конкретных, запрещенных законом действиях, наносящих существенный вред государственным устоям;

3) как комплекс институтов, идей, установок и т. п.:

а) экстремизм – совокупность организационно-политических структур, их радикальных политических установок (крайне правых, крайне левых, национал-экстремистских, сепаратистских) и соответствующей практической деятельности, которая характеризуется использованием насилия в различных формах или угрозами его применения на противоправной, антиконституционной основе для достижения политических целей;

4) как специфическая идеология:

а) экстремизм – идеология, предусматривающая принудительное распространение ее принципов, нетерпимость к оппонентам и насильственное их подавление;

б) экстремизм является своеобразной идеологией, обосновывающей правильность и необходимость совершения различных преступных деяний (например, совершение насильственных преступлений по мотивам расовой, национальной или религиозной вражды и ненависти) для достижения лицом или группой лиц определенной цели, в том числе политической, оправдывающей совершение таких преступлений;

в) экстремизм – идеология нетерпимости, возбуждения ненависти либо вражды, унижения достоинства человека либо группы лиц по признакам расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, выражающаяся в совершении публичных противоправных действий;

Интересны точки зрения современных исследователей в вопросах определения экстремизма. Так Н.Н. Афанасьев даёт определение экстремизма следующим образом: «Экстремизм есть изначальное отрицание всякого чувства меры. Он оперирует искажёнными, деформированными представлениями о действительности, по крайней мере, в той её части, где пытается реализовать свои цели, как ближайшие, так и более отдалённые. В языке это выражается в крайности суждений, безапелляционности, категоричности. В практической деятельности это неизбежно приводит к насилию»[23]. Таким образом, Н.Н. Афанасьев делает акцент на идеологической составляющей экстремизма.

Такой же подход прослеживается и у исследователей В.Ю. Верещагина и М.И. Лабунец, которые определяют экстремизм как «идеологию, предусматривающую: 1. принудительное распространение её принципов, 2. нетерпимость к оппонентам и насильственное их подавление»[24].

[23] Афанасьев Н.И. Идеология терроризма // Социально-гуманитарные знания.2002, № 1. с. 25.

[24] Верещагин В.Ю., Лабунец М.И. Политический экстремизм в контексте модернизации современной российской государственности // Философия права. — Ростов — на — Дону: Изд-во Рост.юрид. ин-та МВД России, 2002, № 2, с. 84.

Е.П. Сергун даёт очень обширное определение понятию «экстремизм». По его мнению, «под экстремизмом следует понимать приверженность к целой системе взглядов, концепций, идей и представлений, основанной на политической, расовой, религиозной или национальной ненависти либо вражде в отношении личности, какой-либо социальной группы, нации или государства, не имеющую внешнего выражения. Как только экстремистские воззрения индивида реализуются во внешнем мире в форме противоправных деяний, следует говорить об экстремистской деятельности»[25].

Исследователь Э.В. Улезко даёт определение экстремизму, как виду противоправной деятельности, направленной на достижение стоящих перед субъектом экстремизма целей с использованием насильственных методов. При этом экстремистскими, по его мнению, можно назвать только такие действия, которые превышают необходимую степень воздействия, независимо от используемых средств физического насилия, морального принуждения, экономического давления и т. д[26].

В России юридическое определение того, какие действия считаются экстремистскими, содержится в статье 1 Федерального Закона № 114-ФЗ «О противодействии экстремистской деятельности».

К экстремистской деятельности (экстремизму) относятся:

1. насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

2. публичное оправдание терроризма и иная террористическая деятельность;

3. возбуждение социальной, расовой, национальной или религиозной розни;

4. пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

5. нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

6. воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

7. воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

8. совершение преступлений по мотивам, указанным в пункте "е" части первой статьи 63 Уголовного кодекса Российской Федерации;

9. пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;

10. публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

11. публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

12. организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

13. финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг;

В 2013 году Президентом РФ была утверждена Концепция общественной безопасности в Российской Федерации, согласно которой «одним из основных источников угроз общественной безопасности является экстремистская деятельность национальных, религиозных, этнических и иных организаций и структур, направленная на нарушение единства и территориальной целостности РФ, дестаби-

[25] Сергун Е.П. Правовое обеспечение экстремистской деятельности в Российской федерации // Правовая политика и правовая жизнь. 2006. № 2, с. 197.

[26] Улезко Э.В. Экстремизм и терроризм: понятийно-категориальный аппарат исследования явления //www.kai.ru

лизацию внутриполитической и социальной ситуации в стране. Особую озабоченность вызывает распространение экстремистских настроений среди молодёжи».

С учетом проведенного анализа можно попытаться сформулировать **определение экстремизма, как формы политической деятельности, отрицающей демократические принципы и основанной на идеологии социальной нетерпимости, национализма, ксенофобии и антисемитизма.**

Противодействие экстремизму

В ст. 3 Федерального закона от 25.07.2002 N 114 – ФЗ «О противодействии экстремистской деятельности» в редакции от 23.11.2015 г. раскрываются основные **направления противодействия экстремистской деятельности**:

- принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности;

- выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

Готовность к проявлению/непроявлению социальной терпимости

Для реализации цели настоящего исследования было введено понятие "готовность к проявлению/непроявлению социальной терпимости". В основе данного понятия лежит психологическая теория установки, которая активно исследовалась такими учеными, как Д.Н. Узнадзе и В.А. Ядовым.

Согласно Узнадзе: "Для удовлетворения потребности необходима соответствующая ситуация. В окружающей среде должно быть средство, позволяющее удовлетворять имеющуюся потребность. При наличии потребности и средства ее удовлетворения у субъекта возникает особое состояние, которое можно характеризовать как склонность, направленность, готовность совершить акт, ведущий к удовлетворению потребности. Это и есть установка – готовность к совершению определенного действия".

Разработанные в школе Узнадзе идеи послужили отправными моментами в создании диспозиционной концепции регуляции поведения личности В.А. Ядова. В качестве системообразующего признака или отношения в системе внутренней регуляции социального поседения человека Ядов выделил диспозиционно-установочные явления. Приняв за основу положение Узнадзе о том, что установка представляет собой целостно-личностное состояние готовности, настроенности на поведение в данной ситуации для удовлетворения определенной потребности, Ядов проанализировал все составные части этой системы.

Триада Узнадзе "ситуация — потребность — установка" претерпела некоторые изменения в ходе исследований В.А. Ядова; в частности, он заменил понятие установки на понятие диспозиции. Под диспозицией личности он понимает систему ее предрасположенностей (установок) к определенному поведению применительно к тем или иным ситуациям, условиям.

В концепции Ядова выделяются четыре уровня потребностей, соответственно тому, в каких сферах деятельности они находят свое удовлетворение. Основанием классификации служат здесь последовательное расширение границ активности личности:

Первая сфера, где реализуются потребности человека - ближайшее семейное окружение.

Вторая сфера - контактная (малая) группа, в рамках которой действует индивид.

Третья сфера - более широкая сфера деятельности, связанная с определенной сферой труда, досуга, быта.

Четвертая сфера - сфера деятельности, понимаемая как определенная социально-классовая структура, в которую индивид включается через освоение идеологических и культурных ценностей общества.

Подобная классификация имеет прямую связь с сущностью проводимого исследования, поскольку формирование диспозиций не в последнюю очередь связано с уровнями социального взаимодействия личности. В данном вопросе нельзя не учитывать, что формирование терпимости или нетерпимости в малой группе обусловлено плотностью и частотой взаимодействия ее членов, тогда как на более высоких уровнях плотность взаимодействия компенсируется количественным фактором социального взаимодействия.

Ситуации структурированы по длительности времени существования данных условий деятельности. Т.е. ситуацию деятельности можно рассматривать как быстро изменяющуюся или же устойчивую.

Первый уровень - быстро изменяющиеся предметные ситуации;

Второй уровень - ситуации группового общения, характерные для деятельности индивида в

рамках малой группы. По своей

длительности подобные ситуации деятельности человека гораздо больше, чем предыдущими;

Третий уровень - устойчивые условия деятельности, имеющие место в различных социальных сферах (труда, досуга, семейной жизни человека);

Четвертый уровень - наиболее длительные, устойчивые условия деятельности в рамках определенного типа общества, широкой экономической, политической и культурной структуры его функционирования.

Представляется, что быстро возникающие предметные ситуации не являются полноценным основанием формирования диспозиционной установки на проявление/непроявление терпимости, однако в конкретных случаях могут выступать как катализаторы для дальнейшего перехода на более высокий уровень длительности взаимодействия и дальнейшего формирования диспозиции.

Определенная диспозиция, как уже было сказано, возникает (и действует) на пересечении определенного уровня потребностей и ситуаций их удовлетворения. При этом выделяются четыре уровня диспозиций:

Первый уровень диспозиций - элементарные установки. Они формируются на основе витальных потребностей и в простейших ситуациях. Эти установки лишены модальности (переживания " за" или " против") и не осознаются субъектом.

Очевидно, что данный уровень диспозиций не имеет существенной связи с проводимым исследованием, поскольку отсутствует логическая связь между удовлетворением витальных потребностей и установкой на проявление или непроявление терпимости.

Второй уровень диспозиций - социальные фиксированные установки. Это более сложные диспозиции, которые формируются на основе потребности человека в общении, осуществляемом в малой (контактной) группе. Социальные установки образуются на базе оценки отдельных социальных объектов (или их свойств) и отдельных социальных ситуаций (или их свойств).

Данный уровень диспозиций в рамках нашего исследования логически связан с оценкой отдельных социальных объектов и отдельных социальных ситуаций, которые абстрагированно друг от друга или в совокупности приводят к необходимости удовлетворения потребности на общение в социальной группе со схожими установками. Возможна и обратная ситуация, когда установка формируется на основе удовлетворения потребности в общении в малой группе под ее социальным влиянием.

Третий уровень диспозиций - базовые социальные установки. В этом случае направленность может быть представлена как идентификация личности со значимой для нее социальной деятельностью. Например, можно обнаружить доминирующую направленность в сферу профессиональной деятельности (тогда основные интересы человека будут связаны, например, с достижением высокого уровня профессионализма, расширением профессиональных знаний и умений, построением профессиональной карьеры и т.п.).

На данном уровне диспозиций наиболее вероятным является формирование установки на основе постоянного взаимодействия с личностями, осуществляющими социально значимую для субъекта социальную деятельность. Типичным примером являются фанатские объединения или посещение на постоянной основе мероприятий типа "Русский марш". Данная социальная активность не всегда связана сугубо с профессиональной деятельностью; если говорить о ней, то в современном мире в этой области преобладают экстремистские установки на гендерной основе.

Четвертый уровень диспозиций - система ценностных ориентаций личности на цели жизнедеятельности человека, а также на средства их достижения.

Четвёртый уровень диспозиций связан с активной деятельностью, направленной на реализацию ценностно-жизненных ориентаций личности, т.е. организация экстремистских объединений, активная пропаганда и проч. Представляется маловероятными, что среди респондентов данного исследования имели место подобные случаи.

Предложенная иерархия диспозиционных образований выступает как регулятивная система по отношению к поведению личности. При этом каждый из уровней диспозиций "ответственен" за регуляцию определенного уровня поведения.

Первый уровень - "поведенческий акт" - означает регуляцию непосредственных реакций субъекта на актуальную предметную ситуацию. Целесообразность поведенческих актов диктуется необходимостью установить адекватное соответствие (равновесие) между специфическими и быстро сменяющими друг друга воздействиями внешней среды и витальными потребностями субъекта в данный момент времени.

Второй уровень регулирует поступки личности. Поступок представляет собой элементарную социально значимую " единицу" поведения. Целесообразность осуществления поступка выражается в

установлении соответствия между простейшей социальной ситуацией и социальными потребностями субъекта.

Представляется маловероятным, что два низших уровня регуляции поведения имеют отношение к предмету данного исследования, поскольку экстремистская диспозиция не является единичным актом поведения и как правило имеет устойчивый характер.

Третий уровень регулирует уже некоторые системы поступков, образующие поведение в различных сферах жизнедеятельности, где человек преследует существенно более отдаленные цели, достижение которых и обеспечивается системой поступков.

Четвертый уровень - регулирует целостность поведения, или собственно деятельность личности. "Целеполагание" на этом высшем уровне представляет собой некий " жизненный план", важнейшим элементом которого выступают отдельные жизненные цели, связанные с главными социальными сферами деятельности человека в области труда, познания, семейной и общественной жизни"[27].

Два высших уровня регуляции поведения так или иначе связаны со вторым уровнем, поскольку представляют из себя систематизированные поведенческие "единицы". Основой их систематизации в данном случае будет являться непосредственно их сущность, на основании которой эти "единицы" будут совокупно переходить на третий (отдалённые цели и система поступков) или четвёртый (целеполагание как жизненный план) уровни.

В целом диспозиционная регуляция социальной деятельности личности может быть описана следующей формулой:

"ситуации" (= условия деятельности) --> "диспозиции" --> "поведение"(= деятельность).

Таким образом, **готовность к проявлению/непроявлению социальной терпимости - ценностная установка поведения субъекта, заключающаяся в совершении определённых действий, направленных на проявление или непроявление терпимости и зависящая от ряда определённых факторов, в частности уровня социального взаимодействия, временного промежутка и систематичности совершения подобных действий.**

Экстремистская обстановка

Категорией, требующей разъяснение, является понятие экстремистской обстановки. Для настоящего исследования понятие экстремистской обстановки имеет ключевое значение, поскольку конечной целью работы является определение характера экстремистской обстановки.

Экстремистскую обстановку можно определить**, как комплексное понятие, включающее в себя уровень экстремизма, готовность к проявлению/непроявлению социальной нетерпимости, состояние защищённости от проявления экстремизма.**

Подробный опрос для выяснения оценки экстремистской обстановки студентами-юристами 1,2,3,4,5 курсов ВУиТ и фокус группой (лица старше 25 лет) предоставлен в данной научно-исследовательской работе. В исследовании выяснялись следующие параметры:

-уровень экстремизма;

-готовность к проявлению/не проявлению социальной терпимости;

-состояние защищённости от проявления экстремизма.

Первым компонентом экстремистской обстановки, является оценка респондентами уровня экстремизма. Он определяется на основании ответов на вопросы (7,8,9,10,13) анкеты, предоставленной студентами.

Для определения этого параметра, респондентам предлагалось дать оценку состояния экстремизма в России: (7 вопрос: «Укажите, какой, на Ваш взгляд, уровень экстремизма в России?») и указать насколько часто им в жизни приходилось сталкиваться с проявлениями социальной терпимости (8 вопрос: «Сталкивались ли Вы с дискриминацией по национальному, религиозному и иному признаку, в отношении другого человека?»). Девятый вопрос: «Какой, на Ваш взгляд, уровень опасности экстремизма в Самарской области?» Для ответа на этот вопрос респондентам была предложена девятибалльная шкала для оценки экстремистской обстановки. На данной шкале цифра 1 соответствует нормальной обстановке (низкий уровень экстремизма), а цифра 9 –резко отрицательной обстановке (высокий уровень экстремизма).

10 вопрос: «Изменится ли, на Ваш взгляд, уровень экстремизма в России через 3 года?» Ответ на данный вопрос должен раскрыть тенденцию развития уровня экстремизма за определённый период.

Последним вопросом для определения параметра «уровень экстремизма» был задан вопрос

[27] Ядов В.А. О диспозиционной регуляции социального поведения личности //Методологические проблемы социальной психологии. 1975. с. 97.

№ 13: «Случалось ли Вам быть свидетелем этнической нетерпимости, по отношению к представителям какой-либо национальности?»

Важной составляющей нормальной обстановки экстремизма, является отношение к этой проблеме. Для определения второго компонента «готовность к проявлению/не проявлению социальной терпимости» предполагалось пять вопросов (15, 23, 32, 36, 37) анкеты.

Предложенные вопросы позволяют определить отношение респондентов к проблеме экстремизма.

15 вопрос: «Согласны ли, Вы, с утверждением «Россия для русских?». В этом вопросе опрашиваемым предлагалось выразить своё мнение в отношении проживания иностранных граждан на территории РФ.

23 вопрос направлен на определение позиции респондентов относительно национальной/религиозной принадлежности при выборе друзей.

32 вопрос: «Как бы, Вы, отнеслись к открытию лагеря беженцев в г. Тольятти?» Для исследования, очень важно мнение в отношении беженцев.

36 вопрос: «Вы согласны или не согласны с тем, что присутствие мигрантов в нашем городе чрезмерно?» Этот вопрос второго блока конкретизирует мнение респондентов по поводу количества мигрантов в нашем городе.

37 вопрос: «Как, Вы, относитесь к идее проведения «русских маршей»?» Последний вопрос этой группы связан с желанием респондентов организовывать, принимать участие в демонстрациях на националистической почве.

Третий блок вопросов (19, 29, 38, 39, 40) анкеты позволяет дать оценку состоянию защищённости от проявления экстремизма.

Для этого респондентам предлагалось высказать своё мнение относительно своей безопасности. 19 вопрос: «Считаете ли, Вы, себя защищённым от проявления экстремизма?»

Следующий вопрос блока, направлен на выявление у респондентов определённых событий, которые могут произойти в РФ на почве национальной розни.

29 вопрос: «Возможны ли в настоящее время в России массовые кровопролитные столкновения на националистической почве?»

В 40-м вопросе респондентам предлагалось оценить возможность столкновений на националистической почве в Самарской области.

Последние вопросы блока посвящены межнациональной напряжённости.

8 вопрос: «Ощущаете ли Вы сейчас в г. Тольятти межнациональную напряжённость?»

39 вопрос: «Чувствуете ли Вы в настоящее время враждебность со стороны людей других национальностей?»

Ответы на поставленные вопросы распределяются от абсолютно-утвердительных до абсолютно-отрицательных. Первый, второй и третий компоненты тестируются пятью вопросами. Ответ на каждый из этих вопросов оценивается как +1,0,-1. Полученные в группе данные заносятся в протокол (Приложение 9).

Для целостной характеристики отдельного компонента сочетание ответов для каждого участника на вопросы обобщаются следующим образом: положительная оценка равная 1 получается при сочетаниях: «+++++», «+++00», «++++0», «+++--», «++++-», «+++0-»; отрицательная оценка, равная -1 получается при сочетаниях: «-----», «----+», «---++», «---00», «----0», «---+0»; иные сочетания характеризуют оценку как неопределённую, равную 0.

Для каждого компонента подсчитывается средняя по группе оценка. По формуле:

$К_{(1,2,3,4,5)}=(X+ - X-\ldots) /n,$

где $К_{(1,2,3,4,5)}$ – обобщённая оценка каждого компонента экстремистской обстановки;

X+ - количество положительных ответов, содержащихся в первом, втором или третьем столбце в зависимости от определяемого элемента экстремистской обстановки;

X- - количество отрицательных ответов, содержащихся в первом, втором или третьем столбце в зависимости от определяемого элемента экстремистской обстановки;

N - количество участников опроса.

Полученные средние оценки могут располагаться в интервале от -1 до +1. Этот континуум подразделяется на три части: от -1 до – 0,33 – отрицательные оценки; от -0,33 до +0,33 – противоречивые или неопределённые оценки и от +0,33 до +1 – положительные оценки. Соотношение оценок трёх компонентов – уровня экстремизма, готовность к проявлению / не проявлению социальной терпимости, состояние защищенности от проявления экстремизма - позволяет охарактеризовать экстремистскую обстановку как нормальную (приемлемую) (+0,33 до +1), неопределённую (-0,33 до +0,33)

и отрицательную (-1 до -0,33).

Глава 1. Анализ результатов анкетирования студентов юридического факультета (I-V курс)

1.1 Анализ результатов анкетирования студентов 1 курса

В результате проведенного опроса среди студентов Волжского университета имени В.Н. Татищева, были получены следующие результаты (таблица 1).

Таблица 1 – анализ результатов анкетирования студентов 1 курса юридического университета.

Параметры определения экстремистской обстановки	Индексы показателей
Уровень экстремизма	0,077
Готовность к проявлению / непроявлению социальной нетерпимости	-0,192
Состояние защищенности от проявлений экстремизма	0,154
Обобщенный показатель	0,013

Индекс первого компонента «характеристика уровня экстремизма» 0,077, что является неопределенной оценкой.

Индекс второго компонента «готовность к проявлению/ непроявлению социальной нетерпимости» составил -0,192, что также является неопределенной оценкой.

Индекс третьего блока «состояние защищенности от проявлений экстремизма» составил 0,154, что является неопределенной оценкой.

Обобщенный индекс, определяющий уровень экстремистской обстановки, основанный на оценке студентами – юристами 1 курса ВУиТ, равняется 0,013. Как видно, обобщенный индекс характеризует экстремистскую обстановку как неопределенную.

Большинство опрошенных (57%) экстремизм рассматривают в качестве формы политической деятельности, отрицающей демократические принципы и основанные на идеологии социальной нетерпимости национализма, ксенофобии и антисемитизма.

Подавляющее большинство респондентов считают, что уровень экстремизма средний – 65%, низкий – 26%. За высокий уровень не высказался ни один респондент.

Однако в вопросе «Об изменения уровня экстремизма в России через 3 года» высказались 11% - быстро увеличиться, 26% - увеличится, 46% - не изменится и 15% - снизится.

На вопрос «Сталкивались ли вы с дискриминацией по национальной, религиозной и иному признаку в отношении другого человека», 7% ответили, что никогда не сталкивались, скорее «нет», чем «да» – 23%, затрудняюсь ответить – 7%, скорее «да», чем «нет» – 38% и лишь 23% ответили что сталкиваются часто. Из этого следует вывод, что около половины респондентов либо никогда в жизни не сталкивались данными явлениями, либо сталкивались часто. Это показывает, что их мнение формируется исходя из обобщенных представлений положения дел в рассматриваемом вопросе, которые складываются, в основном, по средством получения информации из СМИ и интернета, что подтверждает уже следующий вопрос, где респондентов спрашивали в каком источнике можно чаще всего встретить пропаганду экстремистской деятельности: 23% - СМИ, 65% - интернет, баннеры, листовки, граффити – 15% , окружение – 3%.

Оптимистическим настроение наших респондентов назвать тоже очень тяжело. Например, на последующие вопросы: «Случалось ли вам быть свидетелем этнической нетерпимости по отношению к представителям какой-либо национальности» большинство респондентов ответили «периодически» и «многократно».

Так же разделилось мнение опрашиваемых по вопросу – «Согласны ли вы с утверждением «Россия для русских»», 23% студентов ответили – определенно нет, 26% - скорее нет, чем да, 19% - скорее да, чем нет, 7% - определенно да, а 19% студентов затруднились однозначно ответить.

Респондентам было предложено выделить наиболее значимые проблемы современной России, путем расставления предложенных вариантов с 1-го по 13-е место (таблица 2).

На вопрос «Считаете ли вы себя защищенным от проявления экстремизма», определенно да ответили 7% студентов, скорее да – 38%, затрудняюсь ответить - 30%, скорее нет – 15%, определенно нет – 3%. Респонденты не чувствующие своей защищённости: беспокоятся за себя – 7%, за своих близких – 7%, беспокоятся за себя и за своих близких – 46%.

Таблица 2 – Наиболее важные проблемы современной России

а) коррупция	1
в) безработица	3
в) терроризм	6
г) экстремизм	10
в) экономическая нестабильность	2
е) расслоение общества	9
ж) преступность	5
з) социальные протесты	13
и) пенсионная реформа	11
к) внешние угрозы	7
и) допинговый скандал	8
к) дефицит бюджета	4
л) цены на нефть и газ	12

Вопрос о том, знают ли студенты о существовании в городе Тольятти экстремистских организаций (движений) показал, что 3% довольно часто сталкиваются с их представителями, 23% - слышали, но лично не сталкивались и 73% ничего не слышали об этом.

По мнению опрашиваемых, решение проблемы экстремизма зависит от населения – 50% и от воспитания в семье – 46%.

Для большинства респондентов при выборе друзей не важна национальная и религиозная принадлежность, так считают 87%, 3% затруднятся ответить на этот вопрос, и для 6% этот критерий важен.

Позитивным показателем является то, что среди опрошенных студентов первого курса меньшая часть, которая составила: 14% выразила свою готовность вступить в экстремистскую организацию за вознаграждение и 46% - не готовы вступить.

Мнение респондентов по вопросу открыть лагерь беженцев в городе Тольятти разделилось, 14% допускает открытие лагеря, 23% затрудняются ответить, а 53% против данной идеи.

Негативно студенты 1 курса отнеслись к людям с нетрадиционной сексуальной ориентацией. 26% придерживаются мнения, что их надо лечить, 26% изолировали бы их от общества, 15% физически уничтожили, 15% оказали психологическую и иную помощь,30% предоставили бы их самим себе и 15% затрудняются ответить.

Если бы у студентов появилась возможность по управлению государством, то наиболее действенными они считают ужесточение законодательства (11%), воспитание населения – 7%. Так результаты исследования показывают, что наиболее эффективным мерами по борьбе с экстремизмом должны быть: ужесточение законодательства за данное преступление и воспитание населения.

В своей анкете, мы предложили ответить респондентам на вопрос, каким образом можно внедрить антиэкстремистскую составляющую в учебный процесс (школа, колледж, вуз).

Наиболее популярными ответами среди студентов юридического факультета, являлись (таблица 3).

Таблица 3 – Наиболее популярные ответы

Меры внедрения	Количество респондентов, поддерживающие предложенную меру
Развитие молодежных движений (культура, спорт)	
Воспитательное воздействие	2
Профилактика	3

1.2 Анализ результатов анкетирования студентов 2 курса

В результате проведенного опроса студентов Волжского университета имени Татищева, были получены следующие результаты (таблица 4):

Таблица 4 – Результаты анкетирования

Параметры определения экстремистской обстановки	Индексы показателей
Уровень экстремизма	- 0,0385
Готовность к проявлению/непроявлению социальной нетерпимости	0,346
Состояние защищенности от проявлений экстремизма	0,423
Обобщенный показатель	0,2435

Индекс первого компонента «уровень экстремизма» составил -0,0385, что является неопределенным показателем.

Индекс второго компонента «готовность к проявлению/непроявлению социальной нетерпимости» составил 0,346, что является положительным показателем.

Индекс третьего компонента «состояние защищенности от проявлений экстремизма» составил 0,423, что также является положительным показателем.

Обобщенный индекс, определяющий уровень экстремистской обстановки, основанный на оценке студентами-юристами 2 курса ВУиТ, равняется 0,2435. Как видно, обобщенный индекс характеризует экстремистскую обстановку как неопределенную. Однако, полученные индексы находятся на границе с положительной экстремистской обстановкой.

Большинство опрошенных (34%) рассматривают экстремизм в качестве формы политической деятельности, отрицающей демократические принципы и основанной идеологии социальной нетерпимости, национализма, ксенофобии и антисемитизма.

Подавляющее число респондентов считают, что уровень экстремизма в России средний – 73%, низкий – 26%. За высокий уровень не высказался ни один респондент.

Однако, уже в 10 вопросе об изменении уровня экстремизма в России через 3 года половина респондентов высказались об увеличении - 50%, также значительная часть опрошенных показала об не изменении данного уровня – 30%, часть респондентов ответила о снижении уровня – 15 % , а о резком снижении ответило значительно меньше – 3 %.

На вопрос «Сталкивались ли Вы с дискриминацией по национальному, религиозному и иному признаку в отношении другого человека?» 11% ответили «нет», «скорее нет, чем да» ответили 23%, «скорее да, чем нет» - 38%, затрудняются с ответом – 7 % и 19% заявили, что сталкиваются с ней. Из этого следует вывод, что большинство респондентов сталкивались с данным явлением в той или иной мере. Это показывает, что их мнение формируется исходя из обобщенных представлений положения дел в рассматриваемом вопросе, которые складываются, в основном, посредством получения информации из Интернета, что подтверждает уже вопрос, где предлагалось оценить экстремистскую обстановку в Самарской области: 26% затруднились дать однозначного ответа, оценив данный уровень, как средний 3% оценили экстремистскую обстановку в Самарской области как высокую, а 11% - как низкую, большинство респондентов (60%) – показало различную градацию ответов.

Оптимистическим настроение наших респондентов назвать тоже очень тяжело. Например, на вопрос «Какой уровень экстремизма в России будет через 3 года?» получены следующие результаты: 50% опрошенных утверждают, что уровень экстремизма увеличится, 30% - что уровень не изменится, 15 % верят в снижение экстремизма, и лишь 3 % опрошенных утверждают о резком снижении.

Также разделилось мнение опрашиваемых по вопросу - "Следует ли ограничить проживание на территории России людей следующих национальностей?". 26% - высказались за ограничение проживания украинцев и такое же число - выходцев с Кавказа, также большое количество респондентов (23%) - китайцев. «Не следует ограничить» - большое количество респондентов (61%) указало евреев, на втором месте – выходцы с Кавказа и приезжие из стран ЕС, которые имеют по одинаковому количеству процентов – 46%. «Затрудняюсь с ответом» - большее количество (26%) указало все нации, кроме русских, на втором месте – вьетнамцы и украинцы, имеющие по одинаковому количеству процентов (19%). Данная тенденция, по большей части связана с напряжённой внешнеполитической обстановкой в мире.

На вопрос: «Известны ли Вам конкретные экстремистские группировки/организации?», подавляющее большинство респондентов (80%) ответило «не известны» , 19% - «известна одна», «известно две и более» - не ответило ни одного человека.

На вопрос «случалось ли Вам быть свидетелем этнической нетерпимости по отношению к представителям какой-либо национальности» большинство респондентов (42%) ответило «периодически»; «затрудняюсь ответить» - 7%, «скорее нет, чем да» - 23%, «определенно нет» - 23%.

На вопрос о согласии с высказываниями показал следующий результат:

- многонациональность России приносит больше вреда, чем пользы (3%);
- у мигрантов, проживающих на территории РФ должно быть меньше прав, чем у коренного населения (3%);
- представители некоторых национальностей незаслуженно доминируют на рынке труда, в бизнесе и во власти (30%);
- на мое отношение к человеку не влияет то, к какой национальности он относится (61%).

Из вышеизложенных ответов можно сделать определенный вывод о том, что большинство респондентов не выделяют национальность как приоритетный признак при коммуникации с социумом.

Мнение опрашиваемых по вопросу о том, согласны ли респонденты с утверждением «Россия для русских» разделилось следующим образом: большинство опрошенных (30%) скорее не согласны с данным утверждением, 26% - затрудняются с ответом и ответили «определённо нет»

Респондентам было предложено выделить наиболее значимые проблемы современной России, путем расставления предложенных вариантов с 1-го по 13-е место (таблица 5).

Основной причиной экстремизма (национализма, антисемитизма и т.д.) большинство опрошенных (34%) видит в том, что нагнетаются национальные, религиозны, политические противоречия в обществе и СМИ.

На втором месте (23%) респонденты видят причины экстремизма в информационной войне, развёрнутой против России.

Далее одной из причин (19 %) респонденты видят в высокой степени неравенства в обществе.

На вопрос «Считаете ли вы себя защищенным от проявления экстремизма», определенно да ответили 7% студентов, скорее да – 15%, затрудняюсь ответить - 30%, скорее нет – 15%, определенно нет – 0%, Респонденты не чувствующие своей защищённости: беспокоятся за себя – 0%, за своих близких – 7%, беспокоятся за себя и за своих близких – 3%.

Вопрос о том, знают ли студенты о существовании в городе Тольятти экстремистских организаций (движений) показал, что 3% - слышали, но лично не сталкивались и 88% ничего не слышали об этом.

По мнению опрашиваемых, решение проблемы экстремизма зависит от воспитания в семье – 46 % и от населения – 38%.

Для большинства респондентов при выборе друзей не важна национальная и религиозная принадлежность, так считают 61%, 7% затруднятся ответить на этот вопрос, и для 3% этот критерий важен.

Позитивным показателем является то, что среди опрошенных студентов второго курса меньшая часть, которая вступила бы в экстремистскую организацию- 7%, а также - 3% выразившие свою готовность вступить в экстремистскую организацию за вознаграждение и 46% не готовы вступить.

Таблица 5 – Наиболее важные проблемы современной России

а) коррупция	2
в) безработица	1
в) терроризм	4
г) экстремизм	7
в) экономическая нестабильность	3
е) расслоение общества	8
ж) преступность	6
з) социальные протесты	11
и) пенсионная реформа	9
к) внешние угрозы	12
и) допинговый скандал	13
к) дефицит бюджета	5
л) цены на нефть и газ	10

Мнение респондентов по вопросу открыть лагерь беженцев в городе Тольятти разделилось следующим образом - 26% допускает открытие лагеря, 19% затрудняются ответить, а 53% против данной идеи.

Негативно студенты 2 курса отнеслись к людям с нетрадиционной сексуальной ориентацией. 15% придерживаются мнения, что их надо лечить, 7% изолировали бы их от общества, 7% физически уничтожили, 23% оказали психологическую и иную помощь, 26% предоставили бы их самим себе, 15% затрудняются ответить, также 3 % высказали свой вариант решения данного вопроса.

Если бы у студентов появилась возможность по управлению государством, то наиболее действенными они считают миграционный контроль (11%), реформа правоохранительных органов– 7%. Так результаты исследования показывают, что наиболее эффективным мерами по борьбе с экстремизмом должны быть: ужесточение законодательства за данное преступление и воспитание населения.

В своей анкете, мы предложили ответить респондентам на вопрос, каким образом можно внедрить антиэкстремистскую составляющую в учебный процесс (школа, колледж, ВУЗ).

Наиболее популярными ответами среди студентов юридического факультета, являлись (таблица 6).

Таблица 6 – Наиболее популярные ответы

Меры внедрения	Количество респондентов, поддерживающие предложенную меру
Развитие молодежных движений (культура, спорт)	4
Воспитательное воздействие	3

1.3 Анализ результатов анкетирования студентов 3 курса

В результате проведённого опроса среди студентов Волжского университета имени Татищева, были получены следующие результаты (таблица 7).

Индекс первого компонента «характеристика уровня экстремизма» составил -0,2, что является неопределённой оценкой.

Индекс второго компонента «готовность к проявлению/непроявлению социальной нетерпимости» составил -0,18, что является неопределённой оценкой.

Индекс третьего компонента «состояние защищенности от проявлений экстремизма» составил 0,12, что является неопределённой оценкой.

Обобщенный индекс, определяющий уровень экстремистской обстановки, основанный на оценке студентами-юристами 3 курса ВУиТа, равняется -0,087. Как видно, обобщенный индекс характеризует экстремистскую обстановку как неопределённую.

Таблица 7 - Результаты анкетирования

Параметры определения экстремистской обстановки	Индексы показатели
Уровень экстремизма	-0,2
Готовность к проявлению /непроявлению социальной нетерпимости	-0,18
Состояние защищенности от проявлений экстремизма	0,12
Обобщенные показатели	-0,087

Большинство опрошенных (40%) экстремизм рассматривают как форму политической деятельности, отрицающей демократические принципы и основанные на идеологии социальной нетерпимости, национализма, ксенофобии и антисемитизма.

Подавляющее число респондентов считают, что уровень экстремизма по всей России составляет: средний – 56%, низкий -16%, высокий-8%.

А, по мнению респондентов, в Самарской области уровень экстремизма – низкий (22%).

Однако, уже в 10 вопросе об изменении уровня экстремизма в России через три года большинство респондентов (58%) ответили, что он увеличится.

На вопрос «Сталкивались ли Вы с дискриминацией по национальному, религиозному и иному признаку в отношении другого человека?» 6% ответили, что затрудняются ответить, «скорее нет, чем да» - 16%, никогда не сталкивались – 22%, такой же показатель у респондентов, которые сталкивались с дискриминацией и «скорее да, чем нет» - 34%.

Данные показатели подтверждаются в вопросе «Случалось ли Вам быть свидетелем этнической нетерпимости по отношению к представителям к какой-либо национальности?», где большинство респондентов ответили – периодически (40 %).

Темой второго блока вопросов было: готовность к проявлению/непроявлению социальной терпимости.

В вопросе согласны ли вы с утверждением «Россия для русских», респонденты отвечают «скорее да, чем нет» - 28%, не давая определённого ответа. Однако об идеи организации проведения «русских маршей» больше половины респондентов (58%) ничего об этом не слышало. По данному вопросу существует определённая категория студентов, которая ответила определённо положительно - 8%, а остальные склоняются к отрицательному ответу, распределяясь в процентном отношении примерно в равных долях.

Не смотря на ответы предыдущего вопроса, для большинства респондентов (48%) национальность/религиозная принадлежность при выборе друзей определённо не важна.

Когда же вопрос коснулся открытия лагеря беженцев в городе Тольятти, 28% студентов высказались категорически отрицательно по данному вопросу, а скорее «против» и «затрудняюсь ответить» разделились поровну -26%. Вследствие чего, по мнению респондентов, присутствие мигрантов в нашем городе чрезмерно (48%).

Оптимистическое настроение наших респондентов можно наблюдать на примере вопроса «считаете ли вы себя защищённым от проявления экстремизма», где 34% студентов ответили положительно и лишь 10% отрицательно. Данную позицию респонденты подтверждают, отвечая на вопрос «Чувствуете ли вы в настоящее время враждебность со стороны людей других национальностей?» высказывая мнение о редкости своих чувств - 32% и всего лишь 4% - сталкиваются с этим.

Мнения опрашиваемых по вопросу о возможности, в настоящее время, в России массовых кровопролитных столкновений на националистической почве разделилось: 36% допускают возможность, а другие 30% склоняются к отрицательному ответу. А непосредственно в Самарской области – отрицают возможность таких столкновений

Рассматривая состояние межнациональной напряжённости непосредственно в городе Тольятти, большинство респондентов – 32% её не ощущают.

1.4 Анализ результатов анкетирования студентов 4 курса

В результате проведённого опроса среди студентов Волжского университета имени Татищева, были получены следующие результаты (таблица 8).

Индекс первого компонента «характеристика уровня экстремизма» составил -0.316 — что является неопределенным показателем.

Индекс второго компонента «Готовность к проявлению / не проявлению социальной нетерпимости» составил 0.421 — что является положительным показателем.

Таблица 8 - Результаты анкетирования

Параметры определения коррупционной обстановки	Индексы показателей
Уровень экстремизма	- 0.316
Готовность к проявлению / не проявлению социальной нетерпимости	0.421
Состояние защищенности от проявлений экстремизма	0.263
Обобщенный показатель	0.123

Индекс третьего компонента «состояние защищенности от проявлений экстремизма» составил 0.263, что является неопределенным показателем.

Обобщенный индекс определяющий уровень экстремистской обстановки, основанный на оценке студентами - юристами 4 курса ВУИТ, ровняется 0.123

Как видно, обобщенный индекс характеризует экстремистскую обстановку, как неопределенную.

Подавляющее число респондентов считают, что уровень экстремизма средний - 73%, низкий — 26%. За высокий уровень не высказался ни один из опрошенных студентов.

На вопрос сталкивались ли они с дискриминацией по национальному, религиозному и иному признаку в отношении другого человека большинство опрошенных (36%) ответили «скорее да, чем нет».

Как показал опрос, большинство опрошенных 68% периодически были свидетелями этнической нетерпимости по отношению к представителям какой — либо национальности.

Оптимистическое настроение респондентов назвать очень тяжело. Например, на вопрос «Какой уровень экстремизма в России будет через 3 года?»— получены следующие результаты: 42% опрошенных утверждают, что уровень экстремизма увеличится; 36% что уровень не изменится; 5% быстро увеличится; 5% резко снизится. Однако на данный момент большинство респондентов считают, что в Самарской области уровень экстремизма средний (т.е. 62%), а 36% ответили - низкий уровень.

В повседневной жизни люди сталкиваются с фразой «Россия для русских», но большинство респондентов определенно не согласны (42%) с данным утверждением и только 5 % согласны

Важность проблем современной России по мнению студентов 4 курса ВУиТ, расположенных в порядке убывания (таблица 9).

Таблица 9 - Важность проблем современной России

Коррупция	1
Экономическая нестабильность	2
Терроризм	3
Безработица	4
Экстремизм	5
Преступность	6
Внешние угрозы	7
Пенсионная реформа	8
Дефицит бюджета	9
Расслоение общества	10
Цены на нефть и газ	11
Социальные протесты	12
Допинговый скандал	13

Для большинства студентов (68%)национальная/религиозная принадлежность не играет роли при выборе друзей. Ни один из студентов не ставит на первый план национальность и религию при выборе друзей.

Мнение, опрашиваемых студентов ВУиТ проживающих в городе Тольятти разделилось по поводу открытия лагеря беженцев в их городе: категорически против 15%, скорее, против 15%, затрудняюсь ответить 26%, скорее положительно 26%, однозначно положительно 15%.

Так же проживающие студенты в городе Тольятти считают, что присутствие мигрантов чрезмерно 26% и только 10% не согласны с этим утверждением.

По вопросу «Как вы относитесь к идее проведения «русских маршей?» большинство опрошенных затруднилось дать оценку (52%), отрицательно оценили эту идею 21%, положительно высказались 15% респондентов.

На вопрос о защищенности от проявления экстремизма, мнение студентов разделилось. Всего лишь 15% опрошенных уверенны в своей защищенности, 26% затрудняются ответить, а также 26 % ответили «скорее, да» и 10% определенно нет. Из результатов опроса студентов видно, что они не могут дать точного ответа и определить свою позицию относительно защищенности.

На вопрос «возможно ли в настоящее время в России массовые кровопролитные столкновения на националистической почве?», 5% респондентов ответили, что уверены в этом. Больше половины опрошенных, а именно - 42% ответили «скорее да, чем нет». Затрудняются ответить 26%, скорее нет, чем да 21%, определенно нет 5%. Из этого следуют что большинство опрошенных скептически относятся к возможным столкновениям.

В своей анкете, мы предложили ответить респондентам на вопрос «ощущаете ли вы сейчас в г. Тольятти межнациональную напряженность?», где скорее да ответило — 26%, затрудняюсь ответить — 26%, скорее, нет — 26%, определенно, нет — 21%. Однако ни один респондент не ответил «определенно, да».

В Настоящее время враждебность со стороны людей других национальностей практически никогда не сталкивались 10% опрошенных. Сталкиваются постоянно — 5% , наибольшая часть 57% сталкивается с проявлением враждебности довольно редко. Но, не смотря на это, в Самарской области массовые кровопролитные столкновения на националистической почве большинство считают — скорее невозможными 57 . В обратном уверены всего 10%. Считают абсолютно невозможным данный исход — 15 %.

Если бы у студентов появилась возможность по управлению государством, то наиболее действенным они считают ужесточение законодательства (21%), воспитание населения (10%). Так результаты исследования показывают, что наиболее эффективными мерами по борьбе с экстремизмом должны быть: ужесточение законодательства за данное преступление и воспитание населения.

В своей анкете мы предложили ответить респондентам на вопрос, каким образом можно внедрить антиэкстремистскую составляющую в учебный процесс (школа, колледж, вуз).

Наиболее популярными ответами среди студентов юридического факультета, являлись (таблица 10).

Таблица 10 — Наиболее популярные ответы

Меры внедрения	**Количество респондентов, поддерживающие предложенную меру**
Развитие молодежных движений (культура, спорт)	0
Воспитательное воздействие	2
Профилактика	12

1.5 Анализ результатов анкетирования студентов 5 курса

В результате проведенного опроса среди студентов Волжского университета им. В.Н. Татищева были получены следующие результаты (таблица 11).

Таблица 11 — Анализ результатов анкетирования студентов 5 курса юридического факультета.

Параметры определения экстремистской обстановки	**Индексы показателей**
Уровень экстремизма	-0,174
Готовность к проявлению/непроявлению социальной нетерпимости	0,478
Состояние защищенности от проявлений экстремизма	0,391
Обобщенный показатель	0,232

Индекс первого компонента «характеристика уровня экстремизма» составил -0,174, что является неопределенным показателем.

Индекс второго компонента «Готовность к проявлению/не проявлению социальной нетерпимости» составил 0,478, что также является положительным показателем.

Индекс третьего компонента «состояние защищенности от проявлений экстремизма» составил 0,391, что является положительной оценкой.

Обобщенный индекс, определяющий уровень экстремистской обстановки, основанный на оценке студентами - юристами 5 курса ВУиТ, равняется 0,232, что является неопределенным показателем.

Большинство опрошенных (65%) экстремизм рассматривают в качестве формы политической деятельности, отрицающую демократические принципы и основанную на идеологии социальной нетерпимости, национализма, ксенофобии и антисемитизма.

Подавляющие число респондентов считают, что уровень экстремизма в России средний — (30%), высокий — 8%, и низкий — 17%.

В следующем вопросе о столкновении с дискриминацией по национальному, религиозному и иному признаку в отношении другого человека большинство респондентов 34% ответили «да», 26% - «скорее не, чем да», 13% поделили ответы «скорее да, чем нет», «затрудняюсь ответить», «нет».

Студенты на вопрос: «В каком источнике, по вашему мнению, можно чаще встретить пропаганду экстремистской деятельности (социальной, расовой, религиозной, национальной нетерпимости)?» единогласно ответили — интернет, что составляет 100% из всех опрошенных.

Вопрос о том, знают ли студенты о существовании в городе Тольятти экстремистских организаций (движений) показал, что 39% - слышали, но лично не сталкивались и 60% ничего не слышали об этом.

На вопрос: «Какой, на ваш взгляд, уровень экстремизма в Самарской области?» 60% респондентов ответили, уровень является средним, 34% - что он низкий, и только 4% что он высокий.

Однако, на вопрос «случалось ли вам быть свидетелем этнической нетерпимости по отношению к представителям какой-либо национальности?» большинство респондентов 39% ответили «скорее нет, чем да», 26% периодически, 17% многократно, 13% «затрудняюсь ответить», и лишь 4% ответили «определенно нет».

Отношение респондентов в вопросе согласны ли вы, с утверждением «Россия для русских», можно считать положительным так, как 56% ответили «определённо нет», 26% «скорее нет чем да», 14% « затрудняются в своём ответе» и лишь 13 % считают, что «скорее да, чем нет».

Респондентам было предложено выделить наиболее значимые проблемы современной России, путем расставления предложенных вариантов с 1-го по 13-е место (таблица 12).

Таблица 12 – Наиболее важные проблемы современной России

а) коррупция	1
в) безработица	3
в) терроризм	4
г) экстремизм	9
в) экономическая нестабильность	2
е) расслоение общества	6
ж) преступность	5
з) социальные протесты	13
и) пенсионная реформа	12
к) внешние угрозы	8
и) допинговый скандал	10
к) дефицит бюджета	11
л) цены на нефть и газ	7

В вопросе «Важна ли для вас национальность, религиозная принадлежность при выборе друзей»? мнение респондентов разделилось на две группы, причём подавляющее число респондентов 90% считают «определённо нет» и «скорее нет, чем да». Вторая группа 8% считает «определённо да» и «скорее да, чем нет».

Мнение опрашиваемых на вопрос «как бы вы отнеслись к открытию лагерю беженцев в г. Тольятти»? «Скорее, против» считают 34% респондентов, 30% опрошенных «затрудняются в ответе», 21% «категорически против», и лишь 8% - «Скорее положительно», 4% - «Однозначно положительно».

Негативно студенты 5 курса отнеслись к людям с нетрадиционной сексуальной ориентацией: 4% придерживаются мнения, что их надо лечить, 4% изолировали бы их от общества, 17% оказали психологическую и иную помощь, 39% предоставили бы их самим себе и 17% затрудняются ответить.

Также разделилось мнение респондентов по следующему вопросу «Согласны или не согласны с тем, что присутствие мигрантов в нашем городе чрезмерно?», большинство отвечающих 34% затруднились с ответом, 30% ответили «скорее, да», 21% «скорее нет» и 8% ответили «нет», и лишь 4% ответили «определённо, да».

На вопрос «как вы относитесь к идее проведения русских маршей?» ответы респондентов сильно разошлись во мнениях так, как 60% опрошенных считают «Скорее, отрицательно» и «Определённо отрицательно», 30% составило часть респондентов, которые «ничего об этом не слышали» и только 4% отнеслись «определённо положительно» к этой идее.

Вопрос: «Считаете ли вы себя защищённым от проявления экстремизма»? показал, что мнение респондентов совпадает как «определённо нет» и «скорее, нет» - 38%, что равно ответам «скорее да» и «определённо да» - 38%, и лишь 21% на этот вопрос затрудняются ответить.

«Возможны ли в настоящее время в России массовые кровопролитные столкновения на националистической почве»? Ответы респондентов разделились следующим образом, самое большое число отвечающих составило 39% - «скорее нет, чем да», 21% затрудняются ответить и 35% «определённо да» и «скорее да, чем нет».

Большинство респондентов 52%, на вопрос « Ощущаете ли вы в г. Тольятти межнациональную напряжённость»? Ответили «скорее нет» и «определённо нет», 12% ответили «определённо да» и «скорее да», и 26% затруднились ответить.

Мнение студентов 5 курса на вопрос «Чувствуете ли вы в настоящее время враждебность со стороны людей других национальностей?» сложилось следующим образом, где 69% ответили «редко» и «никогда, практически никогда», 21% затрудняются в ответе, 4% «довольно часто».

«Возможны ли в настоящее время в Самарской области массовые кровопролитные столкновения на националистической почве»? Ответы респондентов разделились следующим образом, самое большое число отвечающих составило 43% - «скорее нет, чем да» и «определённо нет», 47% затрудняются ответить и 8% «определённо да» и «скорее да, чем нет».

Если бы у студентов появилась возможность по управлению государством, то наиболее действенными они считают ужесточение законодательства (8%), профилактика – 6%. Так результаты исследования показывают, что наиболее эффективным мерами по борьбе с экстремизмом должны быть: ужесточение законодательства за данное преступление и профилактика.

В своей анкете, мы предложили ответить респондентам на вопрос, каким образом можно внедрить антиэкстремистскую составляющую в учебный процесс (школа, колледж, вуз).

Наиболее популярными ответами среди студентов юридического факультета, являлись (таблицы 13,14).

Таблица 13 – Наиболее популярные ответы

Меры внедрения	Количество респондентов, поддерживающих предложенную меру
Развитие молодежных движений (культура, спорт)	8
Воспитательное воздействие	19

Таблица 14 — Идея цензуры сети Интернет

Отрицательно	3
Нейтрально	6
Положительно	12

Глава 2. Сравнение результатов анкетирования по курсам обучения

В результате анкетирования студентов 1-5 курса юридического факультета, большинство опрошенных считают, что экстремизм – форма политической деятельности, отрицающая демократические принципы и основана на идеологии социальной нетерпимости, национализма, ксенофобии и антисемитизма.

На вопрос: «Какой, на ваш взгляд, уровень экстремизма в России?» студенты единогласно отвечают – «средний».

На вопрос о направлении изменения уровня экстремизма в РФ через 3 года, большинство студентов 2-5 курса отвечают, что уровень экстремизма увеличится, 1 курс указал, что уровень экстремизма не изменится.

Отвечая на вопрос «Сталкивались ли вы с дискриминацией по национальному, религиозному и иному признаку в отношении другого человека?» большинство респондентов сталкивалось с данной ситуацией.

Исходя из сравнительного анализа данных, полученных в ходе ответа на вопрос: «В каком источнике можно чаще встретить пропаганду экстремисткой деятельности?» большинство студентов-юристов считают источником такой деятельности СМИ и Интернет. Однако студенты 5 курса единогласно выделяют основным источником - Интернет.

Единогласно студенты 5 курса ответили, что они не согласны с утверждением «Россия для русских».

Респонденты 1 и 5 курса проблема экстремизма в России не является значимой, но студенты 2, 3, 4 курса полагают, что проблема экстремизма актуальна для современной России.

Касаясь вопроса «Чувствуете ли вы себя защищенным от проявления экстремизма?» студенты 1 курса выразили позицию о том, что они не чувствуют себя защищенными от проявления экстремизма.

Оптимистическое настроение можно наблюдать на примере вопроса «Важна ли национальность, религиозная принадлежность при выборе друзей?» определенно не важна, считают большинство опрошенных.

Касаясь вопроса о вступление в экстремистскую организацию, обобщили полученные результаты и выявили следующее, что 144 опрошенных студентов-юристов, 14 респондентов готовы за вознаграждение вступить в экстремистские организации.

Мнения респондентов по вопросу открытия лагеря беженцев в городе Тольятти разделились, студенты 1, 2 курса категорически против, студенты 3, 4, 5 курса затрудняются ответить.

Негативно студенты 1 курса отнеслись к людям с нетрадиционной сексуальной ориентации, остальные респонденты придерживаются мнения, что их нужно предоставить самим себе.

Исходя из сравнительного анализа данных, полученных в ходе ответа на вопрос «Какие меры возможно предпринять для борьбы с экстремизмом?» большинство студентов поддерживают позицию, что необходимо усовершенствование законодательства и ужесточение наказания за экстремистские преступления.

В своей анкете мы предложили ответить респондентам на вопрос: «Каким образом можно внедрить антиэкстремистскую составляющую в учебный процесс (школа, колледж, вуз)». Наиболее популярными ответами студентов юридического факультета были (таблицы 15, 16):

Таблица 15 - Наиболее популярные ответы

Меры внедрения	**Количество респондентов, поддерживающих предложенную меру**
Развитие молодежных движений (культура, спорт)	56
Воспитательное воздействие	26
Профилактика	15

Таблица 16 - Отношение респондентов к цензуре в сети «Интернет»

Положительно	51
Нейтрально	22
Отрицательно	33

Глава 3. Анализ результатов анкетирования фокус-группы

В результате проведенного опроса, были получены следующие результаты (таблица 17).

Индекс первого компонента «характеристика уровня экстремизма» 0 ,что является неопределенной оценкой.

Индекс второго компонента «готовность к проявлению/ непроявлению социальной нетерпимости» составил 0,341, что является положительной оценкой.

Индекс третьего блока «состояние защищенности от проявления экстремизма» составил 0,5, что также является положительной оценкой.

Таблица 17 – Анализ результатов анкетирования фокус-группы

Параметры определения экстремистской обстановки	Индексы показателей
Уровень экстремизма	0
Готовность к проявлению / непроявлению социальной нетерпимости	0,341
Состояние защищенности от проявления экстремизма	0,5
Обобщенный показатель	0,28

Обобщенный индекс, определяющий уровень экстремистской обстановки, основанный на оценке респондентов, равняется - 0,28. Как видно, обобщенный индекс характеризует экстремистскую обстановку как неопределенную, но стоящую на границе с положительным коэффициентом.

Большинство опрошенных (40%) экстремизм рассматривают в качестве приверженности крайним взглядам/мерам.

Подавляющее большинство респондентов считают, что уровень экстремизма средний – 61%, низкий –34%. За высокий уровень высказались 1 % респондентов.

Однако в вопросе «Об изменения уровня экстремизма в России через 3 года» высказались 2% - быстро увеличиться, 45% - увеличится, 19% - не изменится и 3% - снизится.

На вопрос «Сталкивались ли вы с дискриминацией по национальной, религиозной и иному признаку в отношении другого человека», 22% ответили, что никогда не сталкивались, скорее нет чем да – 13%, затрудняюсь ответить – 6%, скорее да чем нет – 38% и лишь 20% ответили что сталки-

ваются часто. Из этого следует вывод, что около половины респондентов либо никогда в жизни не сталкивались данными явлениями, либо сталкивались часто. Это показывает, что их мнение формируется исходя из обобщенных представлений положения дел в рассматриваемом вопросе, которые складываются, в основном, по средством получения информации из СМИ и интернета, что подтверждает уже следующий вопрос, где респондентов спрашивали в каком источнике можно чаще всего встретить пропаганду экстремистской деятельности: 20% - СМИ, 63% - интернет, баннеры, листовки, граффити – 13% , иные 4%.

Оптимистическим настроение наших респондентов назвать тоже очень тяжело. Например, на последующие вопросы: «Случалось ли вам быть свидетелем этнической нетерпимости по отношению к представителям какой-либо национальности» большинство респондентов ответили «периодически».

Так же разделилось мнение опрашиваемых по вопросу – «Согласны ли вы с утверждением «Россия для русских»», 38% респондентов ответили – определенно нет, 29% - скорее нет, чем да, 11% - скорее да, чем нет, 2% - определенно да, а 20% студентов затруднились однозначно ответить.

Респондентам было предложено выделить наиболее значимые проблемы современной России, путем расставления предложенных вариантов с 1-го по 13-е место (таблица 18).

На вопрос «Считаете ли вы себя защищенным от проявления экстремизма», определенно да ответили 6% респондентов, скорее нет – 31%, затрудняюсь ответить - 27%, скорее да – 25%, определенно нет – 6%. Респонденты, не чувствующие своей защищённости, беспокоюсь за своих близких – 4%, беспокоятся за себя и за своих близких – 40%.

Вопрос о том, знают ли опрашиваемые о существовании в городе Тольятти экстремистских организаций (движений) показал, что 2% довольно часто сталкиваются с их представителями, 22% - слышали, но лично не сталкивались и 75% ничего не слышали об этом.

По мнению опрашиваемых, решение проблемы экстремизма зависит от населения – 20% и от воспитания в семье – 52%, от правоохранительных органов -15%, свой вариант -6 %.

Для большинства респондентов при выборе друзей не важна национальная и религиозная принадлежность, так считают 54%, 6% затруднятся ответить на этот вопрос, и для 2% этот критерий важен.

Позитивным показателем является то, что среди опрошенных большая часть, которых составила 97% не готовы вступить в экстремистскую организацию и 2% готовы вступить.

Мнение респондентов по вопросу открыть лагерь беженцев в городе Тольятти разделилось, 9% допускает открытие лагеря, 27% затрудняются ответить, а 63% против данной идеи.

Негативно респонденты отнеслись к людям с нетрадиционной сексуальной ориентацией: 4% придерживаются мнения, что их надо лечить, 13% изолировали бы их от общества, 2% физически уничтожили, 31% оказали психологическую и иную помощь, 31% предоставили бы их самим себе и 9% затрудняются ответить, ваш вариант 2%.

Таблица 18 – Наиболее важные проблемы современной России

а) коррупция	1
в) безработица	5
в) терроризм	3
г) экстремизм	9
в) экономическая нестабильность	2
е) расслоение общества	8
ж) преступность	7
з) социальные протесты	12
и) пенсионная реформа	11
к) внешние угрозы	4
и) допинговый скандал	13
к) дефицит бюджета	6
л) цены на нефть и газ	10

Если бы у респондентов появилась возможность по управлению государством, то наиболее действенными они считают ужесточение законодательства – 8, профилактика – 3, общесоциальные меры – 9. Так результаты исследования показывают, что наиболее эффективным мерами по борьбе с экстремизмом должны быть: ужесточение законодательства за данное преступление и воспитание населения.

В своей анкете, мы предложили ответить респондентам на вопрос, каким образом можно внедрить антиэкстремистскую составляющую в учебный процесс (школа, колледж, вуз).

Наиболее популярными ответами среди респондентов являлись (таблица 19).

Таблица 19 – Наиболее популярные ответы

Меры внедрения	Количество респондентов, поддерживающие предложенную меру
Развитие молодежных движений (культура, спорт)	56
Воспитательное воздействие	20
Профилактика	8

Глава 4. Сравнение результатов опросов студентов юридического факультета с опросом фокус-группы

В результате анкетирования студентов юридического факультета с 1-5 курс и фокус группы (взрослые), большинство опрошенных студентов считают, что экстремизм – форма политической деятельности, отрицающая демократические принципы и основана на идеологии социальной нетерпимости, национализма, ксенофобии и антисемитизма, в свою очередь взрослые респонденты ответили, что экстремизм – приверженность к крайним взглядам, мерам.

На вопрос: «Какой, на ваш взгляд, уровень экстремизма в России?» все единогласно ответили – средний.

Что касается вопроса «Изменится ли, на ваш взгляд, уровень экстремизма в России через 3 года?» большинство студентов 2-5 курса и фокус группа отвечают, что уровень экстремизма увеличится. А 1 курс указал, что уровень экстремизма не изменится.

Отвечая на вопрос «Сталкивались ли вы с дискриминацией по национальному, религиозному и иному признаку в отношении другого человека?» мнения всех опрошенных сошлись в том, что они скорее сталкивались.

Исходя из сравнительного анализа данных, полученных в ходе ответа на вопрос «В каком источнике можно чаще встретить пропаганду экстремистской деятельности?» большинство опрашиваемых из обеих групп считают источником такой деятельности – интернет.

Единогласно студенты 5 курса ответили, что они не согласны с утверждением «Россия для русских», а мнение фокус группы разделилось. 2% ответили определенно да, 11% скорее да, чем нет, 20% затрудняются ответить, 29% скорее нет, чем да и 38% определенно нет.

На вопрос «Какая на ваш взгляд основная причина экстремизма?» студенты юридического факультета ответили – нагнетание национальных, религиозных, политических противоречий в обществе и СМИ, а большинство опрошенных из фокус-группы считают, основная причина – развёрнутая информационная война против России.

Касаемо вопроса «Чувствуете ли вы себя защищёнными от проявления экстремизма?» студенты 1 курса и фокус группы ответили, что не чувствуют себя в безопасности.

Оптимистическое настроение можно наблюдать на примере вопроса «Важна ли национальность, религиозная принадлежность при выборе друзей?». Большинство респондентов считают, что определенно не важна.

Исходя из сравнительного опроса данных, полученных в ходе ответа на вопрос «Вступили бы вы в экстремистскую организацию, если бы вам предложили вознаграждение?» лишь небольшая группа опрошенных (15 человек) готовы вступить.

Фокус группа более гуманно отнеслась к людям с нетрадиционной сексуальной ориентацией, предложив оказывать им помощь и предоставлять их самим себе.

Мнения респондентов по вопросу межнациональной напряженности в городе Тольятти разошлись, 52 человека считают что обстановка накалена, а оставшаяся часть опрошенных не видят в этом проблему.

В своей анкете мы предложили ответить респондентам на вопрос «Каким образом можно внедрить анти экстремистскую составляющую в учебный процесс (школа, колледж, вуз)». Наиболее популярными ответами студентов юридического факультета были (таблицы 20, 21):

Таблица 20 - Наиболее популярные ответы студентов

Меры внедрения	**Количество респондентов, поддерживающих предложенную меру**
Развитие молодежных движений (культура, спорт)	56
Воспитательное воздействие	46
Профилактика	23

Таблица 21 - Отношение респондентов к цензуре в сети «Интернет»

Положительно	70
Нейтрально	22
Отрицательно	42

Глава 5. Предложения и рекомендации по формированию ценностной антиэкстремистской установки обучающихся юридического факультета Волжского университета имени В.Н. Татищева

На основании проведенного анализа анкетирования среди студентов 1- 5 курсов и фокус-группы, нами предлагаются следующие рекомендации по формированию ценностной антиэкстремистской установки обучающихся юридического факультета Волжского университета имени В.Н. Татищева:

Проведение интерактивов (конференций, круглых столов и т.п.) для студентов 1-5 курсов. Темы для обсуждений:

А) для 1 курса: «Экстремизм в истории России», «Определение понятия экстремизм», «Международный экстремизм»;

Б) для 2 курса: «Основные международные конвенции по противодействию экстремистской деятельности» (Обзор), «Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15.06.2001 года», «Резолюция Парламентской Ассамблеи Совета Европы 2003 года»;

В) для 3 курса: «Понятие и формы экстремизма по российскому законодательству», «Субъекты, осуществляющие противодействие экстремистской деятельности», «Международное сотрудничество в области борьбы с экстремизмом»;

Г) для 4 курса: «Уголовное преследование за экстремизм в РФ», «Профилактика подросткового и молодежного экстремизма», «Криминалистические аспекты в расследовании преступлений экстремистского характера»;

Д) для 5 курса: «Личностно-психологические основы экстремизма», «Политический экстремизм в современной России», «Основные социально-политические проблемы и стратегии противодействия экстремизму в системе мере по обеспечению национальной безопасности России».

2. Организация тематических встреч с сотрудниками уполномоченных государственных органов, осуществляющих профилактику и борьбу с экстремизмом (ФСБ, Прокуратура, МВД).

3. Внесение изменений в Правила внутреннего распорядка ВУиТ, предусматривающих санкции за проявления расовой, национальной и религиозной нетерпимости.

4. Формирование студенческого актива по предупреждению случаев проявления расовой, национальной и религиозной нетерпимости.

5. Введение в образовательную программу курса «Культурные особенности и традиции народов, проживающих на территории РФ», либо соответствующих тем в учебный курс по культурологии.

6. Организация и проведение культурно-образовательных студенческих маршей и шествий с участием представителей различных национальностей.

7. Проведение тематических мероприятий на базе университета (выставок, музыкальных национальных вечеров и т.п.).

8. Организация в университетах комнат по отправлению религиозных верований.

9. Обеспечение психологической помощи пострадавшим от локальных проявлений экстремизма.

10. Обмен культурным опытом и сотрудничество вузов, студенческих организаций на региональном, всероссийском и международном уровне (программы по обмену студентов, видеоконференции, форумы и т.п.).

Библиографический список

1. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) "О противодействии экстремистской деятельности".

2. "Концепция общественной безопасности в Российской Федерации" (утв. Президентом РФ 14.11.2013 № Пр-2685).

3. Приговор Самарского областного суда № 02-62/2010 от 1 ноября 2010 г. по делу № 02-62/2010.

4. http://www.levada.ru/2016/10/11/intolerantnost-i-ksenofobiya/

5. https://мвд.рф

6. Агрессия: причины, последствия, контроль. М., Олма-пресс. 2009. с. 207.

7. Афанасьев, Н.И. Идеология терроризма // Социально-гуманитарные знания.2002, № 1.с.25.

8. Верещагин, В.Ю., Лабунец, М.И. Политический экстремизм в контексте модернизации современной российской государственности // Философия права. - Ростов - на - Дону: Изд-во Рост.юрид. ин-та МВД России, 2002, № 2, с.84.

9. Оценка коррупционной и антикоррупционной установки студентов (на основе опроса студентов юридического факультета «ВУиТ») //Вестник по безопасности. – №8, 2015, Тольятти: ВУиТ.

10. Психология установки / Дмитрий Узнадзе. - СПб. [и др.]: Питер, 2001.

11. Саморегуляция и прогнозирование социального поведения личности: Диспозиционная концепция. 2-е расширенное изд. — М.: ЦСПиМ, 2013.

12. Сергун, Е.П. Правовое обеспечение экстремистской деятельности в Российской федерации // Правовая политика и правовая жизнь. 2006. № 2, с.197.

13. Сигарев, А.В. Правовое регулирование противодействия экстремизму: курс лекций: - Новосибирск: СибАГС, 2015. – С.13-14.

14. Улезко, Э.В. Экстремизм и терроризм: понятийно-категориальный аппарат исследования явления //www.kai.ru.

15. Ядов, В.А. О диспозиционной регуляции социального поведения личности // Методологические проблемы социальной психологии. 1975. с. 97.

16. Ядов, В.А., Магун, В.С., Борзикова, П.В., Водзинская, В.В., Каюрова, В.Н., Саганенко, Г.И., Узунова, В.Н., Семенов, А.А. Саморегуляция и прогнозирование социального поведения личности / Под. ред. В.А. Ядова. Л.: Наука, 1979.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПАНИИ ПРИ ИСПОЛЬЗОВАНИИ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ УДАЛЕННОГО ДОСТУПА СОТРУДНИКОВ К КОРПОРАТИВНОЙ СЕТИ

Андреев А.А., студент
Научный руководитель: к.т.н., доцент О.Ю. Федосеева
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Аннотация. В этой статье рассмотрены наиболее распространенные виды предоставления удаленного доступа к корпоративным ресурсам. Их достоинства и недостатки, а также некоторые нюансы их настройки.

Ключевые слова: удаленный доступ, RDP, VPN, DirectAcces, IPSec, NAP.

В век высоких технологий и информатизации общества информация становится одним из самых важных ресурсов бизнеса и главным элементом производственных сил. Предоставление доступа к информационным активам компании через удаленное подключение является одним из наиболее перспективных направлений развития информационных систем. Уже сейчас, согласно статистическим исследованиям, более 40% сотрудников работают удаленно хотя бы один день в неделю. Опрос J'son & Partners Consulting, в котором приняли участие 315 руководителей из разных компаний в 15 регионах страны, показал, что в России более 40% фирм работает с удаленными сотрудниками. А если верить исследованию, проведенному Vanson Bourne по заказу Citrix, к 2020 году треть служащих в России не будет проводить все рабочее время в офисе. Сотрудники компаний смогут работать из дома (38,4%), или на площадках, где ведутся проекты (26%), или на территории заказчика (31%). Российские компании будут предоставлять в среднем 7 рабочих мест на 10 сотрудников, при этом каждый работник будет иметь доступ к корпоративной сети в среднем с шести различных устройств. Это выгодно и работодателям, и сотрудникам компаний. 66% компаний, которые перешли на мобильный формат работы, уже оценили выгоды, связанные со снижением издержек. 20% российских компаний, которые участвовали в опросе, уже используют такой формат работы. При этом доля «мобильных» компаний сильно варьируется в зависимости от отрасли. Для работников основные преимущества удаленной работы заключаются в сокращении времени на переезды (55%), улучшении показателей производительности труда (34%), повышении мобильности (32%), улучшении соотношения работы и личной жизни (20%). Компаниям мобильный формат работы помогает снижать расходы, связанные с персоналом (32%) и недвижимостью (34%), а также привлекать (27%) и удерживать (23%) высококвалифицированные кадры.

Помимо преимуществ, вытекающих из мобилизации сотрудников, очевидны также и проблемные зоны – прежде всего это безопасность данных, доступных при удаленном доступе. Большинство российских компаний игнорирует вопросы безопасности удаленного доступа и мобильной безопасности и никаким образом не контролирует доступ к корпоративным сервисам и файлам с личных устройств сотрудников.

Существует несколько способов организовать доступ клиента к корпоративным сервисам и каждый из них имеет свои плюсы и минусы. Рассмотрим самые распространенные из них по очереди.

RDP-клиент (подключение посредством удаленного рабочего стола).

Удаленный рабочий стол — это один из наиболее распространенных, удобных, универсальных и часто используемых инструментов, дающих возможность удаленного доступа к рабочему месту. С точки зрения технической реализации для клиента не нужны никакие дополнительные ресурсы и оборудование. Клиент удаленного рабочего стола или Remote Desktop Client – программное обеспечение кроссплатформенное и на сегодняшний день существуют клиенты практически для всех операционных систем семейства Windows, Linux, FreeBSD, Mac OS X, iOS, Android, Symbian, поэтому может быть реализовано где угодно, вплоть до планшетов и смартфонов. Такой клиент использует свой протокол RDP (Remote Desktop Protocol), купленный Microsoft у компании Citrix.

Безопасность же этого решения может только желать лучшего. Используя этот вид удаленного подключения, мы подвергаем опасности не только передаваемую информацию, но и открываем серьезную «дыру» в безопасности самого сервера. «Дыра» в безопасности сервера обуславливается тем, что мы открываем прямой доступ на сервер не только клиентам, но и всем пользователям Интернет и соответственно сервер подвергается различным атакам из вне, что очень небезопасно, поскольку в истории протокола RDP можно насчитать несколько найденных критичных уязвимостей, с

помощью которых взламывали сервера. И если безопасность передаваемой информации на сервер с помощью этой технологии можно зашифровать встроенными средствами клиента удаленного рабочего стола (возможность использования 128-битовое шифрование по алгоритмам RC4, AES или 3DES с проверкой целостности хешем MD5 или SHA1, технология Remote Desktop Gateway (шлюза удаленных рабочих столов) использование TLS шифрования), то проблему в безопасности сервера при прямом доступе к серверу закрыть невозможно.

Так же здесь стоит упомянуть о такой технологии как веб-доступ к службам терминалов. это удобно для конечного пользователя, ведь доступ к определенным приложениям и рабочим столам организуется с помощью браузера, который сегодня установлен на подавляющем большинстве устройств. а от пользователя требуется ввести соответствующий URL для доступа к ресурсу, пройти проверку подлинности и авторизацию, после чего открывается доступ к приложениям или удаленному рабочему столу средствами web.

Клиент VPN

VPN (Virtual Private Network) представляет собой виртуальную частную сеть, позволяющую обеспечить одно или несколько надежных сетевых соединений поверх такой небезопасной сети, как Интернет, используя при этом различные средства криптографии. При подключении через VPN со стороны пользователя устанавливается исходящее VPN-подключение, которое пользователь использует по необходимости. Для реализации доступа к удаленному ресурсу пользователь запускает ярлык VPN, вводит свои верительные данные и, при успешной проверке подлинности, получает доступ к необходимым ресурсам. Иными словами, компьютер пользователя, за счет выданных при VPN-подключении параметров IP-конфигурации, попадает в сеть виртуального удаленного офиса в облаке и может использовать ресурсы так, как если бы он находился непосредственно в офисе (в локальной сети) компании. При использовании технологии VPN есть возможность использования специального ключа для хранения сертификатов для подключения к серверу. Такой электронный ключ называют донгл. Сейчас донгл чаще встречается с usb форм-фактором. Суть такого решения заключается в том, что на донгл записывается и шифруется сертификат пользователя. Подключение к серверу осуществляется только при условии подключенного к машине донгла. Сертификат на донгле шифруется и обычно защищен паролем, поэтому доступ на сервер получается с 3-х факторной защитой:

- получение физического доступа к донглу и подключение его к устройству;
- пароль к сертификату на донгле для построения туннеля между клиентом и сервером;
- пароль для входа на сервер.

Но при всех плюсах безопасности подключения типа VPN существует и обратная сторона медали.

- Клиент VPN подключается к корпоративной сети нерегулярно, а иногда и не подключается вовсе, вследствие чего выпадает из-под действия групповых политик и других систем управления.
- Клиент VPN подвержен воздействию неуправляемых или плохо управляемых сетей, что увеличивает область атак, к которым клиент VPN с удаленным доступом может оказаться уязвим.
- Клиент VPN получает доступ к Интернету, и пользователи могут делать все что угодно при этом, ведь обычно никто не фильтрует содержимое Интернета, когда клиент VPN не подключен к корпоративной сети.

Конечно же, здесь необходимо применять ряд профилактических мер, чтобы при попадании обратно в корпоративную сеть клиент VPN не причинил вреда и не стал «пробелом» в безопасности сети. От физических атак сюда можно отнести шифрование дисков (например, Bitlocker), требование двухфакторной авторизации для входа в систему, причем второй фактор также требуется для разблокировки машины или выхода из спящего режима. От заражения сети такими машинами можно разворачивать NAP (Network Access Protection), для проверки безопасности в конечной точке перед тем, как разрешать машине доступ в корпоративную сеть. Если машина не проходит проверку, в корпоративную сеть она не попадает. Эти действия могут значительно помочь в уменьшении угроз безопасности от клиентов VPN с удаленным доступом.

DirectAccess. DirectAccess позволяет реализовать возможность удаленного доступа к ресурсам корпоративной сети следующим образом: как только компьютер пользователя подключается к сети Интернет, он сразу получает доступ и к ресурсам Интернета, и ко всей корпоративной сети. Пользовательский компьютер, сконфигурированный в качестве клиента DirectAccess, автоматически устанавливает туннель до сервера DirectAccess и через него получает доступ ко всей корпоративной сети. При этом от пользователя не требуется никаких дополнительных действий. Туннель между клиентом и сервером DirectAccess устанавливается автоматически, и этот процесс для пользователя абсолютно прозрачен. Не нужно запускать какие-либо VPN-соединения, не нужно вводить учетные данные — логин и пароль, пин-код для смарт-карты и пр. Более того, если связь с интернетом на какое-то время

теряется (и при этом, естественно, разрывается туннель), а затем восстанавливается, то опять же автоматически, без участия пользователя восстанавливается и туннель в корпоративную сеть.

В целом эта технология предоставления удаленного доступа очень схожа с VPN. Однако имеются очень важные различия. Все время, пока есть связь с интернетом, и существует туннель, клиентский компьютер доступен для управления со стороны ИТ-служб компании. Иными словами, благодаря DirectAccess не только пользователь может постоянно работать с корпоративными ресурсами, но и другие сотрудники, в первую очередь ИТ-отдел и администраторы сети, имеют доступ к компьютеру пользователя. Пользователь все время находится «под колпаком» у ИТ-служб. С практической точки зрения этот факт дает возможность осуществлять мониторинг клиентской машины – проверку антивирусных баз, последних обновлений, включенного firewall и пр. – даже если она находится за пределами корпоративной сети. Также вручную разорвать DirectAccess-туннель не так просто, как в случае с VPN-соединением, которое, как правило, визуально отображается в сетевых подключениях. А вкупе с теми же мерами безопасности, которые я описал в разделе про клиентов VPN, мы получаем вполне себе безопасную и удобную технологию для удаленного доступа к корпоративным данным.

Конечно, DirectAccess, разворачивается сложнее, чем VPN, здесь кроме выделенного сервера нам понадобится протокол IPv6 для связи DA-клиента с DA-сервером и компьютерами интрасети; протокол IPSec поверх IPv6 для защищенной передачи данных по Интернет сети; протоколы, поддерживающие прохождение IPv6 через сети IPv4, например, Teredo — протокол, позволяющий тунелировать трафик IPv6 (это необходимо, т.к. не все маршрутизаторы поддерживают IPv6). Но поскольку клиент DirectAccess всегда управляем, всегда обновляем и всегда находится под контролем и руководством IT-отдела компании, степень угрозы при работе с ним действительно намного ниже, чем та, которая обеспечивается удаленным клиентом VPN.

В заключении хочу отметить, что на данный момент не существует метода, который бы позволил полностью обезопасить компанию от утечки данных при работе с удаленными сотрудниками. Но этот сегмент работников отрицать нельзя. Поэтому стоит уделять больше внимания ИТ-специалистам в области безопасности сети, корпоративных ресурсов и пр. Какой метод удаленного подключения использовать, конечно, полностью зависит от потребностей удаленных сотрудников и требований по защищенности передаваемой информации. Но самой актуальной и интересной на сегодняшний день является технология DirectAccess.

Библиографический список

1. Удаленные подключения и их защита в интернете. URL: http://efsol.ru/articles/protection-remote-connections.html.

2. Руководство по установке и настройке OpenVPN. URL: https://habrahabr.ru/post/ 233971/.

3. Удаленный доступ и утечка данных URL: http://www.itsec.ru/articles2 /Inf_security/udalennyy-dostup-i-utechka-dannyh/.

4. Подключение пользователей к корпоративному облаку URL: https://habrahabr.ru/ company/it-grad/blog/252861/.

5. DirectAccess в Windows 7. URL: https://habrahabr.ru/company/microsoft/blog/105979/.

6. Удобства Direct Access URL: http://www.osp.ru/winitpro/2009/11/13000854/.

7. DirectAccess и VPN: Это НЕ одно и то же URL: https://blogs.technet.microsoft.com/ru_forum_support/2011/01/13/directaccess-vpn/.

8. *Пятая часть россиян будет работать удаленно к 2020 году URL:* http://www. rbc.ru/ technology_and_media.

ОСНОВНЫЕ ПОДХОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Аникеев В.М., Гуренков Е.В.*, студенты*
Научный руководитель: ст. преподаватель Е.В. Плюснина, Н.Г. Губанов***
**ОАНО ВО «Волжский университет имени В.Н. Татищева»*
г. Тольятти, Россия
*** ФГБОУ ВО «Самарский государственный технический университет»*
г. Самара, Россия

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью утраты, преломление и раскрытия данных, адресованных

либо принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития ИТ.

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей с учетом определений ГОСТ Р 50922—96.

Защита информации — это деятельность по предотвращению утечки оберегаемой информации, несанкционированных и непреднамеренных действий на оберегаемую информацию.

Объект защиты — информация, обладатель информации или информационный процесс, в отношении которых нужно обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации или несанкционированного и непреднамеренного действия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения оберегаемой информации от ее разглашения, несанкционированного доступа (НСД) к оберегаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения оберегаемой информации до неконтролируемого количества получателей информации.

Под информационной безопасностью понимают защищенность информации от преступного ознакомления, преобразования и ликвидирования, а также защищенность информационных ресурсов от действий, направленных на нарушение их работоспособности. Природа этих действий может быть самой различной.

Это и попытки проникновения злоумышленников, и ошибки персонала, и вывод из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар) и т. п.

Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из огромного числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Фактически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты АС можно разбить на следующие группы:

– аппаратные средства — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);

– программное обеспечение — приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

– данные — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

– персонал — обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в АС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, соответствуют физические представления в компьютерной среде:

– для представления информации — машинные носители информации в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;

– объектам системы — пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;

– субъектам системы — функциональные составляющие системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Рассмотри современные методы защиты информации:

1. Препятствие;
2. Маскировка;
3. Регламентация;
4. Управление.

Все приведенные способы нацелены на построение действенной технологии охраны информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Под препятствием понимается метод физической охраны информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка — способы охраны информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Регламентация — важнейший метод охраны информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Управление — способы охраны информации, при которых осуществляется управление над всеми компонентами информационной системы.

Способы охраны информационных систем. Способы охраны информации подразумевают использование определенного набора средств. Для предотвращения утраты и утечки секретных сведений используются следующие средства:

1. Физические;
2. Программные и аппаратные;
3. Организационные;
4. Законодательные;
5. Психологические.

Главным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди или специальные системы. С целью предотвращения утрат информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях.

Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства — программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, исполняющие восстановление утраченных сведений. При поддержки комплекса аппаратуры и программ обеспечивается резервное копирование информации — для предотвращения потерь.

Организационные средства сопряжены с несколькими методами охраны: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При действенном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или утрату данных.

Законодательные средства — комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к оберегаемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Психологические средства — комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе компании.

Классы безопасности информационных систем.

1. D — нулевой уровень безопасности;
2. C — системы с произвольным доступом;
3. B — системы с принудительным доступом;
4. A — системы с верифицируемой безопасностью.

Уровню D подходят системы, в которых слабо развита технология защиты. При такой ситуации любое постороннее лицо имеет возможность получить доступ к сведениям.

В уровне C имеются следующие классы — C1 и C2. Класс безопасности C1 подразумевает разделение данных и пользователей. Определенная группа пользователей имеет доступ только к определенным данным, для получения сведений необходима аутентификация — проверка подлинности пользователя путем запроса пароля. При классе безопасности C1 в системе имеются аппаратные и программные средства защиты. Системы с классом C2 дополнены мерами, гарантирующими ответственность пользователей: создается и поддерживается журнал регистрации доступа.

Уровень B включает технологии обеспечения безопасности, которые имеют классы уровня C, плюс несколько дополнительных. Класс B1 предполагает наличие политики безопасности, доверенной вычислительной базы для управления метками безопасности и принудительного управления доступом. При классе B1 специалисты осуществляют тщательный анализ и тестирование исходного кода и архитектуры. Класс безопасности B2 характерен для многих современных систем и подразумевает: Снабжение метками секретности всех ресурсов системы, регистрацию событий, которые связаны с организацией секретных каналов обмена памятью, структурирование доверенной вычислительной базы на хорошо определенные модули, формальную политику безопасности, высокую устойчивость систем к внешним атакам. Класс B3 подразумевает, в дополнение к классу B1, оповещение администратора о попытках нарушения политики безопасности, анализ появления секретных каналов, присутствие устройств для восстановления данных после сбоя в работе аппаратуры либо программного обеспечения.

Уровень A включает один, наивысший класс безопасности — A. К данному классу относятся системы, прошедшие тестирование и получившие подтверждение соответствия формальным спецификациям высшего уровня. Проблема защиты информации не новая, она возникла еще задолго до появления компьютеров. Стремительное совершенствование компьютерных технологий также отразилось на принципах построения охраны информации.

С самого начала своего развития системы информационной безопасности разрабатывались для военных ведомств. Разглашение такой информации могло привести к огромным жертвам, в том числе и человеческим. Поэтому конфиденциальности (то есть неразглашению информации) в первых системах безопасности уделялось особое внимание.

Компьютерная защита - это постоянная борьба с глупостью пользователей и интеллектом хакеров. Даже хакеры чаще всего используют именно некомпетентность и халатность обслуживающего персонала и именно последние можно считать главной угрозой безопасности.

КЛАССИФИКАЦИЯ СОВРЕМЕННЫХ БИОМЕТРИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Беляев П.С., Желтяков О.В., студенты
Научный руководитель: к.т.н., доцент О.Ю. Федосеева
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Все мы в своей деятельности постоянно сталкиваемся с проблемами получения, передачи, сохранности информации, в самых разных сферах. Недаром говорят: «Владею информацией — владею миром», это верно в наш век информационных технологий, как никогда ранее.

На общем фоне рынка наиболее динамично продолжают развиваться современные системы идентификации личности и защиты информации. Вопросы идентификации чрезвычайно актуальны. Как показывает анализ современного рынка технических средств обеспечения безопасности, в развитии индустрии безопасности сегодня обозначился новый этап. Особое внимание привлекают к себе биометрические средства защиты информации (БСЗИ), что объясняется их высокой надежностью идентификации и достигнутым в последнее время значительным снижением их стоимости. Биометрическая технология – наиболее заметное из последних достижений в области методов идентификации и контроля доступа к информации.

Особенности биометрических систем защиты данных

Биометрические системы обеспечивают контроль доступа, дают высокую надежность и широко используются во всем мире. Круг задач, которые с успехом решаются с помощью новых технологий — биометрии:

- вход в электронное рабочее место;
- получение, передача конфиденциальной информации коммерческого характера;
- ведение правительственных ресурсов;
- осуществление банковских и финансовых операций;
- торговля;
- защита данных;
- охрана правопорядка;
- здравоохранение;
- социальные услуги;

– частная жизнь (умный дом, смартфоны).

Виды биометрических систем (рисунок 1).

По степени достоверности и количеству ошибочных отказов можно различать виды биометрических систем:

– идентификационные;
– верификационные.

В первом, конкретное лицо представляет свои биометрические характеристики и получает подтверждение или отказ, что позволяет ему пользоваться доступом к определенным действиям или нет. Здесь не создается всеобщая база данных и нет опасности, что кто-то может знать и использовать чужие биометрические данные.

В другом, система изучает сведения неизвестного объекта и определяет пользователя по базе, дает ему круг полномочий. Так работают биометрические средства защиты информации. В связи с этим, возникает ряд этических вопросов.

Часто пользователи боятся использовать такое оборудование, чтобы не нанести вред себе. Идут дискуссии о том, что это первые шаги к полному контролю над обществом, ограничению гражданских свобод. Есть и обратные примеры. В Англии есть город Ньюхем, где такие системы работают повсеместно, одобрены населением и результаты весьма обнадеживающие.

По списку используемых параметров биометрические системы безопасности можно подразделить:

– динамические (поведение и психология) — походка, речь, ритм набора текста, почерк, голос;
– статические (биология человека) — отпечатки пальцев, форма кист и лица, линии ладони, сетчатка глаза и радужная оболочка, ДНК и др. При анализе могут использоваться один или несколько параметров, с целью уменьшения количества ошибок и необоснованных отказов.

В настоящее время отечественной промышленностью и рядом зарубежных фирм предлагается достаточно широкий набор различных средств контроля доступа к информации, и выбор оптимального их сочетания в каждом конкретном случае вырастает в самостоятельную проблему. На российском рынке в настоящее время представлены как отечественные, так и импортные БСЗИ, существуют и совместно разработанные средства. По конструктивным особенностям можно отметить системы, выполненные в виде моноблока, нескольких блоков и в виде приставок к компьютерам.

Сравнительный анализ показывает, что наиболее надежными системами контроля доступа к информации, в которых не используются карточки, ключи, жетоны, пароли и которые нельзя выкрасть или потерять, являются биометрические системы контроля доступа к информации. Будучи наиболее дорогостоящими, они обеспечивают и наиболее высокий уровень безопасности. Раньше они в основном использовались в государственных учреждениях и там, где предъявляются особые требования к безопасности. В настоящее время биометрические системы контроля доступа к информации завоевывают популярность в банках, фирмах, связанных с обеспечением безопасности в телекоммуникационных сетях, в информационных отделах фирм и т. д. Расширение применения систем этого типа можно объяснить как снижением их стоимости, так и повышением требований к уровню безопасности.

Основными направлениями практического внедрения рассмотренных средств биометрического контроля доступа к информации в настоящее время являются:

– идентификация личности, паспортизация;
– электронная торговля;
– страхование;
– защита систем связи;
– общий контроль доступа к информационным объектам (мобильным и стационарным);
– контроль доступа в компьютерные и сетевые системы;
– контроль доступа в различные информационные хранилища, банки данных и др.

Современные возможности биометрических технологий уже сегодня обеспечивают необходимые требования по надежности идентификации, простоте использования и низкой стоимости оборудования защиты информации, передаваемой по телекоммуникационным сетям.

Биометрическая идентификация позволяет эффективно решать целый ряд проблем:

– предотвратить проникновение злоумышленников в защищенные системы в результате подделки или кражи документов, карт, паролей; ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность; обеспечить допуск к ответственным объектам только сертифицированных специалистов; избежать накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);

– исключить неудобства, связанные с утерей или порчей ключей, карт, паролей; организовать учет доступа и посещаемости сотрудников.

Доступные по цене микропроцессорные системы, основанные на принципе биометрического контроля, появились в начале 90-х годов XX столетия. Сегодня можно привести достаточно много примеров успешной работы устройств, построенных на биометрическом принципе. В США уже используются банкоматы, которые распознают лица клиентов. Сотни и тысячи подобных устройств работают в различных организациях по всему миру.

В качестве уникального биологического кода человека используется целый ряд параметров. Основные из них приведены на рисунке 1.

Биометрические параметры человека можно разделить на физиологические (основанные на анатомической уникальности каждого человека) и поведенческие, основанные на специфике действий человека. Каждый из параметров имеет свои достоинства и недостатки с точки зрения его использования в качестве критерия идентификации.

Метод сканирования радужной оболочки глаза

Еще несколько десятилетий назад было доказано, что нет двух человек с одинаковой радужной оболочкой глаза, однако программное обеспечение, способное выполнять поиск и устанавливать соответствие образцов и отсканированного изображения, появилось только в конце XX века. Технология допуска, основанная на сканировании радужной оболочки глаза, уже несколько лет применяется в государственных организациях и учреждениях с высоким уровнем секретности.

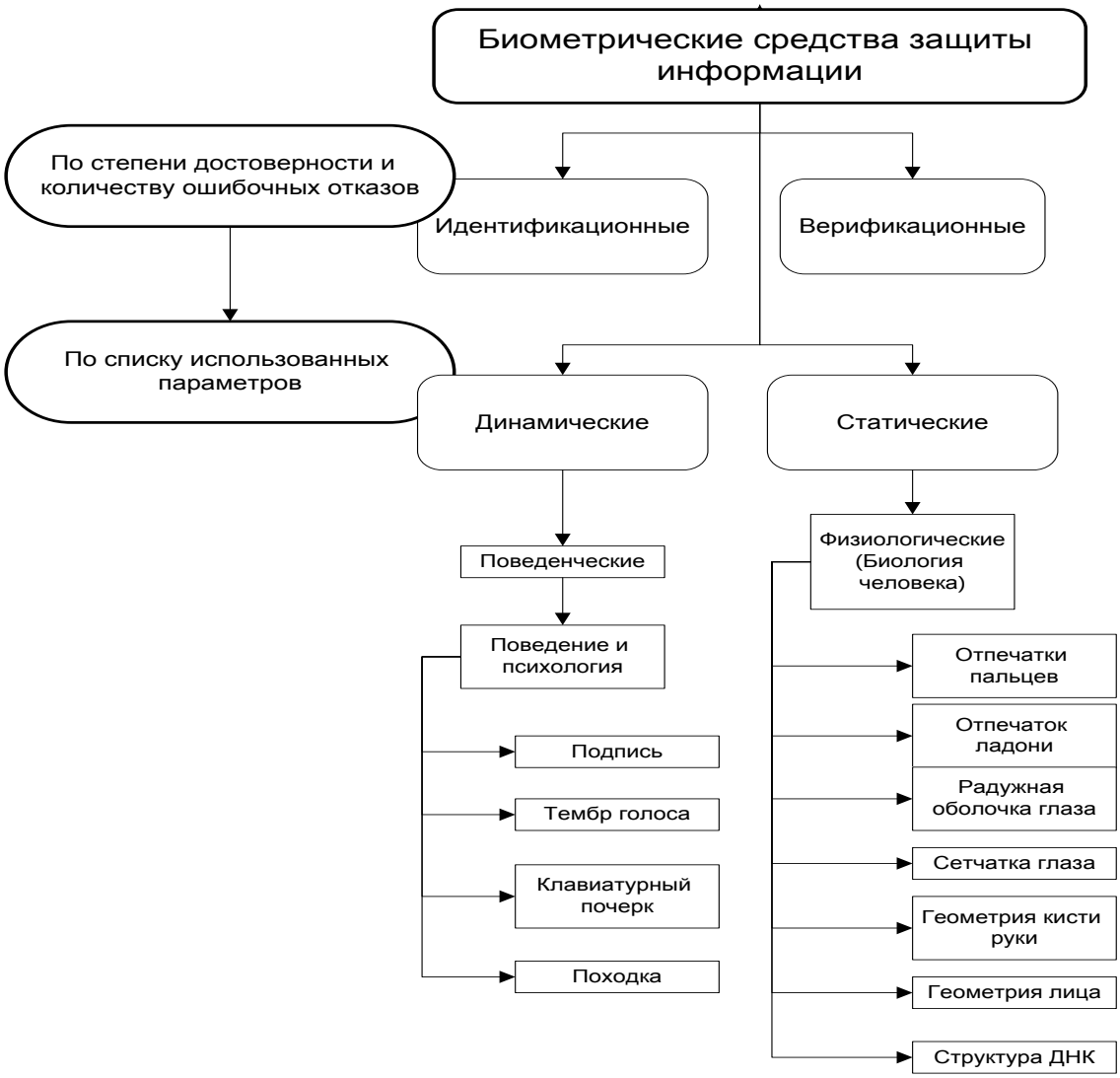


Рисунок 1 – Классификация современных биометрических средств защиты информации

Метод сканирования геометрии лица

Система допуска по распознаванию лица - наиболее древний и распространенный способ. Именно такая процедура осуществляется, когда мы, например, предъявляем паспорт на пропускном

пункте международного аэропорта. Пограничник сверяет фото на паспорте с лицом владельца паспорта и принимает решение - его это паспорт или нет. Примерно такую же процедуру выполняет компьютер, с той только разницей, что фото уже находится в его памяти. О качестве современных систем распознавания лица можно судить по высказыванию вице-президента компании Polaroid, который в качестве доступа к своему ноутбуку использует систему распознавания по лицу FaceIt, разработанную компанией Visionics. "Я все время забывал свой пароль, - говорит он, - но FaceIt мое лицо не забывает. Она узнает меня в очках и без очков, с бородой и без нее".

Распознавание по голосу

Метод узнавания по голосу, как и распознавание лица, был известен до появления биометрии. Поэтому достоинства и недостатки метода знакомы каждому. Как не всегда по ответу на вопрос "кто там?" можно понять, что за дверью находится сосед, и иногда приходится заглядывать в глазок, так и техническая система может ошибаться в силу изменений голоса человека. А голос, как известно, зависит от настроения, состояния здоровья, меняется с возрастом и даже может "ломаться". В связи с этим устройства идентификации по голосу пока не получили широкого распространения.

Распознавание по подписи

Вероятно, все, кто хоть когда-то получал деньги в банке, знакомы с этим методом идентификации личности. Банковские служащие сверяют подпись на глаз и достаточно часто при выдаче крупных сумм просят расписаться несколько раз. То есть вероятность ошибки в данной системе не так уж мала. Известны случаи, когда люди не могли получить деньги из-за изменения почерка и, соответственно, подписи. Компьютерная система, в отличие от банковского служащего, учитывает несколько параметров: саму форму начертания, динамику движения пера, степень нажима, что, как правило, позволяет установить достаточно высокую степень точности при распознавании личности.

Распознавание по отпечатку пальца

Данный метод имеет множество преимуществ - отпечаток пальца компактен, уникален, давно используется как средство дактилоскопического контроля (около 100 лет), поскольку не изменяется в течение всей жизни человека, и поэтому получил массовое распространение. Определенным недостатком, сдерживающим развитие метода, является свойственное многим предубеждение, что не следует оставлять информацию о своих отпечатках пальцев. Разработчики аппаратуры на это возражают, что информация об узоре отпечатка пальца в памяти аппаратуры контроля доступа не хранится - хранится лишь короткий идентификационный код, построенный на базе характерных особенностей вашего отпечатка. По данному коду нельзя воссоздать узор и сравнить его с отпечатками пальца, оставленными, например, на месте преступления.

Основным элементом устройства является сканер, считывающий папиллярный узор, который затем обрабатывается с помощью специального алгоритма, и полученный код сравнивается с шаблоном, хранящимся в памяти.

Подводя итог, можно сказать, что биометрические технологии являются последним достижением в области идентификации и позволяют уже сегодня реализовать наиболее надежные методы защиты информации. Таким образом, биометрические технологии являются одними из наиболее перспективных технологий защиты информации на ближайшие годы.

Библиографический список

1. Защита доступа к информации. Программная защита информации. [Электронный ресурс] - http://www.safensoft.ru/security.phtml?c=882.

2. Средства защиты информации. [Электронный ресурс] - http://cyclowiki.org/wiki/.

3. Биометрическая защита информации. [Электронный ресурс] - http://www.familytree.ru/ru/cipbooks/book002.htm.

СЕТЕВОЙ ПРОТОКОЛ SSH

Васильев Е.С., студент
Научный руководитель: к.п.н., доцент Е.Н. Горбачевская
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

С момента появления вычислительных сетей, в том числе сети Internet, возникла потребность в защите информации, передаваемой между пользователями.

Когда стали широко использоваться алгоритмы шифрования при передаче данных в сети, одной из первых задач стала организация безопасной оболочки. До этого существовала система rsh, которая позволяла определённым пользователям с определённых машин (между ними должны были быть доверительные отношения) работать на сервере с его оболочкой. Это, практически, то же самое, что и telnet доступ. Но с развитием сетей стали видны серьезные уязвимости rsh:

- данные, передаваемые через сеть, никак не шифруются, включая пароли
- данные, передаваемые через сеть, могут быть без проблем получены либо модифицированы третьей стороной
- злоумышленник может подменить ip клиента и, использовав полученный ранее хеш пароля, пройти аутентификацию на сервере со всеми вытекающими последствиями

Поэтому сейчас rsh или telnet применяется в чрезвычайно редких случаях, например, при переносе данных между двумя попарно соединёнными машинами (например, две машины, находящиеся в соседних комнатах). В основном стандартом де-факто стал протокол SSH.

В основном, SSH реализован в виде двух приложений — SSH-сервера и SSH-клиента. Поддержка SSH реализована во всех UNIX-подобных системах, и на большинстве из них в числе стандартных утилит присутствуют клиент и сервер SSH. Существует множество реализаций SSH-клиентов и для не-UNIX-подобных систем. Большую популярность протокол получил после широкого развития анализаторов трафика и способов нарушения работы локальных сетей, как альтернативное небезопасному протоколу Telnet решение для управления важными узлами. Как сказано выше, для работы по SSH нужен SSH-сервер и SSH-клиент. Сервер прослушивает соединения от клиентских машин и при установлении связи производит аутентификацию, после чего начинает обслуживание клиента. Клиент используется для входа на удалённую машину и выполнения команд. Для соединения сервер и клиент должны создать пары ключей — открытых и закрытых — и обменяться открытыми ключами. Обычно используется также и пароль. Более подробно аутентификация описана в пункте 3 данной работы. Наиболее популярные SSH-клиенты и оболочки для некоторых платформ:

- GNU/Linux, *BSD: kdessh, lsh-client, openssh-client, putty, ssh, Vinagre, Tectia SSH (SSH Communications Security) Client;
- MS Windows и Windows NT: PuTTY\KiTTY, SecureCRT, ShellGuard, Axessh, ZOC, SSHWindows, ProSSHD, XShell, Tectia SSH (SSH Communications Security) Client;
- MS Windows Mobile: PocketPuTTy, mToken, sshCE, PocketTTY, OpenSSH, PocketConsole, Tectia SSH (SSH Communications Security) Client;
- Mac OS: NiftyTelnet SSH;
- Symbian OS: PuTTY;
- iPhone: i-SSH, ssh (в комплекте с Terminal);
- Android: connectBot, Admin Hands, Server Auditor, JuiceSSH;
- Blackberry: BBSSH.

Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA, но допускается также аутентификация при помощи пароля (режим обратной совместимости с Telnet) и даже ip-адреса хоста (режим обратной совместимости с rlogin).

Аутентификация по паролю наиболее распространена. При каждом подключении вырабатывается общий секретный ключ для шифрования трафика.

При аутентификации по ключевой паре предварительно генерируется пара открытого и закрытого ключей для определённого пользователя. Оба файла хранятся как на машине с которой требуется произвести подключение, так и на удалённой машине. Эти файлы не передаются при аутентификации, система лишь проверяет, что владелец открытого ключа также владеет и закрытым. При данном подходе, как правило, настраивается автоматический вход от имени конкретного пользователя в ОС.

Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают.

Для создания общего секрета (сеансового ключа) используется алгоритм Диффи — Хеллмана (DH). Для шифрования передаваемых данных используется симметричное шифрование, алгоритмы AES, Blowfish или 3DES. Целостность передачи данных проверяется с помощью CRC32 в SSH1 или HMAC-SHA1/HMAC-MD5 в SSH2.

Для повышения безопасности использования SSH необходимо использовать:

- запрещение удалённого доступа с правами администратора;
- запрещение подключения с пустым паролем или отключение входа по паролю;
- нестандартный порт для SSH-сервера;

- длинные SSH2 RSA-ключей (2048 бит и более) (системы шифрования на основе RSA считаются надёжными, если длина ключа не менее 1024 бит);

- ограничение списка IP-адресов, с которых разрешён доступ (например, настройкой файервола);

- запрещение доступа с некоторых потенциально опасных адресов;

- отказ от использования распространённых или широко известных системных логинов для доступа по SSH;

- регулярный просмотр сообщений об ошибках аутентификации.

С момента создания протокола SSH, в нем было обнаружено несколько уязвимостей, которые, однако, оперативно устранялись, следовательно, данный протокол можно считать надежным, как и протокол передачи и копирования файлов на его основе – SFTP, который не был рассмотрен в данной статье. Так же не был рассмотрен пакет программ OpenSSH – аналог SSH с открытым исходным кодом. Поскольку сейчас SSH является коммерческим продуктом (что само по себе противоречит требованиям безопасности - всем должен быть известен исходный код системы защиты информации, чтобы убедиться в отсутствии всяких «лазеек»), следствием послужило создание OpenSSH.

Библиографический список

1. Таненбаум, Э., Уэзеролл, Д. «Компьютерные сети», изд Питер. 2012 г.

2. Олифер, В., Олифер, Н. «Компьютерные сети. Принципы, технологии, протоколы». изд. Питер. 2012 г.

3. Керниган, Б., Роб, П., «Unix. Программное окружение», изд. Символ-Плюс. 2003 г.

4. Лимончелли Т., Хоган, К. «Системное и сетевое администрирование. Практическое руководство». изд. Символ-Плюс. 2009 г.

ЗАКОНОДАТЕЛЬНОЕ ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ТЕРРОРИСТИЧЕСКИХ МАТЕРИАЛОВ В ИНТЕРНЕТЕ

Винокуров М.Ю., студент
Научный руководитель: к.п.н., доцент Е.Н. Горбачевская
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Радио, телевидение, интернет настолько глубоко проникли в наш мир, что невозможно представить человека, не имеющего доступа к данной информационной среде. Практически все социальные явления освещаются в СМИ и интернете. Значение интернета в современном мире колоссально. С помощью интернета можно достичь практически любой цели, будь то прослушивание музыки или организация «бунта». Как пример – собирание толпы на «Евромайдан», на Украине, агитация людей происходила преимущественно через социальные сети. Свобода общения в интернете нередко становиться эффективным средством манипуляции толпой.

Конечно, правительства многих стран активно борются с терроризмом в интернете, но у преступников есть множество способов обхода преград, как на уровне законодательства, так и на уровне защиты интернет-ресурсов.

Следующие действия могут быть оценены как киберпреступность: распространение компьютерных вирусов, взлом паролей, кража данных кредитных карт и реквизитов, распространение противоправной информации, такие как порнографические материалы, материалы вызывающие вражду между культурными организациями т.д. через интернет и вредоносное влияние на работу компьютерных систем.

Программы для противодействия существуют и создаются за рубежом, например в Израиле, США, Италии, ФРГ, Испании. Как показывает практика, опыт борьбы с киберпреступниками в ФРГ, Италии и Испании в отличие от США представляется более интересным и полезным.

В России существует ряд законов, прописанных в уголовном кодексе:

УК. Глава 28 «Преступления в сфере компьютерной информации» содержит три статьи:

– «Неправомерный доступ к компьютерной информации» (ст. 272);

– «Создание, использование и распространение вредоносных компьютерных программ» (ст. 273);

– «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274).

Для противодействия хакерским атакам создаются системы технической разведки, контроля и защиты (Управление «К» МВД Российской Федерации). Так же в России существуют отдельные общественные инициативы, проекты институтов гражданского общества, но, к сожалению, пока не достаточно эффективные.

Возвращаясь к теории, можно сказать, что эффективной концепции информационного противодействия терроризму еще нет. Сейчас любая экстремистская идея может стать хорошей основой к зарождению конфликта, или даже терроризма. Об этом говориться в материалах международной конференции высокого уровня по борьбе с насильственным экстремизмом, которая состоялась в феврале 2015 года в США. Данный саммит собрал представителей более чем 60 стран с целью объединения усилий в борьбе с насильственным экстремизмом.

Чтобы победить терроризм нужно объединить усилия заинтересованных государств и выработать следующие механизмы борьбы:

– создать критерии определения «вредности» информации;

– создать механизм защиты граждан от «вредной» информации, в первую очередь от молодежи;

– создать механизм, препятствующий распространению террористической идеологии.

Для разработки эффективной стратегии борьбы с террористическо-экстремистским угрозам необходимо знать не только текущую обстановку, но тенденции ее развития.

Множество осуществленных и предотвращенных в 2006 – 2008 годах террористических актов в государствах Северной Африки, Европы, Индии, Пакистане, Афганистане, Ираке говорит о нерушимости основ терроризма и их потенциала.

Подводя итоги, что необходимо сделать, чтобы начать реально бороться с киберпреступностью? Для начала необходимо точно определить максимально допустимый контент. Далее необходимо мониторить «весь интернет», в том числе и личную переписку, для этого, в некоторых случаях, необходимо международное соглашение. Ну и разумеется надо определить меру наказания. А какова ситуация сейчас? Сейчас есть реально действующая организация, Управление «К» МВД Российской Федерации, которая занимается поиском и поимкой хакеров. А вот что касается международного соглашения - здесь ситуация немного другая, все личные данные граждан российской федерации должны храниться только на серверах расположенных в России. Россия отказалась подписывать документ на конвенции совета Европы от 21 ноября 2001 года, основываясь на том, что Россия не увидела выгоды в таком соглашении, хотя многие эксперты критиковали такое решение.

Библиографический список

1. Попов, И.А. Правовое и организационное обеспечение раскрытия и расследования преступлений в сфере компьютерной информации: состояние и пути совершенствования // Библиотека криминал. 2013. N 5(10). С. 314-327.

2. Рассолов, И.М. Право и Интернет. Теоретические проблемы. М.: Норма. 210 с.

3. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. Дис. …канд. юрид. Наук. Владивосток, 2005. 235 с.

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ СВЯЗИ

Вяткин А.С., Юрцев Д.В., студенты
Научный руководитель: ст. преподаватель Е.В. Плюснина
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Развитие средств, методов и форм автоматизации информационных процессов, массовое применение вычислительной техники делают информацию уязвимой. Информация может быть незаконно изменена, похищена или уничтожена. Учитывая, что для построения надежной системы защиты данных требуются значительные материальные и финансовые затраты, необходимо не просто разрабатывать частные механизмы защиты информации, а использовать целый комплекс мер, т.е. использовать специальные средства, методы и мероприятия с целью предотвращения потери данных.

На рисунке 1 приведена классификация основных определений и понятий предметной области «Защита информации».

Рисунок 1 – Классификация определений и понятий предметной области «Защита информации»

Несмотря на предпринимаемые меры, функционирование компьютерных технологий выявило наличие слабых мест (угроз) в защите информации. Угрозы безопасности делятся на случайные (непреднамеренные) и умышленные (преднамеренные). Источником случайных угроз могут быть:

– отказы и сбои аппаратных средств;
– помехи в каналах и на линиях связи;
– форсмажорные ситуации (пожар, выход из строя электропитания и т.д.);
– ошибки и просчеты разработчиков и производителей технических средств;
– алгоритмические и программные ошибки;
– неумышленные действия пользователей, приводящие к отказу технологии или разрушению аппаратных, программных, информационных ресурсов (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ и т.д.);
– запуск программ, способных при некомпетентном использовании вызывать необратимые изменения (форматирование или реструктуризация носителей информации, удаление данных и т.д.);
– заражение компьютерными вирусами;
– неосторожные действия, приводящие к разглашению конфиденциальной информации или атрибутов разграничения доступа (паролей, ключей шифрования и т.д.);
– пересылка данных по ошибочному адресу абонента или устройства и т.д.

К методам обеспечения безопасности информации относятся: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение (рис. 2).

Приведем основные требования, предъявляемые пользователями к системам телекоммуникаций с позиций обеспечения защиты передаваемой информации. Системы телекоммуникаций должны обеспечить:

– конфиденциальность информации – обеспечение просмотра информации в приемлемом формате только для пользователей, имеющих право доступа к этой информации;
– целостность информации – обеспечение неизменности информации при ее передаче;
– аутентичность информации – обеспечение надежной идентификации источника сообщения, а также гарантия того, что источник не является поддельным.
– доступность информации – гарантия доступа санкционированных пользователей к информации.

Методы защиты информации в канале связи можно разделить на две группы:

– основанные на ограничении физического доступа к линии и аппаратуре связи;
– основанные на преобразовании сигналов в линии к форме, исключающей (затрудняющей)

для злоумышленника восприятие или искажение содержания передачи.

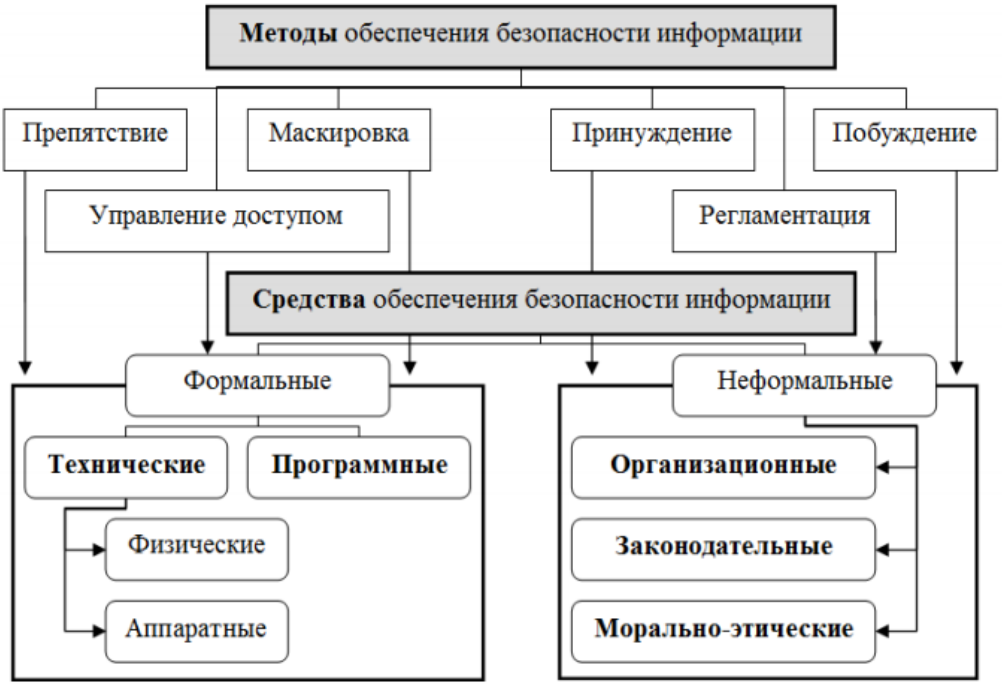


Рисунок 2 - Методы и средства защиты информации

Методы первой группы в основном находят применение в системах правительственной связи, где осуществляется контроль доступа к среде передачи данных.

Методы второй группы направлены на обратимое изменение формы представления передаваемой информации. Преобразование должно придавать информации вид, исключающий ее восприятие при использовании аппаратуры, стандартной для данного канала связи. При использовании же специальной аппаратуры восстановление исходного вида информации должно требовать затрат времени и средств, которые по оценке владельца защищаемой информации делают бессмысленным для злоумышленника вмешательство в информационный процесс.

При защите обмена данными решающее значение имеет форма представления сигнала в канале связи.

Следует учесть, что деление на "аналоговый" или "цифровой" сигнал условно. Для некоторых вариантов механизмов защиты информации требуется взаимная синхронизация и обмен служебными посылками между взаимодействующей аппаратурой защиты, т.е. присутствует цифровой режим, однако, поскольку этот режим не связан непосредственно с речевым обменом, требования к его скоростным характеристикам достаточно свободны.

С другой стороны, символьный (цифровой) обмен в протяженных каналах всегда осуществляется через модемное преобразование в виде аналогового сигнала.

Нормальная передача информации (рисунок 3 а)) в сетях с гарантируемым качеством обслуживания пользователей подразумевает выполнение трех этапов (рисунок 3 а)).

1. В плоскости менеджмента – формирование и корректировка баз данных (БД) о состоянии элементов сети. Конечным результатом функционирования данного этапа является формирование плана распределения информации на сети - расчет таблиц маршрутизации (ТМ) во всех узлах для каждой службы электросвязи.

2. В плоскости управления (стек протоколов сигнализации) - организацию маршрута между узлом – источником (УИ) и узлом – получателем (УП) в виде виртуального коммутируемого либо постоянного соединения (канала или тракта). Конечным результатом функционирования данного этапа является заполнение и обнуление таблиц коммутации (ТК).

3. В плоскости пользователя - непосредственная передача пользовательской информации.

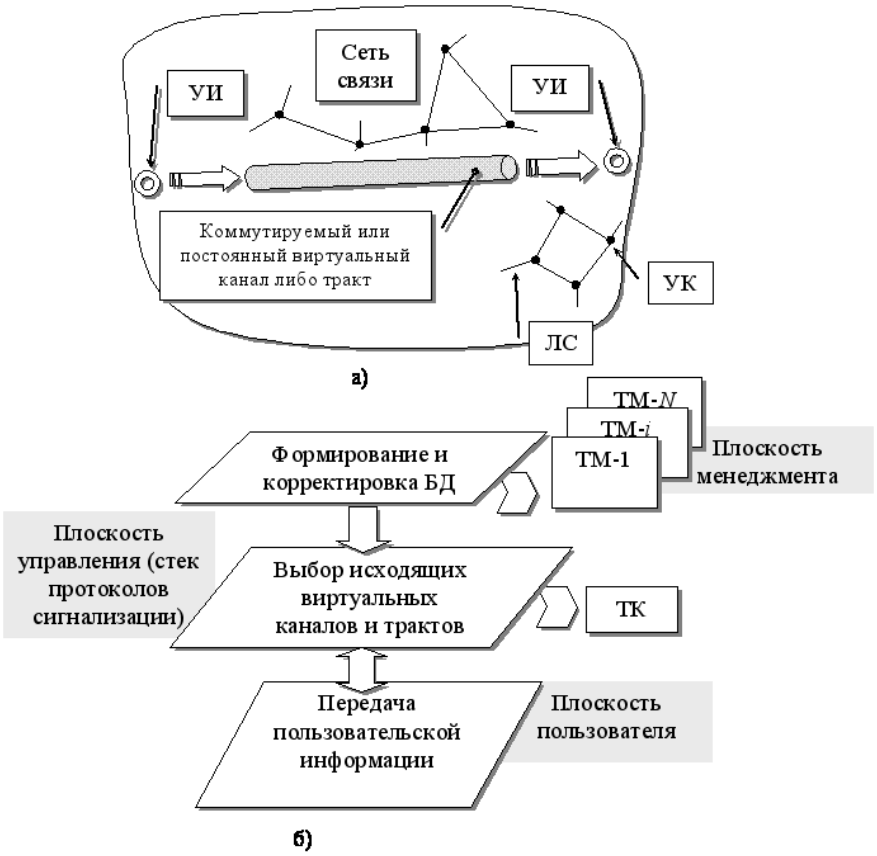


Рисунок 3 – Нормальная передача информации в сети

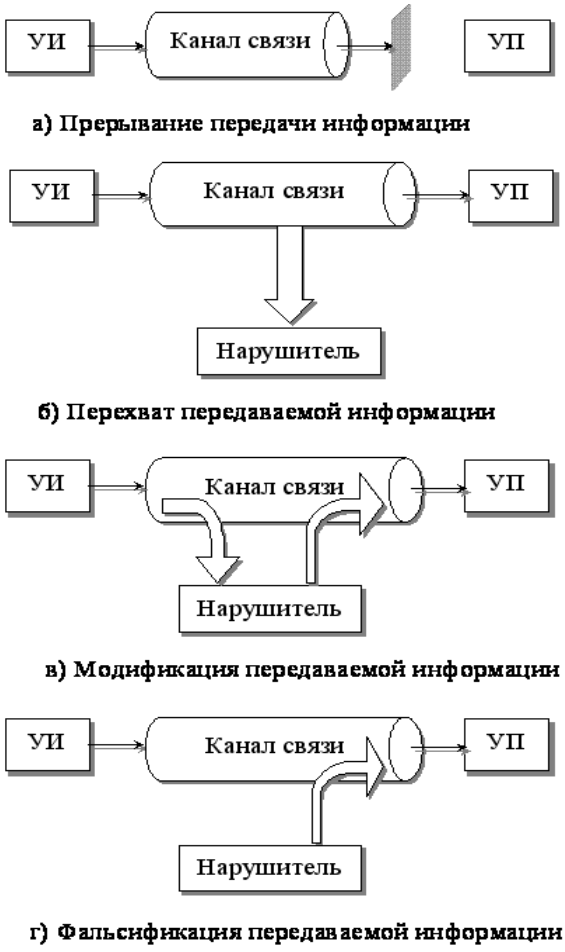


Рисунок 4 – Виды нарушений передачи информации

При этом передача всех видов информации в сети (служебной – для формирования БД и ТК; пользовательской) осуществляется по своим отдельно выделенным виртуальным соединениям (каналам и трактам).

Под *нарушением передачи информации* будем понимать одну из ситуаций, которые могут быть организованы нарушителем (рисунок 4).

1) Прерывание или разъединение (рисунок 4 а)). Информация уничтожается или становится недоступной либо непригодной для использования. В этом случае*нарушается доступность информации*. Примером таких нарушений может быть воздействие нарушителя на элементы сети (линии связи (ЛС), узлы коммутации (УК), устройства управления, БД и так далее) с целью их уничтожения или приведение в нерабочее состояние.

2) Перехват (рисунок 4 б)). К информации открывается несанкционированный доступ. *Нарушается конфиденциальность передаваемой информации*. Примером такого типа нарушений является несанкционированное подключение к каналу связи.

3) Модификация (рисунок 4в)). К информации открывается несанкционированный доступ с целью изменения информации. При этом *нарушается конфиденциальность передаваемой информации и ее целостность*. Целью такого типа нарушений является изменение информации, передаваемой по сети.

4) Фальсификация (рисунок 4 г)). Нарушитель выдает себя за источник информации. При этом *нарушается аутентичность информации*. Примером такого типа нарушений является отправка поддельных сообщений по сети.

Приведенные выше типы нарушений можно разделить на две группы:

– активные;
– пассивные.

К первой группе относятся:

– прерывание - нарушение доступности и конфиденциальности;
– модификация - нарушение целостности;
– фальсификация - нарушение аутентичности.

Данный тип нарушений имеет активный характер воздействия на элементы сети и передаваемую информацию. Основная цель этих нарушений состоит в изменении либо уничтожении потоков информации на сети.

К пассивным нарушениям относится перехват с целью получения передаваемой информации, ее анализа и использования в определенных целях.

Достаточно уверенно можно утверждать, что пассивные нарушения ставят своей конечной целью переход в группу активных нарушений.

Сервисные службы защиты информации (рисунок 5) являются ответственными за обеспечение основных требований пользователей, предъявляемых к телекоммуникационным системам (с точки зрения ее надежности). Причем данные службы должны функционировать во всех трех плоскостях: менеджмента, управления и пользовательской.

Рисунок 5 - Сервисные службы защиты информации

Совокупность сервисных служб защиты информации, обеспечивающих требования пользователей, образуют *профиль защиты*.

За установку и прекращение действия той или иной службы отвечают *агенты защиты* (Security Agent , SA). Согласование служб защиты между агентами происходит *через соединения защиты*. По этим соединениям производится обмен *информацией защиты*.

Рисунок 6 демонстрирует самый простой вариант организации соединения защиты - агенты защиты размещены в пределах конечных систем пользователей. В данном случае конечные системы и агенты защиты взаимодействуют с сетью через интерфейс «пользователь – сеть + защита» (UNI+Sec).

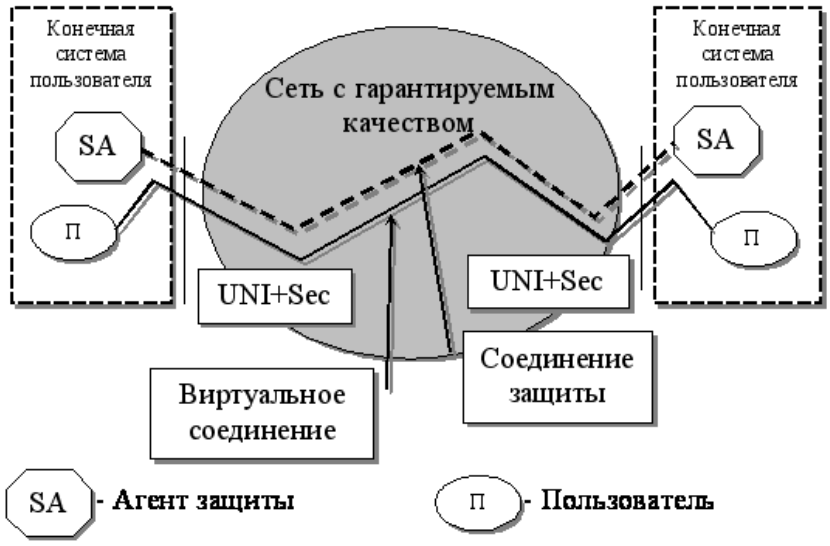


Рисунок 6 - Вариант организации соединения защиты - агенты защиты

Агенты защиты для виртуального соединения (канала либо тракта), который установлен между конечными системами пользователей, последовательно выполняют следующие действия:

– определяют вид сервисных служб защиты, которые должны быть применены к данному виртуальному соединению;
– согласовывают службы защиты между собой;
– применяют требуемые службы защиты к данному виртуальному соединению.

ИСПОЛЬЗОВАНИЕ ПРОГРАММНО-МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ КАК ОРУЖИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Гужвенко В.Ю., курсант
Научные руководители: д.п.н., доцент Е.И. Гужвенко
подполковник, старший преподаватель Н.Н. Тумаков
Рязанское высшее воздушно-десантное командное ордена Суворова дважды Краснознаменное училище имени генерала армии В.Ф. Маргелова
г. Рязань, Россия

Информация всегда играла важную роль в мире. А в наше время она стала неотъемлемой частью жизни. Современные технические средства ускорили процесс добывания, обработки и доставки информации, процесс ее обновления. Она стала оперативной, глобальной и разноплановой. Информация стала средством воздействия на мысли, поступки, поведение, принимаемые решения, на образ жизни и мировоззрение отдельного человека, коллективов, наций и народов. Выразительность показа, богатая цветовая гамма, высокое качество звучания, искусство монтажа и освещения событий резко повысили эффективность воздействия на человека, позволили формировать вектор такого воздействия в требуемом направлении. Таким образом, вмешиваясь в регулирование информационных потоков, в процесс их обработки и управления, можно влиять на события.

Информационным оружием называют способы и средства уничтожения, искажения или похищения информационных массивов, преодоления систем защиты информации, ограничения или запрета доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, инфраструктуры технологического обеспечения жизни общества и функционирования системы управления государством.

Определение «информационное оружие» включает технические и программные средства, обеспечивающие несанкционированный доступ к базам данных, нарушение штатного режима функционирования технических средств и программного обеспечения, а также вывод из строя ключевых элементов информационной инфраструктуры отдельного государства или группы государств.

Правомерность использования термина «информационное оружие» обусловлена тем, что в контексте использования информации как основы вида оружия она может характеризоваться следующими показателями: целенаправленность, избирательность, рассредоточенность, масштабность воздействия, досягаемость, скорость доставки, комплексность влияния на технические способы, системы и на личный состав, возможность регулирования «мощности» воздействия.

Самая большая опасность этого оружия - обезличенный характер его применения, что позволяет вести наступательные действия анонимно, даже без объявления войны. К тому же, запретить разработку и использование информационного оружия (как это сделано, например, в отношении химического или бактериологического) едва ли возможно, как и ограничить усилия многих стран по формированию единого глобального информационного пространства. Все это и объясняет повышенное внимание к информационному оружию и перспективам его дальнейшего развития. [2]

Термин «информационное оружие» получил широкое распространение после завершения военной операции Международных сил против Ирака в 1991 г. Военные специалисты посчитали, что решающий вклад в победу Международных сил над вооруженными силами Ирака внесло комплексное применение средств разведки, управления, связи, навигации и РЭБ. Совокупность этих средств и было определено как информационное оружие, названное потом информационным оружием театра военных действий.

Информационное программно-математическое оружие (ИПМО) – совокупность способов и средств, позволяющая целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, применяемая в ходе информационной борьбы для достижения поставленных целей. Это оружие включает:

– средства разрушения информационного обмена в телекоммуникационных сетях, его фальсификации, передачи по каналам государственного и военного управления нужной (для воздействующей стороны) информации;

– средства воздействия на каналы обмена информацией путем создания помех, искажения содержания информации, введения ложных сведений, дезинформации;

– программные закладки, заранее внедряемые в информационно-управляющие центры, компьютерные сети, программно-технические средства, которые самостоятельно (в установленное время) или по специальному сигналу приводятся в действие, уничтожая (искажая) информацию или дезорганизуя их работу. Специальные программы позволяют осуществить скрытый доступ к информационному массиву противника с целью получения разведывательной информации;

– компьютерные вирусы, способные разрушать, искажать программное обеспечение и информацию в компьютерных сетях, электронных телефонных станциях, системах управления и связи;

– нейтрализаторы тестовых программ, обеспечивающие невозможность выявления недостатков программных средств или наличие в них вирусов с помощью специальных тестовых программ;

– способы и средства, позволяющие внедрять «логические бомбы» и вирусы в информационные сети противника.

Программно-математическое оружие делиться на два типа: средства воздействия на программный продукт и средства воздействия на канал передачи информации.

Особенностями данного типа оружия являются следующие факторы: универсальность; скрытность; экономическая эффективность; масштабность применения; сложность международного контроля; эффект «Цепной реакции»; психологическое воздействие.

В современных войнах объектами информационного влияния станут сознание и психика человека, системы управления и другие информационно-технические системы, средства боевого поражения.

В развитии систем вооружений сейчас прослеживается устойчивая тенденция увеличения в них удельного веса информационного оружия. Подобная «информационная эволюция» происходит в несколько этапов.

1-й этап связан с применением информоружия для противодействия средствам поражения. Здесь следует выделить средства радиоэлектронного противодействия (РЭП), которые не являются оружием, разрушающим объекты, но их применение предшествует в современной войне началу боевых операций, «расчищает» дорогу для беспрепятственного применения боевых систем высокоточного оружия.

РЭП призвано блокировать или усложнять функционирование электронных средств неприятеля способом излучения, отражения электромагнитных, акустических и инфракрасных сигналов. РЭП осуществляется автоматическими наземными, корабельными и авиационными системами постановки помех. За несколько суток до начала операции «Буря в пустыне» США впервые в широких масштабах провели радиоэлектронное подавление активных средств ПВО, органов управления и иных важных объектов на территории Ирака. Как отмечали западные эксперты, это был «шторм в эфире» - американцы нанесли такой мощный радиоэлектронный удар по Ираку, что заглушили даже некоторые радионаправления на территории южных военных округов Советского Союза [1].

Особенность 2-го этапа эволюции в том, что основным объектом информвлияния становятся системы управления и связи, информационные и компьютерные сети. Для вывода из строя таких систем и объектов разработано специальное информационное оружие, к которому относятся средства программно-математического влияния, такие, как компьютерные вирусы, логические бомбы, «троянские кони», нейтрализаторы тестовых программ, и электромагнитное оружие.

К средствам программно-математического влияния относятся также средства подавления информобмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления, а также различного рода ошибки, сознательно внесенные программистами или лазутчиками в программное обеспечение [4].

Разработка электромагнитного оружия началась в 80-х годах в рамках реализации программы «Звездные войны», завершившейся созданием пушки, позволяющей осуществлять направленный выброс высокоэнергетического пучка в радиочастотном диапазоне. Одно из его основных преимуществ - относительная дешевизна.

Применение средств программно-математического влияния способно парализовать функционирование государственной власти в стране и подавить всю систему управления вооруженными силами [3]. Поэтому современная война начинается именно с массированного применения информоружия в таких формах, как радиоэлектронная борьба, радиоразведка, дезорганизация систем управления войсками и оружием, специальное программно-математическое влияние, направленное против существующих информсистем. Комплекс таких действий призван парализовать противника, что позволит свести к минимуму потери при проведении наземных операций.

Но самому большому информвоздействию как сегодня, так и в будущих войнах подвергается человек – ключевой компонент любых вооруженных сил. Концентрация усилий вокруг наращивания информвлияния на человека и является характерным признаком 3-го этапа развития систем информоружия. К таким системам следует отнести, прежде всего, психотропное оружие, средства зомбирования человека и средства психологической войны. Эти системы влияют на сознание и психику людей, что дает возможность руководить их поведением.

Библиографический список

1. Костин, Н.А. Общая математическая модель защиты информации. – М.: Инфо. 2011. – 211 с.

2. Перепелица, Г. Информационные войны. – М.: Спутник +. 2002. – 48 с.

3. Прокофьев В.Ф. К проблеме формирования основных понятий в области информационной безопасности [Электронный ресурс] - http://flot.com/ publications/books/shelf/safety/18.htm.

4. Контроль Разума [Электронный ресурс] - http://ru.wikibooks.org/wiki/.

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Евтеев А.В., студент, Плюснина Е.В.**, аспирант*
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия
*** Поволжский государственный университет телекоммуникаций и информатики*
г. Самара, Россия

Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации», информация - сведения (сообщения, данные) независимо от формы их представления.

Основой для раскрытия сущности и определения понятия защиты информации должно быть определение понятия защиты в целом, безотносительно к предмету защиты.

Термин «защита», интерпретируется двояко: как процесс охраны, сбережения, спасения от враждебного, опасного и как совокупность методов, средств и мер, принимаемых для предотвраще-

ния, предупреждения чего-либо. Что же касается термина «защита информации», то согласно Федеральному Закону «Об информации, информационных технологиях и о защите информации», защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

Безопасность информации - состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии.

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом.

Основные принципы организационной защиты информации:

- принцип комплексного подхода — эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

- принцип персональной ответственности — наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна быть:

- централизованной — обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;

- плановой — объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;

- конкретной и целенаправленной — рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;

- активной — обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

- надежной и универсальной — охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.

Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации — устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

Криптографические средства защиты информации — средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).

Программные средства защиты информации — системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Рисунок 1 – Методы и средства защиты информации

Эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия соответствующих сил и средств. Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют методы защиты информации, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.

Методы защиты информации — применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.

Общие методы защиты информации подразделяются на правовые, организационные, технические и экономические.

Знание принципов построения систем защиты и возможностей, предоставляемых различными компонентами вычислительной системы (операционной системой, программами обслуживания, СУБД, специализированными пакетами защиты и отдельными устройствами) позволяет оценить уязвимость ИС и грамотно организовать в ней защиту конфиденциальной информации.

Для организации комплексной защиты информации в ВС в общем случае может быть предусмотрено 4 защитных уровня.

1. Внешний уровень, охватывающий всю территорию расположения ВС.
2. Уровень отдельных сооружений или помещений расположения устройств ВС и линий связи с ними.
3. Уровень компонентов ВС и внешних носителей информации.
4. Уровень технологических процессов хранения, обработки и передачи информации.

Первые три уровня обеспечивают в основном физическое препятствие доступу путем ограждения, системы сигнализации, организации пропускного режима, экранирования проводов и т. д. Последний уровень предусматривает логическую защиту информации в том случае, когда физический доступ к ней имеется.

Существующие методы защиты можно разделить на четыре основных класса:

- физические;
- аппаратные;
- программные;
- организационные.

С помощью программно-аппаратных средств можно в определенной мере решать как основные

задачи защиты ИПО в ВС (от хищения, от потери, от сбоев и отказов оборудования), так и защиту от ошибок в программах.

Решение этих задач в системах защиты обеспечивается следующими способами:

1. защитой от несанкционированного доступа (НСД) к ресурсам со стороны пользователей и программ;
2. защитой от несанкционированного использования (НСИ) ресурсов при наличии доступа;
3. защитой от некорректного использования ресурсов;
4. внесением структурной, функциональной и информационной избыточности;
5. высоким качеством разработки программно-аппаратных средств.

В целом аппаратные либо технические СЗИ это различные устройства, которые аппаратными средствами решают задачи защиты информации. К ним можно отнести как и классические организационные средства, такие как различные меры противодействия проникновению на объекты, так и специализированные средства противодействия конкретным способам получения доступа к информации в процессе хранения либо передачи.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

– специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

– устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

– схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных;

– устройства для шифрования информации (криптографические методы).

Для защиты периметра информационной системы создаются:

– системы охранной и пожарной сигнализации;

– системы цифрового видеонаблюдения;

– системы контроля и управления доступом.

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

– использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;

– установкой на линиях связи высокочастотных фильтров;

– построение экранированных помещений («капсул»);

– использование экранированного оборудования;

– установка активных систем зашумления;

– создание контролируемых зон.

Для обеспечения сохранности данных разработаны специализированные аппаратные решения, способные обеспечивать как быстры доступ к данным, так и их надёжное компактное хранение. Базово их можно классифицировать на следующие виды:

Специализированная сеть хранения SAN (Storage Area Network) обеспечивает данным гарантированную полосу пропускания, исключает возникновение единой точки отказа системы, допускает практически неограниченное масштабирование как со стороны серверов, так и со стороны информационных ресурсов. Для реализации сетей хранения наряду с популярной технологией Fiber Channel в последнее время все чаще используются устройства iSCSI.

Дисковые хранилища отличаются высочайшей скоростью доступа к данным за счет распределения запросов чтения/записи между несколькими дисковыми накопителями. Применение избыточных компонентов и алгоритмов в RAID массивах предотвращает остановку системы из-за выхода из строя любого элемента – так повышается доступность. Доступность, один из показателей качества информации, определяет долю времени, в течение которого информация готова к использованию, и выражается в процентном виде: например, 99,999% («пять девяток») означает, что в течение года допускается простой информационной системы по любой причине не более 5 минут.

Ленточные накопители (стримеры, автозагрузчики и библиотеки) по-прежнему считаются самым экономичным и популярным решением создания резервных копий. Они изначально созданы для хранения данных, предоставляют практически неограниченную емкость за счет добавления ленточных картриджей, обеспечивают высокую надежность, имеют низкую стоимость хранения, позво-

ляют организовать ротацию любой сложности и глубины, архивацию данных, эвакуацию носителей в защищенное место за пределами основного офиса. С момента своего появления магнитные ленты прошли пять поколений развития, на практике доказали свое преимущество и по праву являются основополагающим элементом практики backup (резервного копирования).

Помимо рассмотренных технологий следует также упомянуть обеспечение физической защиты данных (разграничение и контроль доступа в помещения, видеонаблюдение, охранная и пожарная сигнализация), организация бесперебойного электроснабжения оборудования.

Библиографический список

1. Аверченков, В.И. Разработка системы технической защиты информации: учебное пособие [Электронн. ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стереотип. – М.: ФЛИНТА, 2011. – 187 с.

2. Акулов, О.А. Информатика [Текст]: учебник. Базовый курс / О.А. Акулов, Н.В. Медведев. – М.: Омега-Л, 2009. – 557 с.

3. Амелин, Р.В. Информационная безопасность [Электрон. ресурс] / Р.В. Амелин. – Электрон. дан. – М., 2008. – Режим доступа: http://nto.immpu./sites/default/files/3/__77037.pdf, свободный. - Загл. с экрана. – Яз. рус.

4. Варфоломеев, А.А. Основы информационной безопасности [Текст]: учебное пособие. – М.: РУДН, 2008. – 412 с.

5. Галатенко, В.А. Основы информационной безопасности [Текст] / В.А. Галатенко. – М.: ИНТУИТ.ру, 2008. - 208 с. – (Интернет-университет информационных технологий).

6. Гатчин, Ю.А. Управление доступом к информационным ресурсам [Текст] / А.Г. Коробейников, А. Г. Краснов. - СПб.: СПбГУ ИТМО, 2010. - 45 с.

7. Гатчин, Ю.А. Теория информационной безопасности и методология защиты информации [Текст] / В.В. Сухостат. - СПб.: СПбГУ ИТМО, 2010. - 98 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЁ ОБЕСПЕЧЕНИЕ

Завьялов Д.Л., студент
Научный руководитель: к.т.н., доцент О.Ю. Федосеева
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

При разработке компьютерных систем вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на обеспечение компьютерной безопасности, основными среди них являются технические, организационные и правовые.

Обеспечение безопасности информации — дорогое дело, и не только из-за затрат на закупку или установку средств защиты, но также из-за того, что трудно квалифицированно определить границы разумной безопасности и обеспечить соответствующее поддержание системы в работоспособном состоянии.

Роль и место информации и информационных технологий в современной жизни

В настоящее время обладание информацией позволяет контролировать решение любых проблем мирового сообщества. Она стала фактором, способным привести к крупномасштабным авариям, военным конфликтам и поражению в них, дезорганизовать государственное управление, финансовую систему, работу научных центров. В то же время эффективное использование информации способствует развитию всех сфер деятельности государства в целом и отдельно взятого предприятия в частности и, в конечном счете, приводит к значительным успехам в экономике, бизнесе, финансах.

Обладание ценной информацией, предоставляя существенные преимущества, при этом возлагает на субъекты, имеющие на нее права, высокую степень ответственности за ее сохранность и защиту от возможного внешнего воздействия различного рода факторов и событий, носящих как преднамеренный, так и случайный характер.

Что защищать?

Инвентаризация информационных систем — в данном случае это составление списка объектов, которые будут подлежать защите и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы. При этом необходимо не просто составить список, а указать ряд особенностей той или иной системы. То есть кратко описать ее с точки зрения информационной безопасности. Чем подробнее сделать это на начальном этапе, тем легче будет дальше производить уточнения и строить окончательную модель защиты.

Данная работа обычно инициируется службой информационной безопасности, но выполняется обычно с привлечением специалистов других служб. Это происходит потому, что специалисты по безопасности, скорее всего не обладают полным видением модели и способов функционирования конкретного объекта или информационной системы, таким, каким обладает администратор системы или ее активные пользователи.

Способы проведения такой инвентаризации могут быть различными. В зависимости от конкретной организации, описание может быть дополнено другими разделами. Например, можно включать функциональное назначение отдельных объектов системы.

Кроме того, необходимо определиться с тем, что считать отдельным объектом системы, подлежащим защите. Отдельный компьютер? Отдельный логический модуль?

Если взять в качестве примера систему с трехзвенной архитектурой (клиент—сервер приложений—сервер данных), то в зависимости от особенностей, классификация может быть различной. Можно посчитать всю систему единым объектом, а можно каждое звено рассматривать отдельно (получив три объекта).

Информационная безопасность и ее обеспечение

Информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, которые в первую очередь обусловлены наличием информационной инфраструктуры и информации. Иначе говоря, информационная безопасность — состояние защищенности объекта безопасности от внешних и внутренних угроз.

В случае, когда объект информационной безопасности — коммерческое предприятие, содержание понятия «информационная безопасность» заключается в защищенности интересов собственника информации, удовлетворяемых путем получения, сохранения, обработки и применения либо сокрытия информации.

Защита информационных ресурсов предприятия включает деятельность руководства, должностных лиц и структурных подразделений предприятия по принятию правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;
– соблюдение конфиденциальности информации ограниченного доступа;
– реализацию права на доступ к информации.

Таким образом, обеспечение информационной безопасности есть совокупность деятельности по недопущению вреда свойствам объекта безопасности. Особую роль в системе средств обеспечения информационной безопасности играют организационные средства.

Анализ угроз объекту информационной безопасности

Главными целями деятельности по обеспечению информационной безопасности являются ликвидация угроз объектам информационной безопасности и минимизация возможного ущерба, который может быть нанесен вследствие реализации данных угроз.

К наиболее важным свойствам угрозы относятся избирательность, предсказуемость и вредоносность. Избирательность характеризует нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам объекта безопасности. Предсказуемость характеризует наличие признаков возникновения угрозы, позволяющих заранее прогнозировать возможность появления угрозы и определять конкретные объекты безопасности, на которые она будет направлена. Вредоносность характеризует возможность нанесения вреда различной тяжести объекту безопасности. Вред, как правило, может быть оценен стоимостью затрат на ликвидацию последствий проявления угрозы либо на предотвращение ее появления.

При рассмотрении угроз информационной безопасности объекта особое внимание необходимо уделить классификации подлежащих защите объектов информационной безопасности предприятия. Одно из ключевых понятий в оценке эффективности проявления угроз объекту информационной безопасности — ущерб, наносимый этому объекту (предприятию) в результате воздействия угроз.

По своей сути любой ущерб, его определение и оценка имеют ярко выраженную экономическую основу. Не является исключением и ущерб, наносимый информационной безопасности объекта (предприятия).

С позиции экономического подхода общий ущерб информационной безопасности предприятия складывается из двух составных частей: прямого и косвенного ущерба.

Механизмы информационной безопасности

Объективные факторы или цели информационной безопасности обеспечиваются применением следующих механизмов или принципов:

- политика — набор формальных (официально утвержденных либо традиционно сложившихся) правил, которые регламентируют функционирование механизма информационной безопасности;
- идентификация — определение (распознавание) каждого участника процесса информационного взаимодействия перед тем как к нему будут применены какие бы то ни было понятия информационной безопасности;
- аутентификация — обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно, т.е. действительно является тем, чей идентификатор он предъявил;
- контроль доступа — создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа;
- авторизация — формирование профиля прав для конкретного участника процесса информационного обмена (аутентифицированного или анонимного) из набора правил контроля доступа;
- аудит и мониторинг — регулярное отслеживание событий, происходящих в процессе обмена информацией, с регистрацией и анализом предопределенных значимых или подозрительных событий. Понятия "аудит" и "мониторинг" при этом несколько различаются, так как первое предполагает анализ событий постфактум, а второе приближено к режиму реального времени;
- реагирование на инциденты — совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности;
- управление конфигурацией — создание и поддержание функционирования среды информационного обмена в работоспособном состоянии и в соответствии с требованиями информационной безопасности;
- управление пользователями — обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности. В данном случае под пользователями понимаются все, кто использует данную информационную среду, в том числе и администраторы;
- управление рисками — обеспечение соответствия возможных потерь от нарушения информационной безопасности мощности защитных средств (то есть затратам на их построение);
- обеспечение устойчивости — поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствии требованиям информационной безопасности в условиях деструктивных внешних или внутренних воздействий.

Таким образом, перечислено то, за счет чего достигаются определенные цели информационной безопасности.

Аутентификация сама по себе не может быть целью информационной безопасности. Она является лишь методом определения участника информационного обмена, чтобы далее определить, какая, например, политика в отношении конфиденциальности или доступности должна быть применена к данному участнику.

Инструментарий информационной безопасности

Привести полный список средств и инструментов обеспечения информационной безопасности невозможно. Он, в значительной степени, зависит от конкретной ситуации, в свете которой рассматривается тот или иной аспект информационной безопасности.

Рассмотрим процесс: персонал занимается аудитом, который обеспечивает учет. Значит, персонал — это средство, аудит — механизм, а учет — цель. Пароли, обеспечивающие аутентификацию, сохраняются в шифрованном виде, аутентификация предшествует, например, разрешению на модификацию. Значит, криптография — средство защиты паролей, пароли используются для механизма аутентификации, аутентификация предшествует обеспечению целостности.

Перечень основных средств (инструментов) информационной безопасности будет следующий:

– персонал — люди, которые будут обеспечивать претворение в жизнь информационной безопасности во всех аспектах, то есть разрабатывать, внедрять, поддерживать, контролировать и исполнять;

– нормативное обеспечение — документы, которые создают правовое пространство для функционирования информационной безопасности;

– модели безопасности — схемы обеспечения информационной безопасности, заложенные в данную конкретную информационную систему или среду;

– криптография — методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей — специальных информационных объектов, реализующих эти санкции;

– антивирусное обеспечение — средство для обнаружения и уничтожения зловредного кода (вирусов, троянских программ и т. п.);

– межсетевые экраны — устройства контроля доступа из одной информационной сети в другую;

– сканеры безопасности — устройства проверки качества функционирования модели безопасности для данной конкретной информационной системы;

– системы обнаружения атак — устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности;

– резервное копирование — сохранение избыточных копий информационных ресурсов на случай их возможной утраты или повреждения;

– дублирование (резервирование) — создание альтернативных устройств, необходимых для функционирования информационной среды, предназначенных для случаев выхода из строя основных устройств;

– аварийный план — набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности;

– обучение пользователей — подготовка активных участников информационной среды для работы в условиях соответствия требованиям информационной безопасности.

Приведенный список показывает типовой набор, характерный для предприятия, которое развивает у себя службу информационной безопасности.

Основные направления информационной безопасности

Информационную безопасность можно разделить на два направления — физическая и компьютерная безопасность. Оба направления можно охарактеризовать следующим образом:

Физическая безопасность — обеспечение сохранности самого оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию. Дополнительно сюда может быть включено понятие защиты самих пользователей информационной среды от физического воздействия злоумышленников, а также защиты информации невиртуального характера (твердых копий — распечаток, служебных телефонных справочников, домашних адресов сотрудников, испорченных внешних носителей и т. п.).

Компьютерная безопасность (сетевая безопасность, телекоммуникационная безопасность, безопасность данных) — обеспечение защиты информации в ее виртуальном виде. Возможно выделять этапы нахождения информации в среде, и по этим принципам разделять, например, компьютерную (на месте создания, сохранения или обработки информации) и сетевую (при пересылке) безопасность, но это, в принципе, нарушает комплексную картину безопасности. Единственное, с чем логично было бы согласиться, — это термин безопасность данных, или скорее, безопасность данных в рамках данного приложения. Дело в том, что в конкретном программном комплексе модель безопасности может быть реализована таким образом, что это потребует отдельного специалиста (или даже службы) по ее поддержанию. В этом случае возможно разделить понятия безопасность данных (конкретного приложения) и безопасность сети (всей остальной информационной среды).

Задачи службы информационной безопасности

Несмотря на, казалось бы, прямую очевидность задач службы информационной безопасности ("служба безопасности должна обеспечивать безопасность — что же еще?"), возникает множество вопросов, не бросающихся в глаза на первый взгляд. Разобьем эти вопросы или проблемы на следующие группы:

– размещение службы информационной безопасности;
– взаимодействие ее с другими службами;
– иерархия подчинения.

Иначе говоря, следует определить, где в штатной структуре предприятия должна размещаться служба информационной безопасности, как она будет взаимодействовать с другими подразделениями (особенно с подразделением информационных технологий), сколько начальников должно стоять между руководителем службы безопасности и директором предприятия.

Существует ряд рекомендаций по вопросам размещения, взаимодействия и подчинения службы безопасности, как продвинутые, в основном западные, ориентированные на электронный мир, так и старые, еще советские, пришедшие от первых отделов. Эти процедуры очень зависят от множества факторов конкретного предприятия, быть может, даже таких, как сложившиеся неформальные взаимоотношения между сотрудниками. Если во главу угла на предприятии ставится эффективность работы службы информационной безопасности, то такие аспекты невозможно не учитывать.

Чтобы не очерчивать жестких рамок для всего этого, можно просто рассмотреть проблемы и ответить для себя на возникающие вопросы. Из полученных ответов станет ясно, как и где должна располагаться служба информационной безопасности на организационном дереве предприятия.

Чем должна заниматься служба безопасности?

– Администрировать имеющиеся средства безопасности (межсетевые экраны, антивирусные пакеты, системы обнаружения атак и пр.)?
– Разрабатывать модели и схемы защиты информации, принимать решения о приобретении новых средств безопасности?
– Контролировать работу пользователей информационного пространства предприятия? Каких групп — только конечных пользователей или также и администраторов систем?
– Куда направлен основной фокус внимания службы — на внутренних пользователей (по статистике больше всего нарушений информационной безопасности — как умышленно, так и неумышленно — проистекает изнутри предприятия) или на защиту от доступа из внешнего информационного пространства?

Без сомнения, вопросы информационной безопасности должны учитываться в каждом из перечисленных пунктов. Однако прикладное применение может быть различным и зависеть от множества причин, которые обычно не предусмотрены западными рекомендациями, например, таких как нехватка квалифицированного персонала.

Примером различных решений могут быть две следующие ситуации: служба информационной безопасности только производит анализ ситуации, разработку модели и принимает решение о необходимости приобретения средства защиты, а его администрирование производится в рамках обычной работы подразделения информационных технологий. Противоположный вариант — приобретение средств защиты производится в рамках общей стратегии развития информационных технологий предприятия, а конкретные работы по установке и поддержке средства защиты производит служба информационной безопасности.

Как происходит взаимодействие со службой информационных технологий, а конкретно с администраторами сетей и систем?

– Специалисты информационной безопасности имеют полный контроль над информационной системой, равный правам администратора системы.
– Специалисты по безопасности принимают частичное участие в администрировании системы, например в настройке прав пользователей.
– Специалисты по безопасности имеют доступ в информационной системе ко всем объектам, но имеют право только читать сведения о них.
– Специалисты информационной безопасности не имеют доступа в систему, используют для контроля работы администраторов регистрационные журналы, конфигурационные отчеты и т. п.

Все эти варианты указаны преднамеренно, так как вопрос взаимоотношений службы безопасности и, скажем, администратора локальной сети может быть очень напряженным, особенно если служба только создается, а администратор уже несколько лет выполнял свои функции. Как быть, если администратор действительно честно работает долгое время, а специалисты по безопасности только пришли в организацию, но требуют значительных прав в системе для себя и ограничения прав администратора? Что делать, если администратор в этом случае решил покинуть организацию? А что если квалификация специалистов по безопасности по конкретной информационной системе значительно ниже, чем у администратора, и они могут, при наличии определенных прав, внести помехи в работу

системы? Что если система устроена таким образом, что для того, чтобы контролировать администратора, необходим полный контроль над всей системой? Вопросов больше, чем ответов, решение необходимо принимать с учетом всех этих проблем.

Возможно, болезненный процесс передачи или разделения прав придется растянуть на продолжительный период, пока специалисты службы безопасности не приобретут соответствующий опыт, а администраторы постепенно не привыкнут к частичному, а затем и полному контролю.

Сколько ступеней принятия решения по вопросам информационной безопасности должно существовать?

Если руководитель службы информационной безопасности непосредственно подчинен директору предприятия и вносит проекты решений напрямую, то это дает возможность злоупотребления своим положением (так как топ-менеджер скорее всего не очень компетентен в информационных технологиях, но на слово "безопасность" реагирует немедленным визированием всех документов).

Если процесс согласования решения чересчур распределен по руководителям и растянут во времени, есть риск, что произойдет запаздывание в принятии жизненно важного решения (впрочем, как и для любой другой службы). Кроме того, если представители точек согласования не компетентны в вопросе безопасности, то много времени непродуктивно будет потрачено на выяснение проблем и согласование мнений.

Согласован ли процесс принятия решения по информационной безопасности с общей стратегией развития информационных технологий? Не будут ли в информационном пространстве предприятия установлены средства защиты, которые внесут помехи в работу других информационных систем?

В данном случае существуют конкретные рекомендации, которые советуют подчинять службу информационной безопасности не напрямую директору, а некоему комитету по безопасности, в котором будут присутствовать, с одной стороны, специалисты, способные оценить качество предлагаемого решения, с другой — руководители, способные утвердить принятое решение к обязательному исполнению.

Сфера охвата информационных систем

Для полного контроля ситуации в информационном пространстве служба информационной безопасности должна иметь необходимые знания обо всех информационных системах, объектах и субъектах. Однако как быть в следующих ситуациях?:

- Данная конкретная информационная система для своего функционирования уже предусматривает разделение административных функций между двумя персонами, контролирующими друг друга.
- Функции данной информационной системы, с одной стороны, достаточно специфичны и требуют серьезной подготовки для ее администрирования и/или контроля, а, с другой стороны, слишком незначительны в рамках предприятия для того, чтобы содержать (обучать) двух администраторов для ее контроля.
- Информационная система имеет вид "черного ящика": все работы по ее администрированию выполняются внешним провайдером, который не может допустить посторонних к этому процессу.

Если в третьей ситуации возможна организация соответствующего распределения ответственности в рамках контракта на поставку услуг, то с первыми двумя случаями дело обстоит сложнее. Возможно, придется назначить отдельного специалиста по безопасности данной информационной системы из имеющихся администраторов и подчинить его (полностью или частично) службе информационной безопасности или комитету, о котором шла речь выше. Возможно, придется выделить понятия "прикладной безопасности", оставив ее в ведении службы, администрирующей данную систему, и "системной безопасности" (то есть безопасности взаимодействия данной системы с остальными), которую отдать общей службе информационной безопасности. Возможно, будет достаточно предоставить службе информационной безопасности доступ к упомянутым электронным регистрационным журналам, файлам конфигураций, учету пользователей и т. д.

Однако для всех трех ситуаций нужно разработать процедуру отчета администраторов систем перед службой информационной безопасности. Детализацию и периодичность отчетов можно согласовывать дополнительно, в зависимости от конкретной системы, но службе безопасности следует иметь полную картину работы всех систем информационного пространства.

Другая проблема, приводящая иногда к выпадению отдельных аспектов из сферы деятельности службы информационной безопасности, — это представление о ней только как о компьютерной службе. Это допустимо, но тогда необходимо подумать о следующем.

Кто в организации курирует вопросы безопасности телефонной связи (сотовые телефоны, мини-АТС, факсимильную связь)? Безопасно ли уничтожение бумажных отчетов предприятия? Как защищены источники электроэнергии и т. п.?

Если всем этим занимаются отдельные службы, то следует также продумать вопросы связи их со службой информационной безопасности. Если же есть необходимость передать контроль над ними в службу информационной безопасности, то следует добавить и необходимое число сотрудников, провести их соответствующее обучение.

УГРОЗЫ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Иванова А.В., студент
Научный руководитель: ст. преподаватель Э.В. Гринцевич
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Информационная безопасность – это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю. Все информационные ресурсы постоянно подвергаются объективным и субъективным угрозам утраты носителя или ценности информации.

Под угрозой или опасностью утраты информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Наиболее распространенные угрозы доступности:

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Специальные вредоносные программы:

– **«компьютерные вирусы»**— это небольшие программы, способные самостоятельно распространятся после внедрения в компьютер путем создания своих копий. При определенных условиях вирусы оказывают негативное воздействие на систему. Например: Virus (вирус) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компьютера.

– **«черви»**– утилиты, которые активируются при каждой загрузке компьютера. Они обладают способностью перемещаться в пределах системы или сети и размножаться аналогично вирусам. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке работы. Например: Worm (червь) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях через сетевые ресурсы. Для активации Worm пользователю необходимо запустить его (в отличие от Net-Worm). Net-Worm (сетевой червь) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения (т.е. непосредственно для активации вредоносной программы).

- «троянские кони»— такие программы «скрываются» под видом полезного приложения, а, на самом деле, наносят вред компьютеру: разрушают программное обеспечение, копируют и пересылают злоумышленнику файлы с конфиденциальной информацией и т.д. Например: Trojan– вредоносная программа, предназначенная для осуществления несанкционированных пользователем действий, влекущих уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей, и при этом не попадающая ни под одно из других троянских поведений.

Канал несанкционированного доступа.

Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов. Этот канал представляет собой совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиден-

циальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Каждая конкретная фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества моментов — профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местоположения здания и т.п.

Функционирование канала несанкционированного доступа к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

Механизмы защиты информации:

1. Разграничение доступа.

Разграничение доступа является одним из основных способов сохранения конфиденциальности информации и является дополнением таких процедур как идентификация и аутентификация. Но разграничение доступа не только позволяет сохранять конфиденциальность информации, но и защищает ее от угроз доступности и целостности. Правильное распределение ролей в системе может уберечь объекты безопасности от случайных или некомпетентных действий, которые могут вызвать потерю или искажение информации.

2. Шифрование.

Одним из наиболее мощных средств обеспечения конфиденциальности является шифрование. Например, для портативных компьютеров шифрование является единственным способом соблюдения конфиденциальности. Используют два основных способа шифрования: симметричное и ассиметричное. В первом случае один и тот же ключ используется и для шифрования и для расшифровки. В ассиметричных подходах используются два ключа. Один из них называется открытым (или публичным) и может свободно передаваться третьим лицам. Второй ключ называется закрытым (или секретным), он должен быть известен только одному субъекту.

3. Электронная подпись.

Электронная подпись решает проблему идентификации передаваемых данных. Электронная подпись представляет собой некоторую вставку в данные (документ), зашифрованную закрытым ключом. При этом сами данные могут быть как в зашифрованном, так и в открытом виде.

4. Антивирусные средства защиты информации.

Массовое распространение вредоносного программного обеспечения, серьезность последствий его воздействия на информационные системы и сети вызвали необходимость разработки и использования специальных антивирусных средств и методов их применения.

АНАЛИЗ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ДАННЫМ

Кошелева К.А., студент
Научный руководитель: старший преподаватель Е.В. Плюснина
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями.

Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Однако именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т.п.). Доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

Несанкционированный доступ к информации (НСД) - Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Причины несанкционированного доступа к информации:

– ошибки конфигурации;

– слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников);

– ошибки в программном обеспечении;

– злоупотребление служебными полномочиями (воровство резервных копий, копирование информации на внешние носители при праве доступа к информации);

– прослушивание каналов связи при использовании незащищённых соединений внутри ЛВС;

– использование клавиатурных шпионов, вирусов и троянов на компьютерах сотрудников для имперсонализации.

Методы несанкционированного доступа. С развитием технологий обработки информации получили распространение методы несанкционированного доступа к информации. Наибольшее распространение получили следующие методы:

1. Работа между строк - подключение к линиям связи и внедрение в компьютерную систему с использованием промежутков в действиях законного пользователя.

2. «Отказы в обслуживании» - несанкционированное использование компьютерной системы в своих целях (например, для бесплатного решения своих задач), либо блокирование системы для отказа в обслуживании другим пользователям. Для реализации такого злоупотребления используются так называемые «жадные программы» - программы, способные захватить монопольно определенный ресурс системы.

3. Повторное использование объектов - состоит в восстановлении и повторном использовании удаленных объектов системы. Примером реализации подобного злоупотребления служит удаление файлов операционной системой. Когда ОС выдает сообщение, что, некоторый файл удален, то это не означает, что информация, содержащаяся в данном файле, уничтожена в прямом смысле слова. Информация, которая была в данном блоке, никуда не исчезает до момента записи на это место другой информации. Одной из разновидностей повторного использования объектов является работа с компьютерным «мусором».

4. Маскарад - захватчик использует для входа в систему ставшую ему известной идентификацию законного пользователя.

5. «Подкладывание свиньи» - нарушитель подключается к линиям связи и имитирует работу системы с целью осуществления незаконных манипуляций. Например, он может имитировать сеанс связи и получить данные под видом легального пользователя.

6. Анализ трафика - захватчик анализирует частоту и методы контактов пользователей в системе. При этом можно выяснить правила вступления в связь, после чего производится попытка вступить в контакт подвидом законного пользователя.

7. «Раздеватели» - комплекс специально разработанных программных средств, ориентированных на исследование защитного механизма программного продукта от НСД и его преодоление.

Развитие средств связи и электронной почты выделило злоупотребление, которое в литературе получило название «пинание» (pinging). Суть данного злоупотребления заключается в том, что, используя стандартные или специально разработанные программные средства, злоумышленник может вывести из строя электронный адрес, бомбардируя его многочисленными почтовыми сообщениями. Следствием «пинания» могут стать осложнения и возможность непреднамеренного игнорирования полученной электронной почты.

Необходимо отметить, что при планировании и разработке злоупотреблений нарушителями могут создаваться новые, не приведенные в данной классификации, а также применяться любые сочетания описанных злоупотреблений.

Виды несанкционированного доступа

Угроза информации - пути реализации воздействий, которые считаются опасными для информационной системы. По характеру возникновения их можно разделить на 2 вида: преднамеренные и непреднамеренные.

Непреднамеренные угрозы - это случайные действия, выраженные в неадекватной поддержке механизмов защиты или ошибками в управлении. А преднамеренные - это несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами, самими системами.

По типу реализации угрозы можно различать:

– программные;

– непрограммные.

К программным относят те, которые реализованы в виде отдельного программного модуля или модуля в составе программного обеспечения. К непрограммным относят злоупотребления, в основе которых лежит использование технических средств информационной системы (ИС) для подготовки и реализации компьютерных преступлений (например, несанкционированное подключение к коммуникационным сетям, съем информации с помощью специальной аппаратуры и др.).

Преследуя различные цели, компьютерные злоумышленники используют широкий набор программных средств. Исходя из этого, представляется возможным объединение программных средств в две группы:

– тактические

– стратегические.

К тактическим относят те, которые преследуют достижение ближайшей цели (например, получение пароля, уничтожение данных и др.). Они обычно используются для подготовки и реализации стратегических средств, которые направлены на реализацию далеко идущих целей и связаны с большими финансовыми потерями для ИС. К группе стратегических относятся средства, реализация которых обеспечивает возможность получения контроля за технологическими операциями преобразования информации, влияние на функционирование компонентов ИС (например, мониторинг системы, вывод из строя аппаратной и программной среды и др.).

Потенциальными программными злоупотреблениями можно считать программные средства, которые обладают следующими функциональными возможностями:

– искажение произвольным образом, блокирование и/или подмена выводимого во внешнюю память или в канал связи массива информации, образовавшегося в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

– сокрытие признаков своего присутствия в программной среде ЭВМ;

– разрушение (искажение произвольным образом) кодов программ в оперативной памяти;

– сохранение фрагментов информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– обладание способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;

Рассмотрев основные методы и виды несанкционированного доступа обратимся к определению модели нарушителя, совершающего вышеперечисленные действия.

При разработке модели нарушителя определяются: 1) предположения о категориях лиц, к которым может принадлежать нарушитель; 2) предположения о мотивах действий нарушителя (целях, преследуемых нарушителем); 3) предположения о квалификации нарушителя и его технической оснащенности (методах и средствах, используемых для совершения нарушения); 4) ограничения и предположения о характере возможных действий нарушителя.

По отношению к автоматизированным информационным технологиям управления (АИТУ) нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренними нарушителями могут быть лица из следующих категорий персонала:

– пользователи (операторы) системы;

– персонал, обслуживающий технические средства (инженеры, техники);

– сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);

– технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здание и помещения, где расположены компоненты АИТУ);

– сотрудники службы безопасности АИТУ;

– руководители различного уровня должностной иерархии.

– Посторонние лица, которые могут быть внешними нарушителями:

– клиенты (представители организаций, граждане);

– посетители (приглашенные по какому-либо поводу);

– представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжение и т.п.);

– представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

– лица, случайно или умышленно нарушившие пропускной режим (без цели нарушения безопасности АИТУ);

– любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: а) безответственность; б) самоутверждение; в) корыстный интерес. При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные, тем не менее, со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к системным наборам данных крупным

успехом, затевая своего рода игру «пользователь против системы» ради самоутверждения либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности АИТУ может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в АИТУ информации. Даже если АИТУ имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно. Всех нарушителей можно классифицировать по четырем параметрам (уровню знаний об АИТУ, уровню возможностей, времени и методу действия). 1. По уровню знаний об АИТУ различают нарушителей:

– знающих функциональные особенности АИТУ, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеющих пользоваться штатными средствами;

– обладающих высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

– обладающих высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

– знающих структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам) нарушителями могут быть:

– применяющие чисто агентурные методы получения сведений;

– применяющие пассивные средства (технические средства перехвата без модификации компонентов системы);

– использующие только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;

– применяющие методы и средства активного воздействия (модификация и подключение дополнительных механических средств, подключение к каналам передачи данных, внедрение программных «закладок» и использование специальных инструментальных и технологических программ).

По времени действия различают нарушителей, действующих:

– в процессе функционирования АИТУ (во время работы компонентов системы);

– в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);

– как в процессе функционирования АИТУ, так и в период неактивности компонентов системы.

Библиографический список

1. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации: Учебное пособие. - Тамбов: Издательство ТГТУ, 2006.

2. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. - 372 с.

3. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. - СПб.: Изд-во Политехн. ун-та, 2009. - 126 с.

СТРУКТУРА ГОСУДАРСТВЕННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Мустафаева С., Малкина С., студенты
Научный руководитель: к.э.н., доцент Г.В. Егорова
ФГБОУ ВО «Поволжский государственный университет сервиса»
г. Тольятти, Россия

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение состояния защищённости информационной среды.

В государственных органах имеется собственная система защиты передаваемой информации, основанная на правовых основах защиты информации.

Правовые основы защиты информации – это законодательный орган защиты информации, в котором можно выделить до 4 уровней правового обеспечения информационной безопасности информации и информационной безопасности (ИБ) предприятия (рисунок 1).

1. Первый уровень правовой основы защиты информации

Первый уровень правовой охраны информации и защиты состоит из международных договоров о защите информации и государственной тайны, к которым присоединилась и Российская Федерация с целью обеспечения надёжной информационной безопасности РФ. Кроме того, существует доктрина информационной безопасности РФ, поддерживающая правовое обеспечение информационной безопасности нашей страны.

Правовое обеспечение информационной безопасности РФ:

- Международные конвенции об охране информационной собственности, промышленной собственности и авторском праве защиты информации в интернете;
- Конституция РФ (ст. 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);
- Гражданский кодекс РФ (в ст. 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне);
- Уголовный кодекс РФ (ст. 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, ст. 273 – за создание, использование и распространение вредоносных программ для ЭВМ, ст. 274 – за нарушение правил эксплуатации ЭВМ, систем и сетей);
- Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ (ст. 10 устанавливает разнесение информационных ресурсов по категориям доступа: открытая информация, государственная тайна, конфиденциальная информация, ст. 21 определяет порядок защиты информации);
- Федеральный закон «О государственной тайне» № 5485-1 (ст. 5 устанавливает перечень сведений, составляющих государственную тайну; ст. 8 – степени секретности сведений и грифы секретности их носителей: «особой важности», «совершенно секретно» и «секретно»; ст. 20 – органы по защите государственной тайны, межведомственную комиссию по защите государственной тайны для координации деятельности этих органов; ст. 28 – порядок сертификации средств защиты информации, относящейся к государственной тайне);
- Федеральные законы «О лицензировании отдельных видов деятельности» № 128-ФЗ, «О связи» № 15-ФЗ, «Об электронной цифровой подписи» № 1-ФЗ, «Об авторском праве и смежных правах» № 5351-1, «О право вой охране программ для электронных вычислительных машин и баз данных» № 3523-1.

Как можно заметить, правовое обеспечение информационной безопасности весьма на высоком уровне, и многие компании могут рассчитывать на полную экономическую информационную безопасность и правовую охрану информации, и защиту, благодаря ФЗ о защите информации.

2. Второй уровень правовой защиты информации

На втором уровне правовой защиты информации (ФЗ о защите информации) – это подзаконные акты: указы Президента РФ и постановления Правительства, письма Высшего Арбитражного Суда и постановления пленумов ВС РФ.

3. Третий уровень правовой защиты информации

К данному уровню обеспечения правовой защиты информации относятся ГОСТы безопасности информационных технологий и обеспечения безопасности информационных систем.

Также на третьем уровне безопасности информационных технологий присутствуют руководящие документы, нормы, методы информационной безопасности и классификаторы, разрабатывающиеся государственными органами.

4. Четвёртый уровень правовой защиты информации

Данный уровень правовой защиты информации образуют локальные нормативные акты, инструкции, положения и методы информационной безопасности и документация по комплексной правовой защите информации, рефераты по которым часто пишут студенты, изучающие технологии защиты информации и компьютерную безопасность.

Рисунок 1 - Структура государственной системы защиты информации

Организационно-технические и режимные меры и методы информационной безопасности:

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая Политика информационной безопасности или Политика безопасности рассматриваемой информационной системы.

Политика безопасности (информации в организации) (англ. Organizational security policy)— совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий (англ. ICT security policy) — правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

Для построения Политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

- Защита объектов информационной системы;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

- определение информационных и технических ресурсов, подлежащих защите;
- выявление полного множества потенциально возможных угроз и каналов утечки информации;
- проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- определение требований к системе защиты;
- осуществление выбора средств защиты информации и их характеристик;
- внедрение и организация использования выбранных мер, способов и средств защиты;
- осуществление контроля целостности и управление системой защиты.

Политика информационной безопасности оформляется в виде документированных требований на информационную систему. Документы обычно разделяют по уровням описания (детализации) процесса защиты.

В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций), сама деятельность организуется специальными государственными органами (подразделениями), либо отделами (службами) предприятия.

В свою очередь государственными органами являются:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю;
- Федеральная служба безопасности Российской Федерации;
- Министерство внутренних дел Российской Федерации;
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
- Службы, организующие защиту информации на уровне предприятия:
- Служба экономической безопасности;
- Служба безопасности персонала;
- Служба информационной безопасности.

СПОСОБЫ РЕАЛИЗАЦИИ СТЕГАНОГРАФИИ

Пронин В.А., студент
Научный руководитель: к.т.н., доцент А.В. Леонидов
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

На сегодняшний день актуальна проблема передачи информации ограниченной доступности по открытым каналам, в том числе и по сети Internet. Так же необходимо, чтобы передаваемая информация, была перехвачена злоумышленником. Для решения задач информационной безопасности недостаточно сделать информацию недоступной для злоумышленника. Потребуется утаить сам прецедент ее передачи. С целью решения такой проблемы можно использовать стеганографические методы защиты. Рассмотрим подробнее эти методы защиты.

Методы типа LSB (Least Significiant Bit, наименьший значащий бит) и похожие. Суть их состоит в смене последних значащих битов в контейнере (изображения, видео или аудиозаписи) на биты скрываемого сообщения. Наглядно это выглядит следующим образом: мы заменяем младшие биты в коде цвета пикселя на изображении. Если считать, что код цвета имеет 32-битное значение, то замена единицы на ноль или наоборот не приведет к изменению картинки, ощутимой для человека. А между тем в этих битах картинки можно спрятать данные. Пример. Предположим, имеется 8-битное изображение в градациях серого. 00h (00000000Ь) обозначает черный цвет, FFh (11111111Ь) - белый. Всего - 256 градаций. Также предположим, что сообщение состоит из 1 байта - например, 01101011Ь. При использовании двух младших бит в описаниях пикселей нам потребуется 4 пикселя. Допустим, они черного цвета. Тогда пиксели, имеющие скрытое сообщение, станут выглядеть следующим образом: 00000001 00000010 00000010 00000011.И цвет пикселей изменится: первого - на 1/255, второго и третьего - на 2/255 и четвертого - на 3/255. Такие градации, малозаметны для человека или незаметны совсем. Подобная методика применяется и для других форматов. Методы LSB являются неустойчивыми к различного рода «шуму». К примеру, в случае если на транслируемый контент накладываются какие-либо «мусорные» биты, это искажает как исходный контент, так и (что особенно важно) скрытое сообщение. Оно может стать нечитаемым.

Второй метод заключается в так называемом «впаивании» скрытой информации. В этом случае происходит совмещение скрываемого изображения (аудио или видео файла) поверх оригинала. Простейший пример - надпись белым цветом на белом же фоне в PDF-документе. Злоумышленники обычно не применяют данный способ по причине простоты обнаружения автоматическими методами. Но этот способ часто используется при создании «водяных знаков» с целью защиты авторства контента. В таком случае данные знаки, как правило, не скрываются.

Третий метод - это использование особенностей форматов файлов. К примеру, это может быть запись информации в метаданные, используемые данным форматом файла, или в различные другие, не используемые зарезервированные поля. Например, это может быть документ Microsoft Word,

внутри которого будет спрятана информация, никак не отображаемая при открытии данного документа.

Еще один способ сокрытия информации применим только к аудио-файлам - это эхо-метод. Он использует неравномерные промежутки между эхо-сигналами для кодировки очередности значений. В общем случае возможно создание условий, при которых данные сигналы будут незаметны для человеческого восприятия. Эхо-сигнал характеризуется тремя параметрами: начальной амплитудой, степенью затухания и задержкой. При достижении некоего порога между сигналом и эхом они смешиваются. В такой точке человеческое ухо не может уже отличить эти два сигнала. Для обозначения логического нуля и единицы используется две различных задержки. Они обе должны быть меньше, чем порог чувствительности уха слушателя к получаемому эху.

Но на практике данный способ тоже не слишком надежен, так как не всегда можно точно определить, когда был передан ноль, а когда единица, и в итоге велика вероятность искажения скрытых данных.

Другой вариант применения стеганографии в аудио-файлах - фазовое кодирование (phase coding). Происходит замена исходного звукового элемента на относительную фазу, которая и является секретным сообщением. Фаза подряд идущих элементов должна быть добавлена таким образом, чтобы сохранить относительную фазу между исходными элементами, в противном случае возникнет искажение, ощутимое для человеческого уха.

На сегодняшний день фазовое кодирование является одним из наиболее результативных способов методов скрытия информации.

Рассмотрим стеганографические методы защиты на примере программ и утилит. Утилита ImageSpyer G2 служит для сокрытия информации в графических файлах с использованием криптографии. При этом поддерживается около 30 алгоритмов шифрования и 25 хеш-функций для шифрования контейнера. Скрывает объем, равный числу пикселей изображения. Опционально доступна компрессия скрываемых данных.

Стеганографический архиваторный плагин StegoTC G2 для Total Comander позволяет скрывать данные в любом изображении, при этом поддерживаются форматы BMP, TIFF и PNG

Утилита RedJPEG предназначена для сокрытия любых данных в JPEG в изображении с помощью авторского стеганографического метода. Использует открытые алгоритмы шифрования, поточный шифр AMPRNG и Cartman II DDP4 в режиме хеш-функции, LZMA-компрессию

Профессиональная расширенная версия RedJPEG XT дополнена маскировкой факта внедрения и усиленной процедурой инициализации поточного шифра на основе характеристик изображения. Включены x86 и x86-64 сборки. Также имеется RedJPEG XT for TC WCX плагин Total Comanderr, обладающий аналогичным функционалом.

Наиболее мощная стеганографическая программа, в плане функционала, является DarkCryptTC. Она поддерживает более сотни различных симметричных и асимметричных криптоалгоритмов. Включает в себя поддержку собственной системы плагинов, предназначенной для блочных шифров (BlockAPI), текстовую, аудио и графическую стеганографию (включая реальную стеганографию JPEG), мощный генератор паролей и систему уничтожения информации и ключей

Список поддерживаемых форматов действительно впечатляет: *.txt, *.html, *.xml, *.docx, *. odt, *.bmp, *jpg, *.tiff, *.png, *.jp2, *.psd, tga, *.mng, *.wav, *.exe, *.dll.

Набор программ для стеганографии не слишком большой, но он вполне достаточен для того, чтобы эффективно скрывать информацию в файлах различных форматов

Заключение. В настоящее время компьютерная стеганография продолжает развиваться: формируется теоретическая база, ведется разработка новых, более стойких методов встраивания сообщений. Среди основных причин наблюдающегося всплеска интереса к стеганографии можно выделить принятые в ряде стран ограничения на использование сильной криптографии, а также проблему защиты авторских прав на художественные произведения в цифровых глобальных сетях.

Библиографический список

1. Быков, С.Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии // Защита информации. Защита информации. Конфидент. — СПб.: 2000, № 3.

2. Конахович, Г.Ф., Пузыренко, А.Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

3. Грибунин, В.Г., Оков, И.Н., Туринцев, И.В. Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.

4. Рябко, Б.Я., Фионов, А.Н. Основы современной криптографии и стеганографии. — 2-е 2013 — 2-е изд. — М.: Горячая линия — Телеком, 2013.
5. Завьялов, С.В., Ветров, Ю.В. Стеганографические методы защиты информации : учеб. пособие 2012 . Спб.: Изд-во Политехн. ун-та, 2012. −190 с.

ПРОБЛЕМЫ ЭКСПЕРТИЗЫ ИНФОРМАЦИОННЫХ МАТЕРИАЛОВ, СОДЕРЖАЩИХ ПРИЗНАКИ ИДЕОЛОГИИ ТЕРРОРИЗМА

Рожков Р.О., студент
Научный руководитель: к.п.н., доцент Е.Н. Горбачевская
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Быстрое развитие информационных технологий, в частности сети интернет, способствует обмену большим количеством информации. Но не вся информация полезна или безопасна для общества и страны. В настоящее время в мире актуальна проблема терроризма, а глобальная сеть помогает быстрому распространению различных материалов и пропаганды этой идеологии. Правительство в свою очередь совершенствует законы для противодействия терроризму, например «пакет Яровой» включающий в себя 2 законопроекта:

– Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»;

– Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Одной из проблем экспертизы информационных материалов является поиск в сети интернет незаконной информации. Для решения этой проблемы Роскомнадзором был создан единый реестр запрещённых сайтов, а так же ресурс eais.rkn.gov.ru, в функцию которого входит прием сообщений о наличии на страницах сайтов в сети Интернет противоправной информации.

Проверка жалоб включает в себя нескольких этапов:

– поданные сообщения проверяются на спам;
– сотрудники Роскомнадзора проверяют заявления о потенциально неприемлемых сайтах;
– заявки направляются для получения экспертного заключения о наличии нарушений;
– ресурс вносится в реестр запрещенных сайтов;
– провайдеры этих сайтов получают уведомление.

Если жалоба на ресурс будет принята, то сайт может быть заблокирован в течение шести дней от даты жалобы:

– 24ч на отправку запроса в соответствующий уполномоченный орган;
– 24ч на рассмотрение обращения уполномоченным органом и отправку ответа в Роскомнадзор;
– 72ч на удаление неприемленного контента владельцем ресурса или блокировку страницы хостингом;
– 24ч на блокировку страницы оператором связи, если информация не будет удалена владельцем сайта или доступ к ней не заблокируют интернет-провайдеры.

В тоже время возникает проблема в том, что интернет создавался как самоорганизующееся и саморегулируемое сообщество, и попытки ввести какие-либо дополнительные ограничения вызывают негативную реакцию и общественный резонанс со стороны интернет-сообщества.

Для определения является ли информация допустимой или нет существуют различные виды экспертизы. Например, психолого-лингвистическая экспертиза. Основной проблемой проведения судебной психолого-лингвистической экспертизы материалов по делам, связанным с противодействием экстремизму и терроризму является то, что авторами определены компетенции экспертов: лингвист определяет, «что именно сказано», психолог - «почему, для чего». Возникают вопросы: что изучает психолог в тексте, что является объектом и предметом именно его исследования, как научно и методологически увязать религиоведческое исследование с работой лингвиста и психолога?

В делах подобного рода законодатель делает акцентирует внимание на человеке, а не на тексте. Так как, уголовной ответственности подлежит человек, осуществивший экстремистскую деятельность. Согласно ФЗ № 114 от 25 июля 2002 г. и ФЗ № 148 от 27 июля 2006 г. экстремизмом является деятельность, «направленная на». В ППВС № 11 от 28 июня 2011 г. разъясняется, что, если данная деятельность совершается для разжигания определённой ненависти или вражды, она считается преступлением «независимо от того, удалось побудить других граждан или нет», а в п. 8 имеется указание на учёт «направленности умысла лица», но не текста. Исходя из этого, по данной категории дел экспертам необходимо изучать деятельность субъекта правонарушения, причём существенными являются её цель и мотивы.

Однако в интернете установить личность автора текста бывает крайне сложно, существуют различные методы анонимного входа в интернет, а способы раскрытия порой являются неоправданно ресурсо- и времязатратными. Примером может служить анонимная сеть Tor, принцип ее работы заключается в создании локального прокси-сервера, который подключается к сети Tor, каждый пакет данных перед отправление шифруется 3 ключами для каждого узла и проходит случайным образом через 3 различных прокси-сервера которые по очереди расшифровывают ключи и узнают на какой далее узел отправить пакет. Но поскольку на последнем узле пакеты полностью расшифровываются, то он знает сообщение, но не знает отправителя, так же все интернет-шлюзы до сервера-адресата получают сообщение расшифрованным. Адресата же знает только первый узел, но он не знает сообщения. Техническая информация о сетевом адресе сервера-получателя может выдаваться по средствам DNS-запросов к DNS-серверу которые легко определяются интернет-провайдером.

Следовательно, для решения проблемы экспертизы информационного материала необходимо постоянно повышать квалификацию специалистов в области защиты ИТ-технологий и психолого-лингвистической экспертизе, так же использовать различные сервисы и персонал для выявления неприемлемой информации в сети интернет.

Библиографический список

1. Баранов, А.Н. Лингвистическая экспертиза текста: теория и практика уч. пособие. М.: Флинта: Наука, 2007

2. Дмитриев, А.В., Латынов, В.В., Хлопьев, А.Т. Неформальная политическая коммуникация. М.: РОССПЭН, 1997. – 197 с.

3. Рассолов, И.М. Право и Интернет. Теоретические проблемы. М.: Норма. 210 с.

4. Баранов, А.Н., Грунченко, О.Б., Левонтина, И.Б. Лингвистическое исследование текстов для выявления в них призывов к осуществлению экстремистской деятельности. М., 2008.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ

Федосеев М.Ю., студент
ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева»
г. Самара, Россия

Защита виртуальных сред информации в виртуальных инфраструктурах сегодня актуальна как никогда.

С 1 июня 2017 года в РФ вступит в силу ГОСТ Р 56938-2016 Национальный стандарт РФ «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения», который стандарт устанавливает требования по защите информации, обрабатываемой с использованием технологий виртуализации. В нем рассматриваются угрозы безопасности и меры защиты информации, обрабатываемой с помощью технологий виртуализации.

Виртуализацией называют группу технологий, основанных на преобразовании формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Под термином "виртуализация" объединяется множество информационных технологий, призванных снижать затраты на разворачивание компьютерной сети организации, повышать отказоустойчивость применяемых серверных решений, а также достигать других преимуществ. Виртуализация представляет собой имитацию программного и/или аппаратного обеспечения, в среде (на базе) которого функционируют различные программы.

Виртуализацию проводят в отношении:

- программ;
- вычислительных систем;
- систем хранения данных;
- вычислительных сетей;
- памяти;
- данных.

При использовании технологий виртуализации создаются (виртуальные и виртуализованные) объекты доступа, подлежащие защите наравне с другими объектами информационных систем, в том числе аппаратные средства информационных систем, используемые для реализации технологий виртуализации. К основным объектам защиты при использовании технологий виртуализации относят:

- средства создания и управления виртуальной инфраструктурой (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных, консоль управления виртуальной инфраструктурой и др.);
- виртуальные вычислительные системы (ВМ, виртуальные сервера и др.);
- виртуальные системы хранения данных;
- виртуальные каналы передачи данных;
- отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование и др.);
- виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации;
- периметр виртуальной инфраструктуры (задействованные при реализации технологий виртуализации центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и др.).

Для защиты перечисленных объектов используют как виртуальные средства ЗИ и средства ЗИ, предназначенные для использования в среде виртуализации, являющиеся разновидностями средств ЗИ, так и другие виды средств ЗИ.

На протяжении последнего 10-летия сохраняется неизменно высокий интерес к технологии виртуализации, которая считается одной из наиболее перспективных среди доступных для компаний ИТ-технологий. VMWare, Microsoft, Intel и многие другие производители сегодня занимаются разработкой платформ виртуализации. Среди представленных на рынке одной из наиболее востребованных является платформа VMware. Использование этой технологии виртуализации позволяет не менее чем в два раза снизить расходы на программные и аппаратные ИТ-средства. Однако, как часто и бывает с новейшими разработками, защита информации пока осуществляется не на достаточном уровне. Причиной этого является то, что технологии VMware пришли на российский рынок недавно и находятся в процессе развития. Лидерами индустрии уже активно развивается защита виртуализации, но на сегодняшний день уровень безопасности все еще невысок. Согласно исследованию, проведенному агентством Gartner, 60% виртуальных машин защищены хуже, чем их физические аналоги. Одной из причин отсутствия надежной защиты виртуальных сред, как отмечает агентство, может быть тот факт, что 40% проектов виртуализации в компаниях запускаются без участия специалистов по информационной безопасности.

Преимущества технологии виртуализации. По мнению аналитической компании Gartner, технология виртуализации вошла в число 10 наиболее перспективных технологий для корпоративного сектора. Внедрение виртуализации позволяет снизить капитальные и эксплуатационные затраты на ИТ-инфраструктуру:

- Снижение расходов на оборудование: серверы и аппаратные средства защиты;
- Экономия электроэнергии;
- Экономия площади серверных помещений.

Итоговый экономический эффект обычно выражается в не менее, чем двукратном снижении стоимости владения (TCO).

Основные бизнес-применения виртуализации:

- Виртуализация серверов. Перенос физических серверов в виртуальные машины одного физического сервера, оснащенного средством виртуализации. Применяется для консолидации серверов, позволяет более эффективно управлять инфраструктурой, повысить надежность и снизить расходы (TCO). Примеры: VMware ESX Server + vCenter (vSphere), Microsoft Hyper-V + SCVMM, Citrix XenServer + Essentials.

- Виртуализация рабочих мест пользователей. Это централизованное хранение рабочих мест в виде виртуальных машин на сервере с последующей доставкой на физические рабочие места или предоставление удаленного доступа через виртуализацию представлений (терминальные сервисы). Применяется для сокращения расходов на администрирование и обновления ПО на рабочих местах, повышения безопасности информации на рабочих местах и сокращения расходов на лицензии ПО (в варианте терминальных сервисов). Примеры: VMware View, Microsoft MED-V, Citrix XenDesktop, Sun VDI.

К дополнительным возможностям виртуализации можно отнести:

– Локальные гипервизоры виртуальных машин (VMware Workstation и т.п.);

– Виртуализация приложений (VMware ThinApp, Microsoft App-V, Citrix XenApp).

Безопасность виртуальной инфраструктуры - композиции иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств. Использование технологий виртуализации создает предпосылки для появления угроз безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации. Защита среды виртуализации информационных систем компании требует эффективных решений для борьбы с новыми, ранее неизвестными угрозами. Среди угроз виртуализации, которым открыты данные технологии, можно отметить:

– угроза компрометации гипервизора (Hyper-V, vSphere) как нового, по сравнению с физической средой, элемента управления инфраструктурой;

– угроза утечки данных вследствие злонамеренных или непреднамеренных действий системного администратора, получающего доступ к данным и к инфраструктуре;

– клонирование\копирование, миграция, репликация, создание снимков виртуальных машин;

– компрометация консолидированного хранилища данных при консолидации нескольких серверов на одном аппаратном комплексе, если компания прибегает к серверной виртуализации;

– угроза несанкционированного доступа (НСД) администратора виртуальной инфраструктуры к настройкам и правам пользователей на сервере виртуализации;

– отсутствие контроля за всеми событиями информационной безопасности и невозможность расследования инцидентов при их возникновении.

Безопасность виртуальной инфраструктуры. Безопасность информации, обрабатываемой в виртуальной среде, - один из ключевых вопросов при внедрении технологии виртуализации:

– Виртуальным серверам присущи ровно те же уязвимости, что и физическим;

– Как и любая новая технология, виртуализация несет в себе новые угрозы безопасности.

Угрозы безопасности для виртуальных инфраструктур:

– Атака на гипервизор с виртуальной машины.

– Атака на гипервизор из физической сети.

– Атака на диск виртуальной машины.

– Атака на средства администрирования виртуальной инфраструктуры.

– Атака на виртуальную машину с другой виртуальной машины.

– Атака на сеть репликации виртуальных машин.

– Неконтролируемый рост числа виртуальных машин.

– Защита информации в соответствии с законодательством.

Одной из ключевых проблем использования технологий виртуализации является легитимность защиты информации, которая обрабатывается в виртуальной среде.

Согласно российскому законодательству организации обязаны обеспечить надлежащую защиту конфиденциальной информации, с которой они работают, в том числе с применением сертифицированных средств защиты.

Эти проблемы касаются как информации, содержащей сведения, составляющие государственную тайну, так и конфиденциальной информации – коммерческой тайны или персональных данных.

Недостатки традиционных средств защиты. Проблемы внедрения технологий виртуализации связаны с тем, что с одной стороны, традиционные средства защиты информации не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. С другой стороны, они не защищают от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры.

Если нарушитель получает доступ к среде виртуализации, операционная среда традиционных СЗИ оказывается полностью скомпрометированной.

Из среды гипервизора нарушитель может незаметно для традиционных СЗИ, работающих в виртуальных машинах:

– копировать и блокировать весь поток данных, идущий на все устройства (HDD, принтер, USB, сеть, дискеты);

– читать и изменять данные на дисках виртуальных машин, даже когда они выключены и не работают, без участия программного обеспечения этих виртуальных машин.

Библиографический список

1. ГОСТ Р 56938-2016 Национальный стандарт РФ «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».

2. Защита информации при использовании виртуализации. [Электронный ресурс] - http://www.securitycode.ru/solutions/zashchita-informatsii-virtualization/.

3. Виртуализация. Википедия. [Электронный ресурс] - https://ru.wikipedia.org/wiki/.

4. Виртуализация: новый подход к построению IT-инфраструктуры. [Электронный ресурс] - http://www.ixbt.com/cm/virtualization.shtml.

5. Виртуализация. Классификация и области применения. [Электронный ресурс] - http://www.tadviser.ru/index.php/.

ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ ВИРУСОВ

Калинин М.С., студент
Научный руководитель: к.т.н., доц. Трубачева С.И.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Технологии, применяемые в антивирусах, можно разбить на две основные категории:

– технологии сигнатурного анализа;

– технологии вероятностного анализа.

Сигнатурный анализ

Сигнатурный анализ (СА) - метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур[1] вирусов.

СА является наиболее известным методом обнаружения вирусов и используется практически во всех современных антивирусах. Для проведения проверки антивирусу необходим набор вирусных сигнатур, который хранится в антивирусной базе[2]. Ввиду того, что СА предполагает проверку файлов на наличие сигнатур вирусов, антивирусная база нуждается в периодическом обновлении для поддержания актуальности антивируса. Сам принцип работы СА также определяет границы его функциональности - возможность обнаруживать лишь уже известные вирусы - против новых вирусов сигнатурный сканер бессилен.

Наличие сигнатур вирусов предполагает возможность лечения инфицированных файлов, обнаруженных при помощи СА. Однако, лечение допустимо не для всех вирусов: трояны и большинство «червей» не поддаются лечению по своим конструктивным особенностям, поскольку являются цельными программными модулями (ПМ), созданными для нанесения ущерба вычислительной машине (ВМ).

Профессиональная реализация вирусной сигнатуры позволяет обнаруживать известные вирусы с большой степенью вероятности.

Вероятностный анализ

Технологии вероятностного анализа (ВА), в свою очередь, подразделяются на три группы:

– эвристический анализ;

– поведенческий анализ;

– анализ контрольных сумм.

Эвристический анализ

Эвристический анализ (ЭА) - технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов.

В процессе ЭА проверяется структура файла, его соответствие вирусным шаблонам. Наиболее популярной эвристической технологией является проверка содержимого файла на предмет наличия модификаций уже известных сигнатур вирусов и их комбинаций. Это помогает определять гибриды и новые версии ранее известных вирусов без дополнительного обновления антивирусной базы.

[1] Сигнатура вируса или вредоносной программы — последовательностям байтов данных, характерных для вируса или вредоносной программы.

[2] Антивирусная база - база данных, в которой хранятся сигнатуры вирусов.

ЭА применяется для обнаружения неизвестных вирусов, и, как следствие, не предполагает лечения.

Данная технология не способна на 100% определить вирус, и как любой вероятностный алгоритм «грешит» ложными срабатываниями.

Поведенческий анализ

Поведенческий анализ (ПА) - технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций. ПА достаточно узко применим на практике, так как большинство действий, характерных для вирусов, могут выполняться и обычными приложениями. Наибольшую известность получили ПА макросов, поскольку соответствующие вирусы практически всегда выполняют ряд однотипных действий. Например, для внедрения в систему почти каждый макровирус использует один и тот же алгоритм: в какой-нибудь стандартный макрос, автоматически запускаемый средой MSOffice при выполнении стандартных команд (например, "Save", "Save As", "Open", и т.д.), записывается код, заражающий основной файл шаблонов normal.dot и каждый вновь открываемый документ.

Средства защиты, вшиваемые в BIOS, также можно отнести к поведенческим анализаторам. При попытке внести изменения в MBR ВМ, анализатор блокирует действие и выводит соответствующее уведомление пользователю.

Помимо этого ПА могут отслеживать попытки прямого доступа к файлам, внесение изменений в загрузочную запись, форматирование жестких дисков и т.д.

ПА не используют для работы дополнительных объектов, подобных вирусным базам и, как следствие, неспособны различать известные и неизвестные вирусы - все подозрительные программы априори считаются неизвестными вирусами. Аналогично, особенности работы средств, реализующих технологии ПА, не предполагают лечения.

Возможно выделение действий, однозначно трактующихся как неправомерные - форматирование жестких дисков без запроса, удаление всех данных с логического диска, изменение загрузочной записи без соответствующих уведомлений и пр. Тем не менее, наличие действий неоднозначных - например, макрокоманда создания каталога на жестком диске, заставляет также задумываться о ложных срабатываниях и, зачастую, о тонкой ручной настройке поведенческого блокиратора.

Анализ контрольных сумм

Анализ контрольных сумм (АКС) - это способ отслеживания изменений в объектах ВМ. На основании анализа характера изменений - одновременность, массовость, идентичные изменения длин файлов - можно делать вывод о заражении системы. АКС (также используется название "ревизоры изменений") как и ПА не используют в работе дополнительные объекты и выдают заключение о наличии вируса в системе исключительно методом экспертной оценки. Большая популярность АКС связана с воспоминаниями об однозадачных операционных системах (ОС), когда количество вирусов было относительно небольшим, файлов было немного и менялись они редко. В настоящее время АКС утратили свои позиции и используются в антивирусах сравнительно редко. Чаще применяются в сканерах при доступе: при первой проверке с файла снимается контрольная сумма и помещается в кэш, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

Вывод

Делая вывод, отметим, что сегодня практически каждый антивирус использует несколько из перечисленных выше технологий, при этом использование сигнатурного и эвристического анализа для проверки файлов является повсеместным.

Очевидно, что использование этих технологий не дает стопроцентной гарантии. На сегодняшний день лучшим способом борьбы с новыми угрозами является максимально быстрое реагирование разработчиков на появление новых экземпляров вирусов выпуском соответствующих сигнатур. Также, учитывая наличие активных вредоносных программ, необходимо не менее быстро реагировать на обнаружение новых уязвимостей в ОС и устанавливать соответствующие «заплаты» безопасности.

Библиографический список

1. http://www.kasperskylab.ru
2. http://www.viruslist.com
3. http://support.drweb.com/faq
4. http://www.antivir.ru
5. http://www.drweb.ru/com
6. http://www.avirus.ru/
7. http://ru.wikipedia.org/

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЭКОЛОГИЧЕСКИ БЕЗОПАСНОГО КОМПЛЕКСОНА ОЭДФ ДЛЯ ОПРЕДЕЛЕНИЯ МЕДИ МЕТОДОМ КОМПЛЕКСОНОМЕТРИЧЕСКОГО ТИТРОВАНИЯ

Глухова О.А., Вахрамеев В.В., студенты
Научный руководитель: к.п.н., доцент И.Б. Богатова
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

В аналитическом контроле определение содержания меди варьируется в широких пределах. Для определения низких концентраций меди в природных объектах используются инструментальные, физико-химические методы анализа. Для более высоких концентраций меди в травильных растворах машиностроительной и радиоэлектронной промышленности, сточных водах гальванических производств используют метод комплексонометрического титрования. [1].

Сегодня подавляющее большинство комплексонных препаратов базируется на использовании этилендиаминтетрауксусной кислоты (ЭДТА) и ее солей. Однако доказано, что ЭДТА накапливается в мировом океане и вызывает растворение отложений токсичных металлов с переходом их в раствор в виде стабильных и часто липидорастворимых комплексонатов, что приводит к отравлению планктона, рыб, птиц и высших животных. [2]. Поэтому исследование возможностей замены применяемых комплексонов на менее токсичные, ввиду сложившейся экологической обстановки является важным и актуальным.

В качестве эффективной альтернативы ЭДТА и её аналогам, загрязняющим окружающую среду, нами предлагается использование в аналитическом контроле экологически безопасного комплексона – **1-гидрокси этилиден-1,1-дифосфоновой кислоты (**ОЭДФ).

Кислота ОЭДФ – пятиосновная кислота, молекулярная формула: $C_2H_8O_7P_2$ [3]. Оксиэтилидендифосфоновая кислота пожаро- и взрывобезопасна, по степени воздействия на организм относится к веществам 3-го класса опасности. Оксиэтилидендифосфоновая кислота не проявляет кумулятивных свойств при попадании в водоемы, это объясняется способностью некоторых микроорганизмов расщеплять молекулу ОЭДФ с помощью выделяемых ферментов и потреблять фосфор. Несмотря на то, что в первую очередь потребляется фосфор из неорганических соединений, наличие процесса разрушения ОЭДФ под действием бактерий исключает ее накопление в водоемах.

ОЭДФ содержит две фосфоновые группы, способные к комплексообразованию в кислой среде, и оксиэтильную группу, кислота способна образовывать хелатные соединения с ионами меди (Cu^{+2}) с условной константой устойчивости $7{,}9\cdot10^{16}$. При соотношении Cu^{2+} и ОЭДФ равном 1:1 образуются моноядерные комплексы состава CuHL, для которых установлены следующие оптимальные области устойчивости при pH: 3.8-6.0 и 8.2-9.0. Процессы комплексообразования начинаются в кислой области pH 1,0-2,5; при pH> 12,5 комплексные соединения разрушаются. [4].

Нами проведено сравнительное определение содержания меди с использованием традиционного комплексона ЭДТА и предлагаемого ОЭДФ методом комплексонометрического титрования. В качестве металлоиндикатора использовали мурексид, который с катионами меди образует желтое окрашивание при PH 8 с константой устойчивости $1{,}4\cdot10^{14}$. Количество катионов меди, находящихся в связанном состоянии определяли титрованием соответствующим комплексоном известной концентрации. Поскольку титранты образуют более прочные комплексы с медью (константа устойчивости комплекса ЭДТА с медью состава CuL – $6{,}3\cdot10^{18}$) по сравнению с мурексидом, то последний вытесняется из комплекса, и в точке эквивалентности желтая окраска исчезает, появляется фиолетовое окрашивание, соответствующее раствору свободного мурексида.

Выполнение определения. В колбу для титрования емкостью 100 мл отбирали пипеткой 1,5, 2,0, 2,5 мл стандартного раствора меди (II), содержащего 1мг/мл Cu^{2+}, мерным цилиндром прибавляли 25 мл дистиллированной воды, 1мл аммиачного буферного раствора с pH = 8 – 10 и на кончике шпателя вносили 10-20 мг металлоиндикатора. Смесь перемешивали, и полученный раствор титровали раствором соответствующего комплексона - ЭДТА либо ОЭДФ до изменения окраски от красной в синюю с использованием эриохромого черного Т, либо от желтой в фиолетовую с использованием мурексида. Если при добавлении 1мл аммиачного буферного раствора цвет раствора не изменялся, титрование прекращали и измеряли объем израсходованного на титрование раствора комплексона. Содержание меди(II) в анализируемом растворе рассчитывали по формуле

$$C\,Cu^{+2} = \frac{V \cdot N}{V_1}$$

где: V - объём раствора комплексона, пошедшего на титрование (титранта), куб. см;
N - нормальность раствора комплексона;
V_1 - объем анализируемой пробы, куб. см.
Массу меди в пробе рассчитывали по формуле:

$$mCu = C_{Cu+2} \cdot Э_{Cu} \cdot V_1$$

где: $Э_{Cu}$- грамм-эквивалент меди в данной реакции с комплексоном;
V_1 – объем стандартного раствора меди, куб. дм.
Результаты представлены в таблицах 1 и 2:

Таблица 1 - Содержание меди (II) в искусственных смесях при использовании комплексона ЭДТА

V_1 стандарт. раствора Cu^{+2}, С 1мг/мл, мл	Металлоиндикатор	V ЭДТА, мл C_N =0,05моль/л	mCu, введено, мг	mCu, определено, мг
1,5	мурексид	1,0	1,5	1,58
2,5	мурексид	1,6	2,5	2,54
1,0	Эриохром черный -Т	0,6	1,0	0,95
2,5	Эриохром черный -Т	1,5	2,5	2,38
2,0	Эриохром черный -Т	1,3	2,0	2,06

Таблица 2 - Содержание меди (II) в искусственных смесях при использовании комплексона ОЭДФ

V_2 стандарт. раствора Cu^{+2}, С 1мг/мл, мл	Металлоиндикатор	V ОЭДФ, мл C_N =0,1моль/л	mCu, введено, мг	mCu, определено, мг
1,0	мурексид	0,3	1,0	0,93
1,5	мурексид	0,5	1,5	1,58
2,5	мурексид	0,8	2,5	2,54
2,0	Эриохром черный -Т	0,7	2,0	2,22
3,0	Эриохром черный -Т	1,0	3,0	3,17

Эксперимент показал, что в оперативном контроле меди можно использовать экологически безопасный комплексон **ОЭДФ – (1-Гидрокси Этилиден-1,1-Дифосфоновая Кислота), обладающий способностью в условиях живой природы распадаться на фрагменты, что выгодно его отличает от других соединений подобного класса.**

Библиографический список

1. Определение содержания меди комплексонометрическим методом в промывочных растворах. РД 34.37.305.3-97.

2. Пршибил, Р. Аналитические применения этилендиаминтетрауксусной кислоты и родственных соединений – М.: Мир, 1975. – 533 с.

3. Дятлова, Н.М., Темкина, В.Я., Попов, К.И. Комплексоны и комплексонаты металлов. М.: Химия, 1988. – 544 с.

4. Аксенова, Н.В., Попова, Т.В., Грунин, Ю.Б. Стабилизация меди(I) комплексообразованием с фосфорсодержащими лигандами. Материалы VIII Всероссийской конференции «Структура и динамика молекулярных систем» Яльчик, 25-30 июня, 2001.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ПОТРЕБИТЕЛЬСКОГО КРЕДИТОВАНИЯ НАСЕЛЕНИЯ

Аринина Д.В., студент
Научный руководитель: ст. преподаватель Г.И. Гончарова
ОАНО ВО «Волжский университет имении В.Н. Татищева»
г. Тольятти, Россия

Сфера потребительского кредитования подвержена определенным внешним и внутренним факторам, которые негативно влияют на экономическую безопасность кредитной организации.

Рынок потребительского кредитования населения является неотъемлемой составляющей экономической стабильности, важнейшим фактором ускорения роста российской экономики. В связи с этим определяется актуальность темы статьи.

Цель данной работы: выявить проблемы обеспечения безопасности кредитной организации в сфере потребительского кредитования населения, и определить мероприятия по ее укреплению.

Исходя из поставленной цели, можно обозначить следующие задачи нашей работы:

- дать понятие экономической безопасности потребительского кредитования;
- определить проблемы экономической безопасности в сфере потребительского кредитования;
- предложить мероприятия по устранению угроз экономической безопасности потребительского кредитования;

Потребительское кредитование в настоящее время – это особая форма кредита, предоставляемая его получателям. В потребительском кредите заемщиками являются физические лица - население, а кредиторами - специальные кредитные учреждения.

Экономическая безопасность кредитной организации, работающая с потребительскими кредитами, основывается на том, насколько эффективно удается устранять ущербы от негативных воздействий на аспекты экономической безопасности кредитования.

На сегодняшний день российские банки - лидеры потребительского кредитования сократили объемы деятельности в данной сфере.

Рассмотрим таблицу 1, где представлена динамика объемов потребительского кредитования банков ведущих в данной сфере.

Таблица 1 – Изменение рейтинга банков по объему потребительского кредитования, млн. руб.

Наименование банка	**1.10.2016**	**1.10.2015**	**Изменение**	
			абс., млн. руб.	**отн., %**
Сбербанк России	4118,5	4014,7	103,8	2,59
ВТБ 24	1368,5	1401,2	-32,6	-2,33
Газпромбанк	289,8	301,1	-11,3	-3,76
Россельхозбанк	286,3	274,6	11,6	4,23
Альфа - банк	247,9	281,9	-33,9	-12,04

Нестабильность банковского сектора, ухудшение его положения в экономической среде напрямую связаны с ростом невозвратности кредита.

Рассмотрим на рис. 1 динамику объемов потребительских кредитов и просроченной задолженности в целом по России.

По данным рисунка 1, можно определить, что существенно увеличилась сумма невозвратности по потребительским кредитам, на 01.10.2016 год данный показатель составил 862 млрд. руб., что значительно выше, чем на 01.10.2011, который составлял 281,7 млрд. руб.

Стоит отметить, что по состоянию на 01.10.2016 г. объем потребительских кредитов составил 10656,5 млрд. руб., а число просроченных задолженностей составило 862 млрд. руб.

Таким образом, можно утверждать, что объем предоставления потребительских кредитов по сравнению с 2015 г. сократился на 647,2 млрд. руб., при этом уровень просроченной задолженности по кредитам увеличился на 195,6 млрд. руб.

Рост невозвратности по потребительским кредитам и напрямую связан со сложной социально-экономической ситуацией в стране: ростом уровня безработицы в Российской федерации. Рассмотрим источник негативного воздействия на экономическую безопасность банковского сектора, такой как безработица населения.

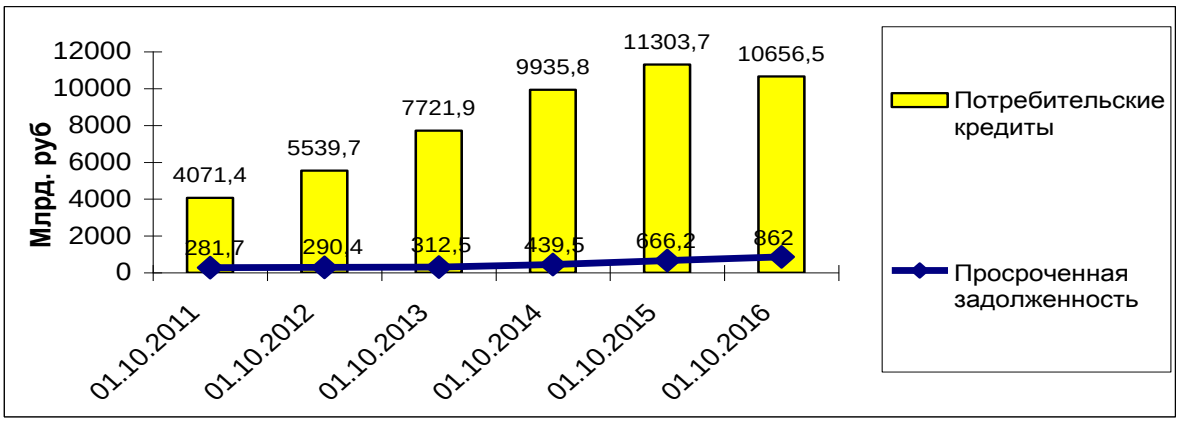


Рисунок 1 – Динамика объемов потребительского кредита и просроченной задолженности, руб.

На рис. 2 показана динамика уровня безработного населения в Российской Федерации в тыс. чел.

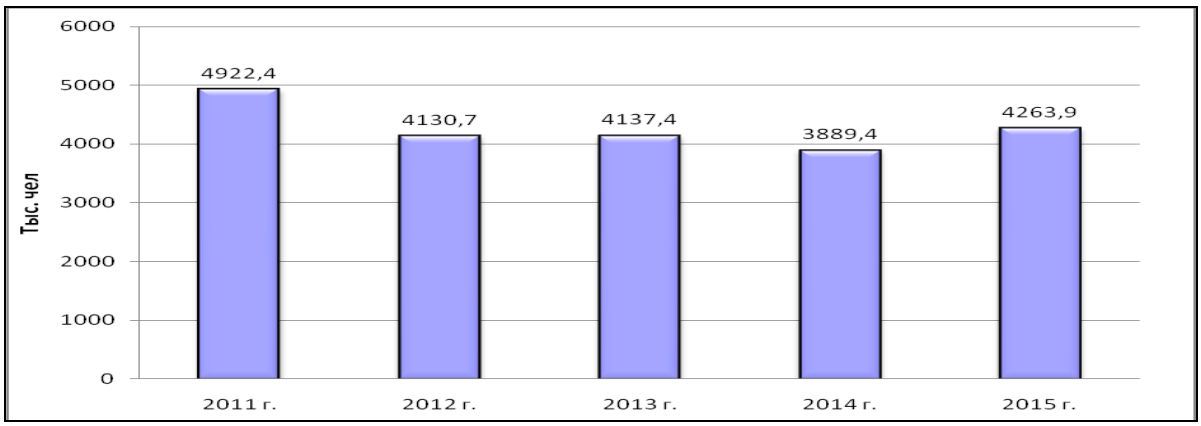


Рисунок 2 – Динамика уровня безработицы в России, тыс. чел.

По данным рис.2 можно сделать следующий вывод: уровень безработного населения на 2015 год составил 4263,9 тыс. чел от общей численности населения страны, это существенно выше, чем показатель на 2011 год, который составил 2889,4.

Сопоставив рис. 1 и рис. 2 можно выявить закономерность в росте безработицы и росте невозвратности кредита, что подвергает нестабильности безопасность деятельности банков в сфере потребительского кредитования населения и экономики страны в целом.

Подведя итог вышесказанному, можно определить следующие проблемы в сфере потребительского кредитования населения:

1. Финансовый кризис последних лет.
2. Проблемы с трудоустройством потенциальных клиентов.
3. Минимум прогрессивных кредитных программ.
4. Завышенные ставки по потребительским кредитам.
5. Мало отлаженная работа кредиторов с должниками.

В целях устранения выявленных проблем следует принять во внимание следующие рекомендации в сфере потребительского кредитования населения:

1. Создавать гибкие программы кредитования для различных категорий граждан.
2. Сокращать уровень негативных социально-экономических последствий для населения.
3. Создавать программы или мероприятия, направленные на уменьшения просроченной задолженности.

Таким образом, экономическая безопасность кредитной организации, работающей с потребительскими кредитами, базируется на том, насколько эффективно службам данной организации удается предотвращать угрозы и устранять ущербы от негативных воздействий на аспекты экономической безопасности кредитования.

ВЗАИМОСВЯЗЬ УСТОЙЧИВОГО РАЗВИТИЯ ГОСУДАРСТВА И ЕГО НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Безрукова Е.А, Бурундукова Д.В., студенты
Научный руководитель: д.э.н., профессор А.Я. Щукина
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

До недавнего времени под национальной безопасностью понималось сохранение суверенитета и территориальной целостности государства, обеспечение его дееспособности перед лицом угрозы применения вооруженной силы со стороны других субъектов международных отношений. Однако реалии последних лет потребовали иной трактовки содержания национальной безопасности. Сегодня национальная безопасность видится как комплексная системная проблема, которая должна рассматриваться в более широком контексте и учитывать наличие многообразных факторов и угроз, а не только угрозы военного нападения, захвата территории и физического уничтожения населения.

В настоящее время проблема безопасности испытывает настоятельную потребность в поиске новых идей и решений, определении долговременных интересов и приоритетов внешней и внутренней политики, проведении последовательных, сбалансированных, системных преобразований в обществе и государстве. Поэтому сегодня в обеспечении национальной безопасности на первый план выступает проблема комплексного видения всех составляющих безопасности в их взаимоувязанном и взаимообусловленном виде. Иными словами, комплексная безопасность – это совокупное решение ключевых проблем жизни и деятельности человека, а также создание такой стратегии, которая обеспечит ему устойчивое развитие на продолжительный период времени. Задача создания такой стратегии стала еще более актуальной в связи с кризисными явлениями в экономике, ростом техногенных и природных катастроф. В связи с этим данная проблема является актуальной.

Для того чтобы уяснить сущность и содержание национальной безопасности, дадим определение субъекта безопасности. Субъектом безопасности является тот, кто обладает правами и обязанностями по ее обеспечению; тот, кто защищает. Отсюда объект безопасности - это то, что подлежит защите.

Основным же субъектом обеспечения национальной безопасности выступает государство, осуществляющее функции в этой области через органы власти. Так трактует объекты безопасности Закон РФ 1992 г. «О безопасности».

Таким образом, сущность национальной безопасности определяется как состояние защищенности страны, которое возникает в процессе взаимодействия органов государственной власти, организаций и общественных объединений для защиты национальных интересов от угроз. Содержание же этого понятия образуют понятия «национальный интерес», «угроза национальной безопасности» и «система обеспечения национальной безопасности [1].

К основным принципам обеспечения национальной безопасности относят [2]**:**

- соблюдение и защита прав и свобод человека и гражданина;
- законность;
- системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
- приоритет предупредительных мер в целях обеспечения безопасности;
- взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Согласно «Стратегии национальной безопасности Российской Федерации до 2020 года» от 12 мая 2009 г., основные характеристики состояния национальной безопасности предназначаются для оценки состояния национальной безопасности и включают [3]:

- уровень безработицы (доля от экономически активного населения);
- децильный коэффициент (соотношение доходов 10% наиболее и 10% наименее обеспеченного населения);
- уровень роста потребительских цен;
- уровень государственного внешнего и внутреннего долга в процентном отношении от валового внутреннего продукта;

- уровень обеспеченности ресурсами здравоохранения, культуры, образования и науки в процентном отношении от валового внутреннего продукта;

- уровень ежегодного обновления вооружения, военной и специальной техники;

- уровень обеспеченности военными и инженерно-техническими кадрами.

Устойчивое развитие (sustainable development) — процесс изменений, в котором эксплуатация природных ресурсов, направление инвестиций, ориентация научно-технического развития, развитие личности и институциональные изменения согласованы друг с другом и укрепляют нынешний и будущий потенциал для удовлетворения человеческих потребностей и устремлений [4].

Устойчивое развитие цивилизации планеты предполагает наличие единой и определенной системы ценностей и установок, на которую смогли бы ориентироваться государства при формировании своих национальных стратегий. В декларации, утвержденной на Конференции ООН по окружающей среде и развитию в Рио-де-Жанейро в 1992 г., были сформулированы 27 принципов устойчивого развития, представляющие собой содержательную составляющую нового механизма глобального партнерства, заключения международных соглашений, обеспечивающих уважение интересов всех и защиту целостности глобальной системы охраны окружающей среды и развитию. Важнейшими являются принципы [5]:

– обеспечения права людей на здоровую и плодотворную жизнь в гармонии с природой; удовлетворения потребностей нынешнего и будущих поколений; сохранения окружающей природной среды как неотъемлемой составляющей права на развитие;

– неотъемлемого суверенитета государств над собственными природными ресурсами при соблюдении принципа непричинения ущерба окружающей среде за пределами национальной юрисдикции;

– рассмотрения экологических вопросов при участии всех заинтересованных граждан и обеспечения каждому человеку доступа к информации, касающейся окружающей среды, широкого предоставления такой информации населению; принятия эффективных законодательных актов в области охраны окружающей среды и национальных законов, касающихся ответственности за ущерб, причиненный экологически вредной деятельностью;

– международного природоохранного сотрудничества в контексте устойчивого развития, направленного на: искоренение бедности; признания общих обязанностей и ответственности в сфере охраны окружающей среды; наращивания научного потенциала; создания благоприятной и открытой международной экономической системы; противодействия или воспрепятствования перемещению и передаче экологически опасных и вредных веществ и др.

Эти принципы заложили основу для обеспечения мировым сообществом и отдельными государствами устойчивого развития правовыми и другими средствами.

В Российской Федерации основы устойчивого развития изложены и утверждены Указом Президента РФ № 440 от 1 апреля 1996 г. В России предполагалась разработка системы программных и прогнозных документов: государственной стратегии действий долгосрочного характера; долгосрочных и среднесрочных прогнозов, включающих в качестве составного компонента прогнозы изменений окружающей среды и отдельных экосистем в результате хозяйственной деятельности; краткосрочных прогнозов и программ отраслевого, регионального (территориального) и федерального уровней. Комиссией по проблемам устойчивого развития Государственной думы Федерального Собрания Российской Федерации были разработаны Основные положения стратегии устойчивого развития России, в соответствии с которой необходимо [6]:

– создание правовой основы перехода к устойчивому развитию, включая совершенствование действующего законодательства, определяющего, в частности, экономические механизмы регулирования природопользования и охраны окружающей среды;

– разработка системы стимулирования хозяйственной деятельности и установление пределов ответственности за ее экологические результаты, при которых биосфера воспринимается уже не только как поставщик ресурсов, а как фундамент жизни, сохранение которого должно быть непременным условием функционирования социально-экономической системы и ее отдельных элементов;

– оценка хозяйственной емкости локальных и региональных экосистем страны, определение допустимого на них антропогенного воздействия;

– формирование эффективной системы пропаганды идей устойчивого развития и создание соответствующей системы воспитания и обучения.

Следует констатировать, что устойчивое развитие на международном или национальном уровне невозможно без целенаправленной системы действий на местном уровне, поэтому регионы являются главными участниками процесса устойчивого развития, т.к. они вступают во взаимодействие между государством, ассоциациями, предприятиями и гражданами, и тем самым претворяют крупные международные соглашения в конкретные мероприятия на местном уровне.

Таким образом, целью устойчивого развития является процесс изменений, в котором эффективное использование имеющихся ресурсов, направление инвестиций, структурная перестройка осуществляются в гармонии, способствуют повышению текущего и будущего потенциала. Следует подчеркнуть важность обеспечения общего вектора развития системы, сопровождающегося ростом возможностей удовлетворения потребностей нынешнего и будущих поколений в длительной перспективе при сохранении баланса интересов, гармонии между всеми элементами социально-экономической системы.

Рассмотрение устойчивого развития в аспекте проблемы безопасности означает не только новое видение механизмов и перспектив ее обеспечения, но фактически — переход к более широкому и адекватному пониманию такого развития, которое в этом случае представляет собой нерегрессивный тип эволюции, элиминирующий (либо снижающий до приемлемого уровня) любые негативные воздействия на объект с целью его сохранения. В целом, устойчивое развитие в широком смысле представляет собой наиболее безопасное развитие, в которое входит ставшее достаточно распространенным его «экологическое» понимание как обеспечение экологической безопасности в глобальном масштабе.

В связи с принятием в 2009 г. Стратегии национальной безопасности РФ до 2020 года можно констатировать новое видение проблем устойчивого развития: «Стратегия исходит из фундаментального положения о взаимосвязи и взаимозависимости устойчивого развития государства и обеспечения национальной безопасности» [7].

Нужно иметь в виду, что понятие устойчивого развития, которое ставит целью выживание человечества и сохранение биосферы, имеет системно-комплексный характер. Отсутствие существенных позитивных результатов в экологической области реально компенсируется другими прогрессивными тенденциями и эффектами на пути к устойчивости. К достижениям в этих областях в рассматриваемой Стратегии относятся многие позитивные политические, социально-экономические преобразования и реформы: укрепление государственности, усиление институтов гражданского общества, переход национального законодательства на качественно новый уровень, особенно в сфере защиты конституционных прав человека, укрепление национальной обороны, а также общественной и государственной безопасности, устранение ряда угроз экологической и информационной безопасности, создание возможностей более быстрого развития высокотехнологичных отраслей экономики и появление реальных условий перехода на инновационные механизмы развития и другие важные результаты.

Вместе с тем, особенно в условиях современного мирового финансово-экономического кризиса, появились негативные тенденции, которые можно квалифицировать как опасности и угрозы дальнейшего системного продвижения по пути устойчивого развития России. Эти негативные тенденции проявляются, прежде всего, в социально-экономической сфере. Подтверждением происходящих процессов являются рост безработицы и усиление инфляции.

Таблица 1-Уровень безработицы в России за 2000-2015 гг.

2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
10,6	9,0	7,9	8,2	7,8	7,1	7,1	6,0	6,2	8,3
2010		2011		2012		2013		2014	2015
7,3		6,5		5,5		5,5		5,2	5,6

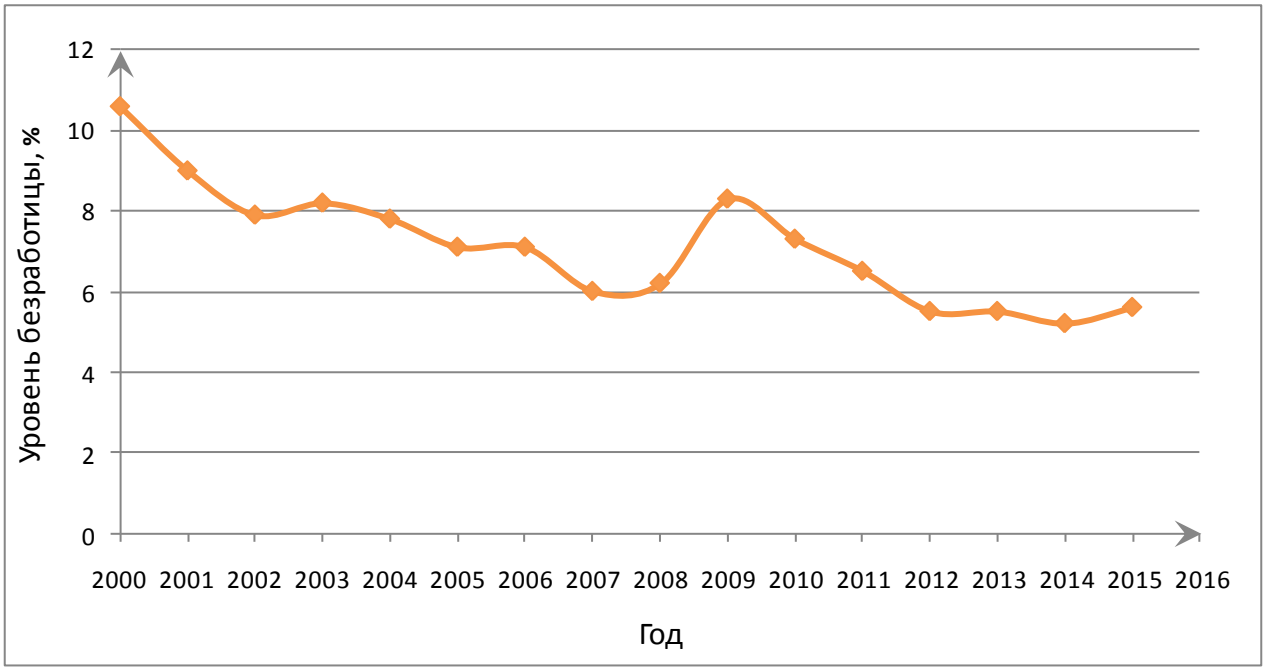
Источник: официальные данные Федеральной Службы Государственной статистики.

Таблица 2- Уровень инфляции в России за 2000-2015 гг.

2000	2001	2002	2003	2004	2005	2006	2007
20,1	18,8	15,06	11,99	11,74	10,91	9	11,87
2008	2009	2010	2011	2012	2013	2014	2015
13,28	8,8	8,78	6,1	6,58	6,45	11,36	12,91

Источник: официальные данные Федеральной Службы Государственной статистики.

Покажем в графическом виде динамику уровня безработицы за предыдущие года (рисунок 1).



- фактический уровень безработицы (по данным Федеральной службы государственной статистики)

Рисунок 1 - Динамика уровня безработицы с 2000 по 2015 год

Покажем в графическом виде динамику уровня инфляции за предыдущие годы (рисунок 2).

Чтобы существенно уменьшить эти опасности и угрозы, в основу Стратегии 2020 решено положить фундаментальное методологическое положение о взаимосвязи и взаимозависимости устойчивого развития государства (и общества) с обеспечением национальной безопасности (статьи 2 и 3 Стратегии национальной безопасности Российской Федерации).

Новый подход к обеспечению безопасности, используемый в модели устойчивого развития, предполагает системное видение проблемы, когда в одно целое с обеспечением безопасности соединяются экономические, экологические, политические, социальные и прочие аспекты и направления развития, т.е. создается новая целостная система деятельности [8].

Обеспечение безопасности через переход к устойчивому развитию характеризуется рядом новых приоритетов. Так, в России в «Стратегии национальной безопасности Российской Федерации до 2020 года» выделяются с позиций обеспечения национальной безопасности следующие приоритеты устойчивого развития:

– повышение качества жизни российских граждан путем гарантирования личной безопасности, а также высоких стандартов жизнеобеспечения;

– экономический рост, который достигается прежде всего путем развития национальной инновационной системы и инвестиций в человеческий капитал;

– наука, технологии, образование, здравоохранение и культура, которые развиваются путем укрепления роли государства и совершенствования государственно-частного партнерства;

– экология живых систем и рациональное природопользование, поддержание которых достигается за счет сбалансированного потребления, развития прогрессивных технологий и целесообразного воспроизводства природно-ресурсного потенциала страны;

– стратегическая стабильность и равноправное стратегическое партнерство, которые укрепляются на основе активного участия России в развитии многополярной модели мироустройства.

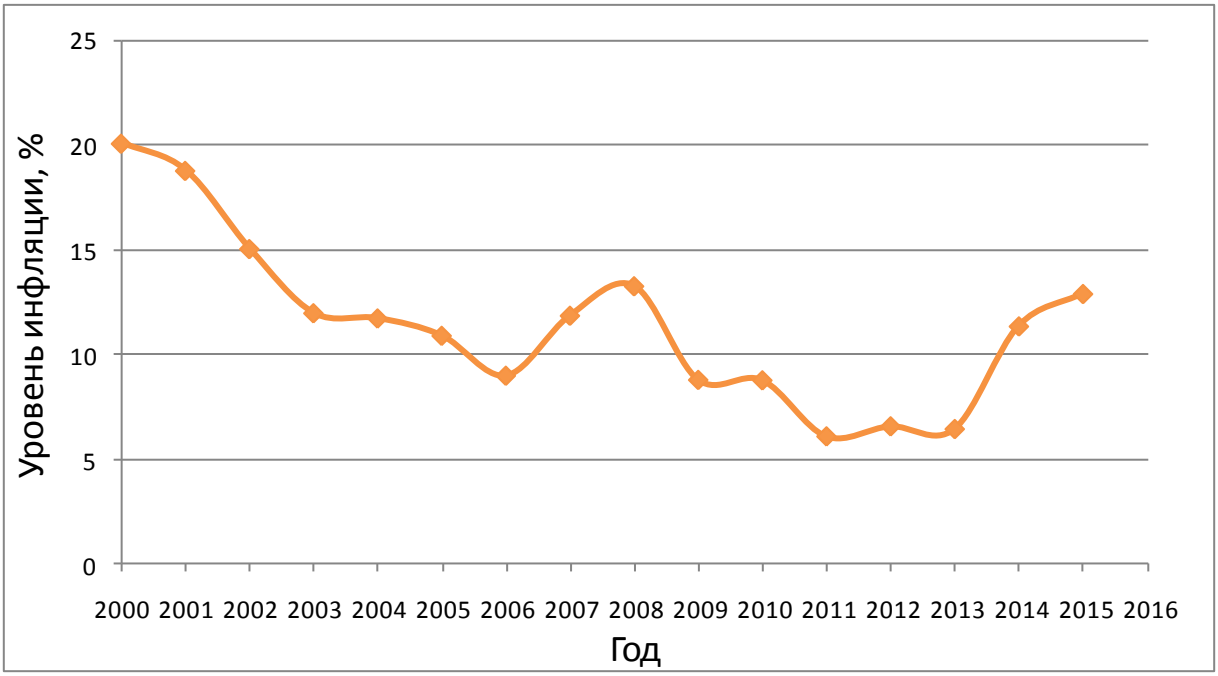


Рисунок 2 - Динамика уровня инфляции за 2000-2015 гг.

Таким образом, обеспечение безопасности преследует цель сохранения объекта (прежде всего личности, общества и государства), а устойчивое развитие – его дальнейшее, но уже безопасное прогрессивно-поступательное развитие. Их объединение превращает развитие в безопасное, а безопасность, в свою очередь, обеспечивается через устойчивое развитие. В результате реализации такой модели опасности и угрозы достигнут минимального уровня, и не будут препятствовать продолжению прогрессивного развития общества и его коэволюционного взаимодействия с природой.

Библиографический список

1. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 05.10.2015) «О безопасности», 2010.
2. http://www.grandars.ru/student/nac-ekonomika/nacionalnaya-bezopasnost.html.
3. Указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014) « О Стратегии национальной безопасности Российской Федерации до 2020 года».
4. http://regreenhub.ru/принципы-устойчивого-развития/
5. Рио-де-Жанейрская декларация по окружающей среде и развитию. Принята Конференцией ООН по окружающей среде и развитию, Рио-де-Жанейро,3-14 июня 1992.
6. Дедегкаева, С.М. Анализ динамики объема государственного внутреннего и внешнего долга на период 2009-2015 гг. 2015.
7. Урсул, А.Д. Экологическая безопасность и устойчивое развитие // Государственное управление ресурсами. Специальный выпуск. №4. 11.3.2012
8. Урсул, А.Д.- Обеспечение национальной безопасности через приоритеты устойчивого развития. Сетевое издание «Вопросы безопасности» Издательство: ООО <НБ-Медиа>2013 г. 61 с.

НЕДОИМКИ ПО НАЛОГАМ И СБОРАМ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Ворушило Б.А., Уружбеков Р.Н., студенты
Научный руководитель: к.э.н., доцент О.В. Голикова
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Взимание налогов и сборов – это одно из основных условий существования государства, развития общества, экономического и социального процветания. Ни одно государство не может обходиться без налогов, так как для обеспечения государства и общества требуется определенная сумма денежных средств. Налоги составляют свыше 70% государственного бюджета.

С каждым годом экономическое состояние в стране изменяется не в лучшую сторону. Экономический кризис, безработица, низкая заработная плата. Все это приводит к тому, что организации и физические лица уклоняются от уплаты налогов и сборов и государственный бюджет, в свою очередь, теряет основную часть своих доходов. Такая ситуация оказывает негативное воздействие на экономическую безопасность страны.

Особо актуальной и трудноразрешимой проблемой в России является организация эффективного налогового контроля в России. Налоговый контроль является важным средством защиты имущественных интересов, как частных собственников, так и государства. Эффективность работы налоговых органов, которые обеспечивают формирование доходов государственного бюджета, является важным условием правильного функционирования всей системы налогового контроля.

Актуальность темы исследования состоит в том, что в настоящее время существует устойчивая проблема непоступления налоговых платежей в бюджет и внебюджетные фонды, следствием чего является недополучение бюджета страны финансовых средств и образование недоимки.

Экономическая безопасность - это состояние экономики государства, которое характеризуется наличием стабильного дохода и других ресурсов, при котором осуществляется защита национальных интересов, устойчивость к внутренним и внешним угрозам.

Налогообложение является связующим звеном между экономикой и бюджетной системой, которая осуществляет перераспределение средств между хозяйствующими субъектами, физическими лицами и государством. Система налоговых органов в условиях рыночной экономики остается одним из механизмов регулирования социально-экономических процессов, которыми обладает исполнительная и законодательная власть, так как налоги являются основными источниками доходов, которые требуются государству для выполнения законодательно закрепленных за ним функций. Поэтому налоговая безопасность является важным элементом экономической безопасности страны в современных условиях.

Налоговая безопасность государства – это состояние экономики, при котором обеспечивается гарантированное поступление налоговых платежей в государственный бюджет. Она осуществляет защиту национальных интересов, достаточный потенциал при неблагоприятных условиях развития внутренних и внешних процессов, социальную направленность налоговой политики. Обеспечение экономической безопасности в налоговой сфере зависит от многих факторов, и, в основном, от налоговой политики государства, которая формирует налоговую систему.

Механизм обеспечения экономической безопасности в налоговой сфере - это набор законодательно-нормативных актов и наличие институциональных структур, которые своевременно предупреждают о возникновении угроз экономической безопасности в налоговой сфере, снижают уровень их воздействия или полностью ликвидируют возможность их возникновения. Этот механизм должен иметь инструменты устранения коррупции при налоговом администрировании.

Основной источник, который создает угрозу налоговой безопасности, это действия хозяйствующих субъектов и населения по уклонению от уплаты налогов. Уклонение от уплаты налогов подразумевает под собой уменьшение налоговых платежей, путем умышленного уклонения от уплаты налогов, сокращения их выплат, как правило, способами, которые противоречат законодательству.

Умышленным считается уклонение, при котором лицо осознанно совершило деяние, которое повлекло за собой негативные последствия.

Причины уклонения от уплаты налога могут быть разными. Они могут включать: экономические, политические, правовые, организационные и другие причины. В академической среде особое внимание сосредотачивается на определенном ряде причин. Так уклонение от уплаты налогов связано с:

ухудшением финансового положения бизнеса:

общим снижением доходов населения;

наличием спорных моментов и недоработок в налоговом законодательстве и налоговой политике;

отсутствием стимулирующих условий для обеспечения конкурентоспособности.

Классификация способов уклонения от уплаты налогов отражена на рисунке 1.

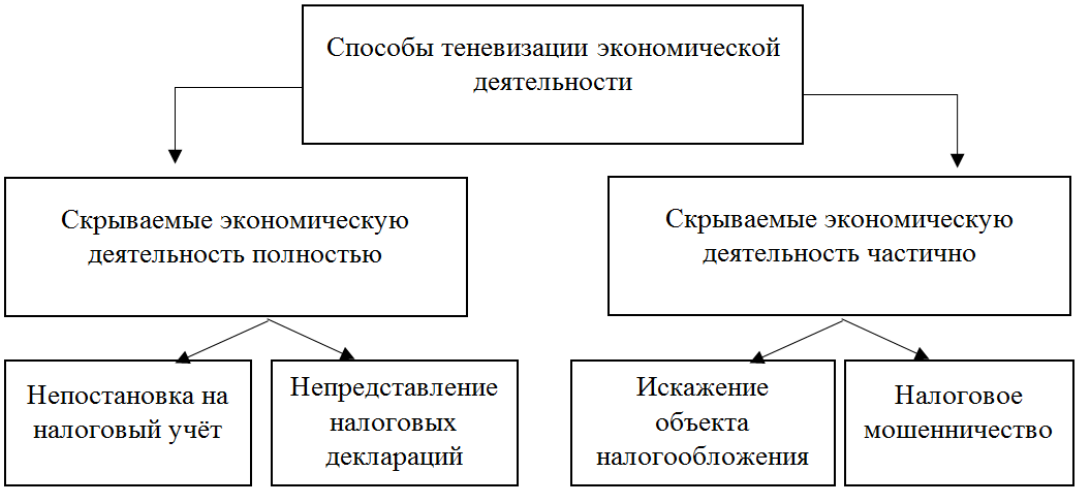


Рисунок 1 - Классификация способов уклонения от уплаты налогов

Таким образом, существует необходимость комплексного подхода к решению проблем, которые связаны с уклонением от уплаты налоговых платежей. Первоначально это связано с совершенствованием деятельности органов налоговой службы.

Недоимка является суммой налога или сбора, не уплаченной в установленный налоговым законодательством срок, поэтому также представляет угрозу для экономической безопасности. Непоступление налогов в бюджет ведет к недополучению государства своих доходов. А определение экономической безопасности характеризует состояние экономики государства наличием стабильного дохода.

Существует много способов, которые используют для уклонения от уплаты налогов. Они разнообразны, но их можно объединить в следующие группы:

1. полное или частичное искажение результатов финансово-хозяйственной деятельности предприятия в документах бухгалтерского учета;
2. использование операций с наличностью, которая не фиксируется в бухгалтерских документах;
3. необоснованное отнесение на издержки производства затрат;
4. искажение экономических показателей;
5. занижение объема или стоимости реализованных товаров, работ, услуг;
6. способы, которые основаны на маскировке объекта налогообложения (подмена объекта налогообложения);
7. осуществление операций с фирмами-однодневками или посредническими аффилированными лицами (лицами, способными оказывать влияние на деятельность юридических или физических лиц, осуществляющих предпринимательскую деятельность)

Таким образом, существует необходимость комплексного подхода к решению проблем, которые связаны с уклонением от уплаты налоговых платежей. Первоначально это связано с совершенствованием деятельности налоговых органов.

Внешний аспект роли налоговых органов в обеспечении экономической безопасности предполагает выявление и устранение угроз в налоговой сфере, а внутренний – подразумевает ликвидацию недостатков в самой системе налоговых органов.

Отсутствие единого массива данных о плательщиках налогов представляет собой одну из основных проблем, препятствующих эффективной деятельности налоговых органов и противодействующих налоговым правонарушениям. Поэтому в настоящее время существует необходимость формирования систем мониторинга соблюдения налогового законодательства. Формирование системы мониторинга налоговой безопасности требует наличия развитой системы, которая будет обеспечивать сбор и накопление информации, а также анализ и обработку данных, принятие и реализацию управленческих решений, и контроль их исполнения. Но такие системы требуют решения технических проблем (например, таких как обеспечение защиты каналов связи) и проблем подбора квалифицированных кадров.

Важной мерой, необходимой для повышения уровня собираемости налогов и сборов, является усиление налоговой дисциплины. Санкции за совершение налоговых правонарушений должны быть достаточно жесткими, но соизмеримыми с допущенными правонарушениями.

ЗАРУБЕЖНЫЙ ОПЫТ В ОБЛАСТИ ПЕРЕРАБОТКИ ОТХОДОВ

Горшкова Ю.В., студент
Научный руководитель: д.э.н., профессор А.Я. Щукина
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Основные для мирового сообщества пути управления отходами были определены на Международной конференции по устойчивому развитию в Йоханнесбурге (ЮАР) в 2002 году. Они включают предотвращение образования отходов, максимальное повторное использование и вторичную переработку, а также применение альтернативных экологически безопасных материалов[4].

Европа в силу своей четко отлаженной системы сбора и сортировки отходов с легкостью может использовать отходы в качестве сырья для строительного материала, а так же другого вторсырья. К примеру, большое внимание уделяется утилизации полимеров - одному из основных компонентов отходов потребления, которые имеют огромное количество разновидностей.

Рассмотрим ряд стран, в которых действует система рециклинга.

Каждый житель Швейцарии обязан сортировать мусор – это закон. Нарушителям – крупный штраф. За соблюдением закона следит мусорная полиция, которая способна найти и привлечь к суду даже человека, выбросившего из окна машины окурок. Тот же, кто не желает «пачкать руки», должен заплатить налог, чтобы его отходами занялся "специалист".

Еще одна прямая обязанность каждого законопослушного швейцарца – привезти рассортированный мусор на пункты приемки, откуда его направляют на перерабатывающие предприятия.

Система сортировки мусора в Швейцарии доведена практически до самого высокого уровня необходимости дифференциации отходов. В стране на перерабатывающие заводы попадает более 90% использованной стеклотары [1].

На улицах Женевы расставлены металлические контейнеры для битых и нестандартных бутылок, причем стекло сортируется по цвету: белое, зеленое, коричневое, для этого на контейнерах имеются соответствующие надписи.

Почти треть печатной продукции тоже возвращается в пункты приема вторсырья. Батарейки, содержащие опасные для живых организмов реагенты, никогда не выбрасываются в мусорное ведро, как и старые электрические приборы,

домашняя техника, строительный мусор. Например, для отработанных батареек вокруг крупных магазинов и школ ставят "скворечники" – небольшие ящики.

Отдельно собираются PET (пластиковые), лампы дневного света, пенопласт (их жители обязаны спрессовать с помощью домашнего магнитного пресса) [1].

В Германии также действует система раздельного сбора мусора. Для каждого вида отходов имеется своя секция. Секции должны стоять далеко от домов, но не далее 15 км от жилой части, чтобы облегчить работу мусорщикам.

В серую секцию несут только остаточный мусор, старые бытовые отходы. В желтую секцию выбрасывают банки, бутылки, полимерную и бумажную, а также частично металлическую упаковку, на которой стоит "зеленая точка". Зеленая бочка предназначена для органических отходов, которые перерабатываются в компост.

Лишнюю стеклянную тару, которая по каким-либо причинам не попала в желтую бочку для упаковок, нужно складывать в большие контейнеры, также расположенные в нескольких точках каждого района. Зеленые, белые и коричневые бутылки сортируются на месте. Лекарства с просроченной датой принимают аптеки. Для старых батареек есть приемные пункты в любом супермаркете. О вывозе холодильников нужно договариваться заранее. Мусор, собранный в городе, в зависимости от расстояния между местом сбора и полигоном, доставляется или непосредственно на полигон, или в центр по сортировке, или на мусороперегрузочную станцию [3]. Здесь посредством мусороприемника на несколько десятков тонн со встроенным гидравлическим прессом осуществляется перегрузка отходов в большие (грузоподъемностью 24-40 т) автоконтейнеры. Таким образом, сокращаются транспортные расходы.

В центрах по сортировке собранные упаковочные материалы сортируются вручную. Различные виды бытовых отходов перерабатываются стекольной промышленностью; обществом по утилизации бумаги; обществом по утилизации использованной упаковки из искусственных материалов, полимерных пленок, банок, бутылок, пенопласта; металлургической промышленностью; обществом по утилизации упаковки из алюминия и др [2].

Система раздельного сбора мусора действует и в Швеции. Семья, живущая в отдельном доме, платит половину стоимости вывоза отходов, если подписывает обязательство сортировать пластик, жесть, стекло и бумагу, а также компостировать органические остатки. Вредные отходы выносятся в специальном красном контейнере непосредственно перед сбором мусора.

В многоквартирных домах сбор мусора происходит так: в мусорные контейнеры выкидывается все, кроме того, что положено нести в специальные емкости для жести, пластмассы и т.п. Вредные отходы относятся на специальные экологические станции, которые могут располагаться, например, на бензоколонке.

На станции размещают контейнеры зеленого и красного цвета для аккумуляторов и батареек, светло-голубого цвета – для фотохимикатов, остатков краски, аэрозольных баллончиков, использованного машинного масла, растворителей и люминисцентных ламп.

Старые газеты забираются раз в неделю, их собирают в пакеты и выставляют за дверь. В ряде мест располагаются специальные "газетосборники". Алюминиевые банки возвращаются в супермаркеты, за них там выплачивается залоговая стоимость. Прозрачное и зеленое стекло выбрасывается в специальные контейнеры белого и зеленого цвета [2].

Швеция настолько мощно занялась развитием собственной инфраструктуры по переработке различного рода отходов, что в данный момент просто не может обеспечить полноценную производственную мощность своих предприятий посредством снабжения их собственными мусорными отходами. В такой ситуации эта страна вынуждена заниматься импортом чужого мусора. Множество европейских стран, таких как: Норвегия, Великобритания, Италия и Ирландия поставляют в Швецию свои отходы.

На данный момент тридцать два шведских завода работает по системе «отходы в энергию», или же WTE (waste to energy). Само по себе это понятие подразумевает самую настоящую переработку различных видов мусора в электроэнергию. Постройка всех этих тридцати двух заводов производилась практически в одно и тоже время, а именно за считанные годы. Вся политика шведской науки и промышленности направлена на предотвращение образования отходов.

При создании новых производств и реконструкции действующих предприятий серьезное значение имеет охрана окружающей среды и создание замкнутых энерготехнологических процессов. В Швеции используются различные приемы переработки отходов для комплексного решения вопросов создания безотходных или малоотходных производств. Такой подход предполагает комплексную переработку сырьевых ресурсов и анализ производства как большой системы. Комплексная переработка сырья определяется спецификой сырьевых ресурсов, возможностью целенаправленной их переработки и создания по существу замкнутых технологических циклов с использованием вторичных материальных ресурсов.

Производство рассматривается как большая система, которая разделяется на подсистемы вплоть до рассмотрения с системных позиций отдельных типовых процессов технологии. При рассмотрении отдельных типовых процессов в аспекте создания безотходных производств, определяющим параметром является время завершения процесса, необходимое для достижения заданных характеристик. С этой точки зрения по-новому ставится вопрос о расчете процессов используемой технологии и необходимости учета реального времени пребывания обрабатываемых веществ в аппарате [5].

Существенное влияние на организацию безотходных производств оказывает распределение нагрузок между аппаратами. Одновременно используются возможности отдельных процессов для обезвреживания газовых выбросов, сточных вод и твердых отходов.

Оптимизация технологических схем и производств в целом открывает пути создания замкнутых по материальным и энергетическим потокам технологических схем, исключающих вредные выбросы в окружающую среду и приводящих к экономии энергии .

В этой связи, в самой Швеции «производится» совсем мало мусора, несколько сотен килограмм в год, эти цифры абсолютно ничтожны. Но в этой ситуации всего половина данного материала идет на выработку электричества. Остаток используется на производство полезных в хозяйстве вещей. В Швеции очень активно развита позиция борьбы с различными, загрязняющими окружающую среду, веществами.

Вся суть заключается в том, что отходы проходят предварительную отсортировку, прежде чем попасть на завод. Ответственность за такой вид деятельности несут рядовые шведы и лица, представляющие различные бизнес – организации. В Швеции работает система очень жестких штрафов за не соблюдение правил работы с отходами. Это подразумевает то, что производитель и ретейлер товара и

услуги отвечает за то, как будет производиться утилизация тары после использования ее потребителем.

Обратный прием этого материала, является нормой во всех магазинах и барах по всей стране. Законодательная база Швеции заставляет производителей заниматься сбором употребленной тары, произведенной именно этой торговой маркой, у населения. В задачу обывателя входит доставка пришедшего в негодность или уже примененного по назначению товара до специализированного пункта приема. Сдача мусора происходит за счет его владельца. Положительные результаты не достигаются за относительно короткий промежуток времени [6].

В данный период в Англии строится первое здание, полностью состоящее из переработанных отходов (рис. 1). Его разработал архитектор Дункан Бейкер-Браун, который придумал использовать в качестве строительных материалов производственный мусор заводов или больших строек.

Рисунок 1 - Первое здание из переработанных отходов

В Шотландии недавно построили "мусорный" мост. На создание 90-футового моста ушло более 50 тонн пластиковых отходов (рис. 2). Он достаточно прочен, чтобы выдержать даже тяжелые транспортные средства. Стоит заметить, что впоследствии, при необходимости, этот мост может быть полностью переработан.

Рисунок 2 - «Мусорный» мост в Шотландии

За рубежом люди мотивированы на правильный сбор строительного мусора - для этого существуют различные государственные программы, а также предусмотрена система штрафов для той части населения, которая пренебрегает общепринятыми правилами.

Российская практика утилизации, переработки и применения отходов, к сожалению, довольно сильно отличается от европейской. Не в последнюю очередь потому, что у нас о раздельном сборе мусора и его сортировке думают единицы. По статистике, в странах Евросоюза перерабатывается до

60% отходов, в России же эта цифра составляет всего 4-5% [3]. Даже несмотря на то, что переработка мусора не только забота об экологии, но и выгодный бизнес.

Постоянное увеличение отходов во всех сферах жизнедеятельности предъявляет особенные требования к формированию систем применения вторичных ресурсов на государственном и региональном уровнях. Производство вторичных ресурсов способно не только уменьшить количество мусора в стране, но также повысить экономическую эффективность промышленных предприятий.

Таким образом, стабильное экономическое и экологическое развитие зарубежных стран является формированием и практическим внедрением технологий, близких к биологическим циклам природы. Подобные технологические процессы качественно и эффективно должны перерабатывать первичные ограниченные ресурсы, при этом, уменьшая их поток в цикл производства, за счет многократного повторного использования, то есть - рециклинга. Мировое хозяйство и, в первую очередь, российское должно заимствовать опыт ЕС обращения с отходами, поскольку его система утилизации, переработки и использования отходов практически находится на нулевом уровне.

Библиографический список

1. Ринкевичюс, С. Утилизация отходов в РФ [Электронный ресурс], -http://www.russian council.ru - статья в интернете.

2. Гурбанов, И. Проблемы обращения с отходами производства и потребления. Пути их решения [Электронный ресурс] / И. Гурбанов. – Режим доступа: http://www.rosaro.ru/docs/AWR.pdf .

3. Замятина, М.Ф. Отходы производства и потребления как экологическая, социальная и экономическая региональная проблема / М.Ф. Замятина, Р.С. Фесенко // Гуманитарное образование: креативность и инновационные процессы: материалы международной научно - практической конференции / ред. И сост. И.П. Вишнякова - Вишневецкая. – СПб.: СПбИГО, ООО « Книжный дом», 2015. - 240 с.

4. Государственный доклад «О состоянии и об охране окружающей среды Российской Федерации в 2013 году». – М., 2014.

5. Хомич, В.А. Экология городской среды / В.А. Хомич: уч. пособие. – М.: Издательство Ассоциации строительных вузов, 2014 – 240 с. (С. 180)

6. Аргументы и факты: Как работает полигон по утилизации бытовых отходов. — М., 2014.

ПРОБЛЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ МАЛЫХ ПРЕДПРИЯТИЙ В ОБЛАСТИ ФИНАНСОВОГО УЧЁТА И НАЛОГООБЛОЖЕНИЯ НА ПРИМЕРЕ ООО «УГЛЕРОД»

Данилина М.С., студент
Научный руководитель: к.э.н., доцент Ю.Н. Богдашкин
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Актуальность данной темы обусловлена тем, что деятельность малых предприятий подвержена различным рискам, ставящим под угрозу их экономическую безопасность.

Значительная часть проблем малых предприятий возникает в области ведения учёта и налогообложения. Ресурсов малого предприятия недостаточно для организации полноценного бухгалтерского и налогового учёта, подготовки полного комплекта бухгалтерской финансовой отчётности.

Для поддержки малых предприятий государство разрабатывает программы поддержки, в том числе упрощённые системы учёта, отчётности и налогообложения

Целью данной работы является изучение теоретических и практических вопросов экономической безопасности малых предприятий в области финансового учёта и налогообложения на примере предприятия ООО «Углерод».

Задачи исследования:

- рассмотреть теоретические основы обеспечения экономической безопасности малых предприятий в области финансового учёта и налогообложения;

- изучить организацию бухгалтерского учёта малого предприятия и её влияние на экономическую безопасность ООО «Углерод»;

- выявить угрозы и риски экономической безопасности в области налогообложения ООО «Углерод»;

- разработать рекомендации по совершенствованию организации учёта и оптимизации налогообложения на предприятии.

Критерии субъектов малого предпринимательства приведены в статье 4 Федерального закона от 24.07.07 № 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации». Основные критерии – это доход, который не должен превышать предельные значения, установленные Правительством Российской Федерации, 800 млн. руб. и численность персонала, которая не должна превышать 100 человек.

Главным преимуществом малых предприятий в условиях современной экономики, является более быстрая реакция на постоянно меняющийся спрос: умение понять формирующуюся потребность, мобилизовать свои ресурсы и предложить на рынке товар, удовлетворяющий потребности клиента.

Недостатки малых предприятий являются продолжением их достоинств и приводят к возникновению следующих рисков (угроз экономической безопасности): неполнота информации для принятия решений из-за нерегулярности ведения бухгалтерских записей; большая вероятность преднамеренных и непреднамеренных ошибок в учёте за счёт человеческого фактора; формальное и (или) неправильное проведение контрольных процедур, в первую очередь инвентаризаций; повышенный риск искажения отчётности; высокая вероятность хищений из-за широкого использования наличных денег в расчётах с партнёрами; значительная вероятность начисления крупных штрафов и пеней за неверные расчёты налогов и использование нелегальных налоговых схем; высокая вероятность существенных потерь в результате ошибок при проведении экономических расчётов и принятии управленческих решений; высокая вероятность банкротства из-за неблагоприятной внешней конъюнктуры, утраты ключевого персонала, рынков сбыта или ресурсов.

Как и на любом предприятии, целью бухгалтерского учёта малого предприятия является формирование документированной систематизированной информации о хозяйственной деятельности и составление на её основе бухгалтерской отчётности, содержащей информацию необходимую внутренним и внешним пользователям для принятия экономических решений.

Для достижения этой цели используются традиционные бухгалтерские методы: документирование и инвентаризация, оценка и калькулирование, счета и двойная запись, баланс и отчётность. В тоже время, субъекты малого предпринимательства вправе применять упрощённые способы ведения бухгалтерского учёта, включая ведение упрощённой бухгалтерской (финансовой) отчётности.

Рассмотрим основные льготы (особенности), предоставленные субъектам малого предпринимательства в области бухгалтерского учёта: микропредприятиям вправе вести учёт по простой схеме без применения двойной записи; сокращённый план счетов; ведение учёта без применения регистров бухгалтерского учёта; использование кассового метода учёта доходов и расходов; право не исполнять некоторые требования ПБУ, обязательные для крупных предприятий; право составлять отчётность по упрощённой системе; возможность передать ведение бухучёта на аутсорсинг.

В области налогообложения малые предприятия имеют возможность использовать специальные налоговые режимы, такие как: упрощённая система налогообложения (УСН); единый налог на вменённый доход (ЕНВД); единый сельскохозяйственный налог (ЕСХН); патентная система налогообложения (ПСН).

Объектом исследования является ООО «Углерод». Основным видом деятельности является: "Изготовление и монтаж металлоконструкций". Организация также осуществляет деятельность по следующим неосновным направлениям: "Производство крепёжных изделий и пружин", "Оптовая торговля скобяными изделиями, ручными инструментами, водопроводным и отопительным оборудованием", «Оказание услуг строительных машин и механизмов». Бухгалтерский учёт ООО «Углерод» ведётся автоматизированным способом в программе 1С.

Анализ основных технико-экономических показателей предприятия показывает что предприятие работает нестабильно. В разные годы наблюдаются значительные колебания выручки, себестоимости продаж.

Из-за высокого уровня управленческих расходов и отрицательного сальдо прочих доходов и расходов предприятие получило убыток от продаж в 2015 году и убыток до налогообложения и чистый убыток в течение 2013 – 2015 г.г. Причём величина убытка имеет тенденцию к увеличению.

В качестве негативной тенденции можно выделить постоянное сокращение величины собственного капитала. Причиной такого снижения является неэффективная деятельность и непокрытые убытки в течение всего рассматриваемого периода. Из-за этого предприятие нуждается в привлечении заёмных средств для финансирования своей деятельности на прежнем уровне.

Предприятие формирует следующие формы бухгалтерской отчётности: бухгалтерский баланс, отчёт о финансовых результатах, отчёт об изменениях капитала, отчёт о движении денежных средств, пояснения к бухгалтерскому балансу и отчёту о финансовых результатах.

В качестве рекомендаций по совершенствованию организации бухгалтерского учёта ООО «Углерод» предложено использовать бухгалтерский аутсорсинг, что позволит сократить затраты на ведение учёта, представленные в таблице 1.

Стоимость бухгалтерского сопровождения в аутсорсинговой компании для предприятия размером с ООО «Углерод» составляет около 8000 рублей в месяц или 24000 ежеквартально, что значительно ниже текущих затрат на ведение учёта в ООО «Углерод». Экономический эффект от изменения организации бухгалтерской службы составит 264000 рублей в год что позволит предприятию сократить управленческие расходы и уменьшить убыток от продаж.

Кроме того, для сокращения затрат на бухгалтерское обслуживание рекомендуем перейти на упрощённые системы учёта и отчётности, разрешённые для субъектов малого бизнеса. Ведение упрощённого учёта и отчётности в аутсорсинговой компании стоит в несколько раз дешевле. Обычно не более 10000 рублей за квартал, что ещё больше снизит операционные издержки.

ООО «Углерод» начислялись и уплачивались в 2015 году следующие налоги: налог на добавленную стоимость; налог на прибыль; налог на имущество; налог на землю; транспортный налог; плата за негативное воздействие на окружающую среду; НДФЛ (налоговый агент); страховые взносы в государственные внебюджетные фонды. Величина налоговой нагрузки ООО «Углерод» составила 1395404 рубля.

Для оптимизации налоговой нагрузки необходимо осуществить переход с общей на упрощённую систему налогообложения. В результате такого перехода предприятие сможет не уплачивать НДС, налог на прибыль, налог на имущество, а также существенно сократит величину платежей в государственные внебюджетные фонды.

Таблица 1 – Затраты на содержание бухгалтерской службы ООО «Углерод»

Наименование затрат	Ориентировочная стоимость, руб	Затраты времени
1. Создание рабочего места для бухгалтера: письменный стол, стул, шкаф, вентилятор и/или обогреватель канцелярские принадлежности;	10000 единоразово 1000 ежеквартально	3 часа
2. Приобретение офисной техники для бухгалтера: компьютер, принтер, копировальный аппарат, телефон, подключение телефонного номера	50000 единоразово 1500 ежеквартально	3 часа
3. Установка офисных и бухгалтерских программ, правовых баз, необходимых для работы	- Windows – от 3 000 - MS Office – от 5 000 - 1С 8.0 – от 9 000 - КонсультантПлюс – от 24 000 год	8 часов
4. Поиск бухгалтера – профессионала: поиск и мониторинг резюме, обзвон соискателей, собеседование	Невозможно оценить	Несколько дней или недель
5. Повышение квалификации бухгалтера, которое необходимо в связи с постоянно меняющимся законодательством	12000 в год	Приблизительно неделю бухгалтера нет на месте
6. Бухгалтерская пресса («Главбух», «Бухгалтерский учёт» и т.п.	4000 в квартал	2 часа в неделю
7 Оплата труда, социальные отчисления	20000 ежемесячная заработная плата 20000*30% = 6000 ежемесячные социальные отчисления	
8. Оплачиваемый отпуск	26000 средняя заработная плата плюс социальные отчисления	28 дней бухгалтера нет на месте
9. Возможные затраты на оплату пособия по временной нетрудоспособности	Средний заработок за первые 3 дня нетрудоспособности	Минимум неделя
Итого	77000 единоразово 90000 ежеквартально	1,5 – 2 месяца в год бухгалтера нет на месте

Налоговая нагрузка предприятия ООО «Углерод» с учётом оптимизационных мероприятий составит 905457 рублей, что на 489997 рублей меньше, чем налоговая нагрузка фактически сложившаяся в 2015 году

Таким образом, цель исследования достигнута, задачи решены.

«СИЛОВОЕ ДАВЛЕНИЕ» НА СРЕДНИЙ И МАЛЫЙ БИЗНЕС РОССИИ

Димакис М.А., студент
Научный руководитель: к.т.н., доцент Ильичев В.М.
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Актуальность данной темы определена в первую очередь объективно значительным силовым давлением и нагрузкой внешних и внутренних факторов на средний и малый бизнес в России. Это влияние очень плохо сказывается на существовании новых предприятий и фирм. Каждый четвертый новый вид предпринимательства сворачивается из-за силового давления. А малое и среднее предпринимательство — это существенная составляющая цивилизованного рыночного хозяйства, неотъемлемый элемент присущего ему конкурентного механизма. Поэтому государство должно обеспечивать безопасность бизнеса и всячески помогать его развитию. Так же актуальность данной проблемы подтверждает недавнее внесение законопроекта, который внес президент Российской Федерации Путин В.В., об установлении уголовной ответственности за незаконное преследование бизнеса.

Одним из ключевых вопросов, связанных с взаимодействием бизнеса и государства, является проблема применения силы со стороны власти и криминала. Важнейший институт рыночной экономики – права собственности – не может существовать без развитых механизмов защиты собственности и противодействия насилию со стороны государственных агентов или организованной преступности.

В данной статье предлагается использовать индикатором «силового давления» – количество обращений, поступающих в Центр общественных процедур «Бизнес против коррупции» (ЦОП «БПК»). Заявления от предпринимателей с жалобами на рейдерство или незаконное уголовное преследование зачастую является предварительным этапом захвата компании.

Анализ данных, представленных в таблице 1 « Категории обращений в Центр общественных процедур» [4] показывает, что с силовым давлением на бизнес предприниматели сталкиваются очень часто, притом, что нельзя с полной уверенностью утверждать, что частота обращений отражает реальную ситуацию в регионах.

Таблица 1 - Категории обращений в Центр общественных процедур

№п/п	**Категория**	**Число обращений**
1	Рейдерская атака	119
2	Уголовное преследование	278
3	Коррупция	28
4	Административные барьеры	26
5	Другое	76
	Всего	527

Источник: расчеты авторов на основе базы ЦОП за февраль 2014 – ноябрь 2015 г.

Неопределенность с достоверностью данных, представленных в Таблице 1, может объясняться тем фактом, что не все предприниматели обращаются за помощью в деловые организации: часть бизнесменов делает это более охотно, тогда как другие предпочитают решать свои проблемы самостоятельно или с использованием других механизмов, например, использования влиятельных покровителей.

Государство в курсе данной проблемы и пытается обезопасить Российских предпринимателей и бизнес в России в целом.

При разработке приоритетной программы «Реформа контрольной и надзорной деятельности» решено взять за основу следующие показатели. Качество администрирования контрольно-надзорных функций к 2024 году должно возрасти на 50%. При этом административная нагрузка на бизнес к этому сроку должна снизиться вдвое, говорится в документах правительства. К 2018 году административная нагрузка на бизнес должна быть снижена на 20 %, а к 2024 году — на 50 %. Но, на мой взгляд, увеличение контрольно-надзорных функций, это путь в некуда. Бизнесу и так приходиться не просто в нынешних условиях частого и порой не объективного контроля со стороны представителей власти.

В части административной нагрузки и давления со стороны правоохранительных органов — недавний пленум Верховного суда России принял постановление (от 15.11.16), защищающее предпринимателей от необоснованного возбуждения уголовных дел. Теперь правоохранительным органам запрещено возбуждать на предпринимателей дела по статье УК "Мошенничество" без заявления потерпевших. Так что следователи не смогут выдумывать на ровном месте обвинения для давления на бизнесмена. Введены и более строгие толкования, запрещающие арест предпринимателей по обвинениям в экономических преступлениях. Так же в Госдуме прошло первое слушание (от 16.11.16) законопроекта по ужесточению ответственности силовиков за незаконное преследование бизнеса. Дума одобрила этот президентский законопроект, который предполагает лишение свободы на срок до 10 лет. В дальнейшем в ГД хотят ввести наказание не только для не чистых на руку силовиков, но и тех, кто заказал им прессинг бизнесмена.

Данная проблема очень актуальна в настоящее время в России, так как бизнесу приходиться тяжело, кроме всемирного экономического кризиса на него давит государство и прочие факторы. На данный момент ситуация неуверенности в завтрашнем дне, к сожалению, нивелирует все усилия, которые были сделаны за многие годы по созданию всей этой инфраструктуры, которая у нас уже есть. И мы наблюдаем, как уменьшается рентабельность бизнеса, потому что большую часть времени предприниматели вынуждены тратить не на развитие своего бизнеса, а на его защиту. Мое убеждение в том, что сегодня необходимо создать условия, чтобы предприниматели занимались своим делом. Печешь булочки — пеки, соблюдая необходимые нормативные требования по безопасности своей продукции для потребителя, и не думай, как найти того, кто будет прикрывать и обеспечит защиту от необоснованных требований. У бизнеса нужно убрать чувство страха. Если его убрать, рост экономики может быть очень серьезный. Для этого бизнесу нужно гарантировать безопасность, и это, пожалуй, единственное, чем должна заниматься власть. Введение новых законопроектов и постановлений Верховного суда позволяют нам видеть позитивное движение в защите бизнеса от «силового давления», а как скажется это на развитии бизнеса в дальнейшем остается только гадать.

Библиографический список

1. Реестр обращений в ЦОП «БПК» [Электронный ресурс] URL:http://www.nocorruption.biz/category/register/ (дата обращения: 11.11.2016).

2. Волков, В. Силовое предпринимательство.- Спб.: Питер, 2002. – 282 с.

3. «Заседание экспертного совета при бизнес-омбудсмене Борисе Титове» [Электронный ресурс] //Автономная некоммерческая организация «Центр общественных процедур «Бизнес против коррупции» в Краснодарском крае» URL:http://corruption-no.ru/novosti/ - статья в интернете (дата обращения 11.11.2016 г.).

4. Нехорошев, Ю.С., Таран, Е.А. Портал «Воздействие рейдерства на модернизацию экономики России» [Электронный ресурс] URL: http://sun.tsu.ru/mminfo/ (дата обращения: 11.11.2016).

5. Статья на RBK Владислава Гордеева « Медведев поручил вдвое снизить давление на бизнес при реформе надзора» [Электронный ресурс] URL: http://www.rbc.ru/economics/- статья в интернете. (Дата обращения 11.11.2016 г.).

6. Статья на портале Российская газета Татьяны Замахиной «Госдума одобрила сроки до 10 лет за давление на бизнес» [Электронный ресурс] URL: https://rg.ru/2016/11/16/gosduma-odobrila-sroki-do-10-let-za-davlenie-na-biznes.html (Дата обращения 17.11.2016 г.).

7. Статья на портале Российская газета Владислава Куликова «Процесс бизнес-класса» Российская газета - Федеральный выпуск №7127 (259) URL: https://rg.ru/2016/11/15/v-rossii-zapretili-aresty-biznesmenov-po-ekonomicheskim-delam.html (Дата обращения 17.11.2016 г.).

ВОЗМОЖНОСТЬ И БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ВИЧ-ИНФИЦИРОВАННЫХ ТРУДОВЫХ РЕСУРСОВ В ОРГАНИЗАЦИИ

Захаров И.В., студент
Научный руководитель: к.т.н., доцент В.М. Ильичев
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

Россия по итогам 2015 года стала страной с крупнейшим процентом ВИЧ-инфицированных в мире, следует из доклада ЮНЭЙДС, структуры ООН по профилактике этого заболевания. По темпам прироста новых случаев ВИЧ наша страна опережает большинство государств мира, но российские

власти продолжают экономить на финансировании закупок лекарств и профилактике. Единственными регионами в мире, где эпидемия ВИЧ продолжает быстро распространяться, остаются Восточная Европа и Центральная Азия, говорится в свежем докладе ЮНЭЙДС. На Россию в этих регионах приходится 80% новых случаев возникновения ВИЧ в 2015 году. Доля новых случаев заболеваний ВИЧ в 2015 году в России — больше 11% от общего числа человек, живущих с ВИЧ (95,5 тыс. и 824 тыс. соответственно, по данным Федерального центра СПИД). В подавляющем большинстве африканских стран число новых случаев не превышает 8%.

Основную причину ухудшения ситуации эксперты ЮНЭЙДС видят в том, что Россия потеряла международную поддержку программ против ВИЧ и не смогла заместить ее адекватной профилактикой за счет бюджета [1].

В ноябре 2016 Свердловская область заняла первое место по количеству ВИЧ-инфицированных в России. В столице региона — Екатеринбурге — болен каждый пятидесятый.

По критериям Всемирной организации здравоохранения (ВОЗ), если в регионе вирус выявлен более чем у 1-го процента жителей (особенно у беременных), это значит, что началась стадия «генерализованной» эпидемии. То есть болезнь выходит за пределы групп риска, где она циркулировала на протяжении долгого времени.

По данным Роспотребнадзора, эпидемиологический порог в 1 процент превышен в Кемеровской, Ульяновской, Иркутской, Тюменской областях, Пермском крае, Ленинградской, Челябинской и Оренбургской областях, Ханты-Мансийском автономном округе, Томской области, Алтайском крае, Новосибирской, Мурманской, Омской, Ивановской, Тверской и Курганской областях, Самарская. В лидерах — Свердловская области. Тут заражены более 2-х процентов беременных.

В целом по России число ВИЧ-инфицированных перевалило за миллион. Эксперты считают, что еще около 500-800 тысяч россиян не подозревают о своей болезни, так как не относят себя к группам риска и ни разу не проверялись.

Раньше ВИЧ в России считался уделом маргиналов — наркоманов, проституток, гомосексуалистов. Но генерализованная эпидемия означает, что теперь заразиться может каждый. Это еще не грипп — все же воздушно-капельным путем ВИЧ не передается, но чтобы гарантированно избежать заражения, уже недостаточно просто избегать общения с группами риска. Многие не знают, проверен их партнер на ВИЧ-инфекцию или нет, мог ли он в прошлом заразиться. Между тем каждый сороковой мужчина в возрасте 30–35 лет инфицирован ВИЧ. В зависимости от региона заражен каждый двадцатый мужчина в возрасте 21-40 лет. Вероятность инфицирования весьма велика [2].

В конце октября глава Минздрава Вероника Скворцова предупредила об угрозе эпидемии ВИЧ в России. По ее словам, к 2020 году число ВИЧ-инфицированных в России может увеличиться на 250%. Это произойдет в случае, если финансирование лечения со стороны государства останется на прежнем уровне [3].

Из выше сказанного можно сделать вывод, что в России, и в частности Самарской области живет множество ВИЧ-инфицированных людей. Их можно встретить не только на улице, но и в организации, в которой вы работаете.

Цель данной статьи - определить возможности использования и защиты ВИЧ-инфицированных трудовых ресурсов в организации.

В статье произведен обзор законов, защищающих ВИЧ-инфицированных работников предприятий, приведены результаты опросов о взаимодействии между здоровыми и ВИЧ инфицированными сотрудниками в организации.

Основной закон, касающихся ВИЧ-инфицированных людей был принят в 1995 году [4]. Перечень видов профессиональной деятельности, запрещенных для лиц, зараженных вирусом иммунодефицита человека утвержден в **Приказе министра здравоохранения в 2014 году** [5].

В обновленный Перечень вошли 9 видов профессиональной деятельности, запрещенных для лиц, зараженных ВИЧ. Это профессии, связанные с:

1. заготовкой и переработкой крови и ее компонентов;
2. приемом крови и ее компонентов, спермы и грудного молока;
3. гемотрансфузией;
4. медицинскими процедурами (инъекции, диализ, венесекция, катетеризация);
5. косметическими и пластическими операциями;
6. стоматологическими процедурами;
7. родами;
8. абортами и иными гинекологическими операциями;
9. стрижкой и бритьем, пирсингом, маникюром, педикюром и татуажем.

О том, как относятся россияне к ситуации взаимодействия с ВИЧ-инфицированными проводятся многочисленные опросы. Ниже представлены два опроса и их результаты[6], [7].

Первый опрос был проведен 5-8 июня 2006 года по заказу радиостанции "Милицейская волна". Всего было опрошено 1600 респондентов. Исследуемая совокупность - экономически активное население России в возрасте от 18 лет и старше.

Был задан вопрос: Как Вы будете себя вести, если узнаете, что ваш коллега по работе ВИЧ-инфицирован? Ответы респондентов на данный вопрос представлены в виде круговой диаграммы на рисунке 1.

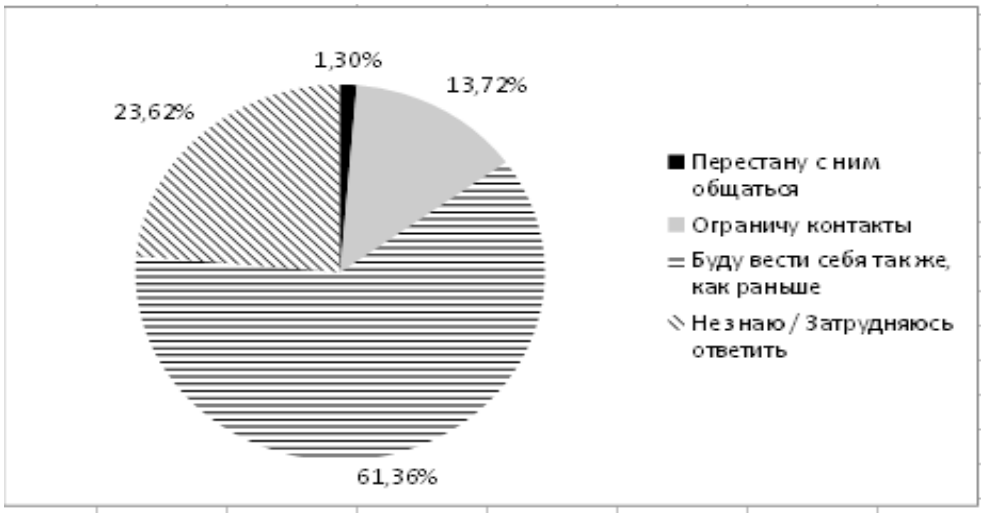


Рисунок 1 - Диаграмма ответов респондентов на вопрос «Как Вы будете себя вести, если узнаете, что ваш коллега по работе ВИЧ-инфицирован»

Ниже перечислены несколько комментарий респондентов на поставленный вопрос:

1. "Я, конечно, немного доверяю тем врачам, которые уверяют, что заболеть от простого пожатия рукой ВИЧ невозможно, но, тем не менее, мне кажется, данный человек очень опасен. (...) Можете себе представить, что такое находящийся с тобой на рабочем месте ВИЧ больной? Это просто смерть под боком на рабочем месте, да я скорее перейду на другую работу менее оплачиваемую, чем останусь с таким человеком..."
2. "Несмотря на то, что не хочется придавать этому значение, но эта болезнь очень серьезна и опасна. Я бы не дала повода себе чем-то обидеть этого человека, но контакты бы ограничила".
3. "ВИЧ - не грипп, воздушно-капельным путём не передаётся!"
4. "Общеизвестный факт, что СПИД передается ТОЛЬКО при половом контакте и через кровь! Грубо и бестактно изменять свое отношение к человеку в подобной ситуации!!!"
5. "ВИЧ-инфицированные люди ничем не отличаются от обычных людей, и сторонится их совсем не стоит. Просто в нашей стране многие малограмотны в этом вопросе и ведут себя неправильно по отношению к таким людям, они просто не знают, как себя вести. Ведь ВИЧ-инфицированным людям, наоборот, нужна наша поддержка: им и так нелегко приходится".
6. "Умом каждый человек понимает, что на бытовом уровне заразиться сложно. Но психологический страх заставляет вести себя по-другому".
7. "В теории - общение останется прежним. Но на практике - невозможно, общаясь с этим человеком, не думать о том, что он заражен. Дело даже не в информированности о способах передачи вируса, - а во внутренней боязни: "Мало ли что! Всякое бывает. А вдруг я могу все-таки заразиться?"

Второе социологическое исследование проводилось среди жителей г. Перми. Сбор первичных данных осуществлялся с помощью метода формализованного интервью. Объем опрошенных составил 609 человек. Из них 50.5 % женщин и 49.5 % мужчин в возрасте от 15 до 59 лет. С разным уровнем образования.

В ходе опроса респондентам было предложено представить ситуацию, когда в их окружении могут находиться ВИЧ-инфицированные, при этом предполагалось как личное окружение (близкий друг, член семьи), так и более отдаленные социальные контакты (коллеги на работе и соседи). Большинство участников заявило об изменении своего поведения и отношения к человеку, который подвергся инфицированию ВИЧ. Постараются меньше общаться 27% с соседом, 19% с коллегой и 0.5% с близким человеком. Высказались о том, что им будет неприятно, но постараются вести себя как обычно: 18% опрошенных к соседу, 21% к коллеге и 2.5% к близкому человеку. Сказали, что окажут посильную помощь и поддержку ВИЧ-инфицированному: 10% соседу и коллеге, а ВИЧ-инфицированному близкому человеку уже 47% респон-

дентов. Ничего не измениться в отношении: у 24% респондентов к коллеге, у 27% к соседу и у 38% к близкому человеку. Также задавались вопросы о передачах инфекции.

Для оценки типологической толерантности к ВИЧ-инфицированным, респондентам было задано три вопроса (таблица 1).

Таблица 1 - Оценка типологической толерантности к ВИЧ-инфицированным

Вопрос респондентам	Ответ (в % от числа опрошенных)	
	Да	Нет
1. Если учитель имеет положительный ВИЧ-статус, но хорошо себя чувствует, может ли он или она дальше преподавать в школе?	39.9	29.6
2. Если спортивный инструктор имеет положительный ВИЧ-статус, может ли он или она дальше проводить тренировки?	31.0	37.4
3. Если врач имеет положительный ВИЧ-статус, но хорошо себя чувствует, может ли он или она продолжать принимать больных и производить медицинские манипуляции?	5.9	62.1

Из результатов опроса следует:

1. Треть респондентов не ответили на вопросы, возможно они считают, что это не их проблема?

2. Только 6% респондентов ответили, что ВИЧ-инфицированный врач может принимать больных и производить медицинские манипуляции.

Также задавались вопросы о передачах ВИЧ-инфекции. Оценка информированности показала вполне удовлетворительные знания основных путей передачи ВИЧ-инфекции: 76 - 92 % респондентов дали верные ответы на вопросы об основных путях передачи ВИЧ. Но у респондентов достаточно высокий уровень заблуждений о путях передачи ВИЧ. Четверть опрошенных людей дали ответ «не знаю» на вопрос о возможности ВИЧ-инфицирования через укус комара и 16% не знают можно ли инфицироваться при совместном приеме пищи с ВИЧ-инфицированным. Что может являться основой для образования «спидофобии».

Что думают в компаниях работодатели о сотрудниках с ВИЧ-инфекцией

Не все работодатели, узнав, что у кандидата ВИЧ, в ужасе закатывают глаза. Многие предпочитают разумный подход. Решая вопрос, принимать ли на работу специалиста с ВИЧ, они обращают внимание на четыре момента.

1. Профессиональные качества. «Главное - эффективность специалиста и его необходимость компании», - считает Екатерина Грипась, заместитель директора по персоналу инвестиционного холдинга «Финам».

2. Отношение человека к его заболеванию. По словам Анны Михеевой, административного директора RU-CENTER, одни люди больны и физически, и психологически, и эмоционально. Другие воспринимают свою болезнь как шанс стать более сильным, преодолеть свои внутренние конфликты и сложности, стать целостной личностью. «Такой человек, оказавшись лицом к лицу с необходимостью постоянно бороться за свою жизнь, может быть более зрелым и сильным и в личностном, и в профессиональном плане. Мотивация его может быть гораздо сильнее, и ресурс, который он готов предложить, возможно, окажется несравнимо больше, несмотря на физические недуги. Мне известны случаи, когда в компании работали люди с неизлечимыми и трудноизлечимыми заболеваниями — они вносили огромный вклад в дело».

Участница форума Работы.ру: «Мы можем быть лучшими работниками, потому что переосмыслили наши цели и стремления. Мы работаем на результат, не отвлекаясь на мелочи. Я знаю, чего я хочу добиться. ВИЧ как стимул, не дает мне сбиться с цели». Кстати, у нее нет проблем с работой и заработком.

3. Физические возможности**.** «Я вижу только одно ограничение при приеме на работу специалиста с ВИЧ — сможет ли он работать по предложенному графику. Это касается любых хронических заболеваний, связанных с посещением врачей, прохождением обследований», — говорит рекрутер с форума Работы.ру.

4. Мнение непосредственного руководителя**.** Екатерина Грипась: «Скорее всего, я бы донесла до руководителя специалиста информацию о его заболевании (думаю, жесткого негатива не было бы — у нас работают интеллектуальные сотрудники). Если бы у него не возникло возражений, то сотрудник был бы принят на работу».

Решая вопрос, узнавать ли мнение остальных сотрудников или сохранить необходимый уровень конфиденциальности, Екатерина Грипась выбрала бы второй вариант, ведь ВИЧ не относится к числу заболеваний, передающихся при личных контактах. «ВИЧ-инфицированным специалистам я бы посоветовала принять свою ситуацию, — говорит она. — Суметь увидеть себя полноценным и полноправным специалистом и человеком» [8].

Таким образом, по результатам данного исследования о возможности использования и безопасности ВИЧ-инфицированных работников в организации сделаны следующие выводы.

1 Уровень ВИЧ-инфицированных в стране, в том числе в Самарской области, достаточно высокий и, следовательно, необходимо соблюдать определенные правила их использования в качестве работников в организациях.

2 Существует 9 профессий, в которых ВИЧ-инфицированные люди не могут работать. Если профессия не входит в список запрещенных профессий, работодатель не имеет право отказывать ВИЧ-инфицированным людям в устройстве на работу, либо в увольнении по причине болезни.

3 Идет сильная стигматизация ВИЧ-инфицированных людей, как на эмоциональном уровне, так и на рациональном. В глазах социального окружения и в обществе ВИЧ-инфицированные воспринимаются как обладающие существенным дефектом, своего рода неполноценные члены общества. Выражается это в восприятии их как людей распущенных, источник смертельной опасности для окружающих, носителей отвратительных черт. Все это является основой для произвольной дискриминации.

4 Опрос показал, что среди населения прослеживается сильная дискриминация ВИЧ-инфицированных. Среди респондентов высокая доля считающих, что нужно ограничивать во всех социальных сферах, или они должны быть исключены из общества. Так же свой посильный вклад в стигматизацию и дискриминацию вносят не достаточная информированность и заблуждения о ВИЧ.

5 Однако работодатели адекватно относятся к ВИЧ-инфированным и многие готовы взять их на работу, если они смогут выполнять свои трудовые обязательства.

Библиографический список

1. Елена Малышева, Карина Романова, Петр Нетреба. «ВИЧ африканского масштаба» 15.07.2016 год. [Электронный ресурс] // URL: https://www.gazeta.ru/ business/2016/07/14/9689903.shtml (дата обращения: 12.11.2016).

2. Наталья Гранина «Угрожает ли России масштабная эпидемия ВИЧ» 02.11.2016 год. https://lenta.ru/articles/2016/11/02/hiv/ (дата обращения: 12.11.2016).

3. Настя Березина «Число ВИЧ-инфицированных в России достигло 1 млн человек» 20.01.2016 год. http://www.rbc.ru/society/ (дата обращения: 12.11.2016).

4. «Федеральный закон от 30 марта 1995 г. № 38-ФЗ» http://base.garant.ru/ 10104189/#ixzz4PuQSw2rB (дата обращения: 12.11.2016).

5. 13.05.2016 год. «Обновлен перечень профессий, запрещенных для ВИЧ-инфицированных» http://www.norma.uz/novoe_v_zakonodatelstve/obnovlen_perechen_professiy_zapreshchennyh_dlya_vich-inficirovannyh (дата обращения: 12.11.2016).

6. Исследовательский центр портала Superjob.ru 08.06.2006 год. «Если ваш коллега ВИЧ-инфицирован?» https://www.superjob.ru/research/articles/374/esli-vash-kollega-vich-inficirovan/ (дата обращения: 12.11.2016).

7. Пермский краевой центр по профилактике и борьбе со СПИД и инфекционными заболеваниями. «Толерантность по отношению к ВИЧ-инфицированным и больным СПИДом» http://aids-centr.perm.ru/ (дата обращения: 12.11.2016).

8. Наталья Полетаева. 14.10.2008 год. «Как работать ВИЧ-инфицированным» http://www.rabota.ru/soiskateljam/rights/ kak_rabotat _vich_ infitsirovannym.html (дата обращения: 12.11.2016).

ВЗАИМОСВЯЗЬ ИМПОРТОЗАМЕЩЕНИЯ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Килин А.В., студент
Научный руководитель: д.э.н. профессор А.Я. Щукина
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

С начала 2014 года страны Европы неоднократно принимали решение ввести санкции экономического характера в отношении Российской Федерации. Основные причины были следующие:

– присоединение Крыма после референдума 16 марта 2014, на котором большинство проголосовало за вхождение в состав РФ;

– обострение ситуации на востоке Украины. Россию обвинили в снабжении повстанцев оружием;

– крушение пассажирского самолета над Донецкой областью, в чем также обвиняют Россию.

Список санкций на сегодняшний день, примененных к РФ, достаточно широк и касается многих сфер.

Так, остаются в силе ограничения на доступ к европейскому кредитованию, введенные для трех крупнейших российских кредитных учреждений – Сбербанка России, ВТБ и Газпромбанка.

Продлен срок оружейного эмбарго, что подразумевает прекращение поставок в Россию продукции двойного назначения, особенно электроники.

Следующее ограничение касается продажи РФ инновационного технологического оборудования для шельфовой и сланцевой добычи «черного золота». Однако в условиях резкого снижения стоимости нефти данные санкции не оказывают сильного влияния.

Запрет на въезд в зарубежные страны определенным гражданам и руководству некоторых предприятий. В черный список входят свыше 150 человек – политики, звезды эстрады и представители самопровозглашенных ДНР и ЛНР.

Рассмотрим более подробно экономические последствия введения санкций против нашей страны. Если проанализировать отраслевую структуру санкций против России, то можно обнаружить, что они направлены против ключевых отраслей экономики РФ: нефтяной, газовой, атомной и военной промышленности, а также против российского банковского капитала.

Мировой рынок нефти и нефтедобычи в основном контролируется американскими и британскими транснациональными компаниями: ExxonMobile, Shell, BP, Chevron и прочие. С 2007 года в США росли объемы внутренней нефтедобычи. Если в 2006 году США ежедневно производили 8316 тыс. баррелей нефти в сутки, то в 2013 году этот показатель составил 12304 тыс. баррелей [1], т.е рост объемов добычи нефти в США с 2006 по 2013 гг. составил 48% (рис.1).

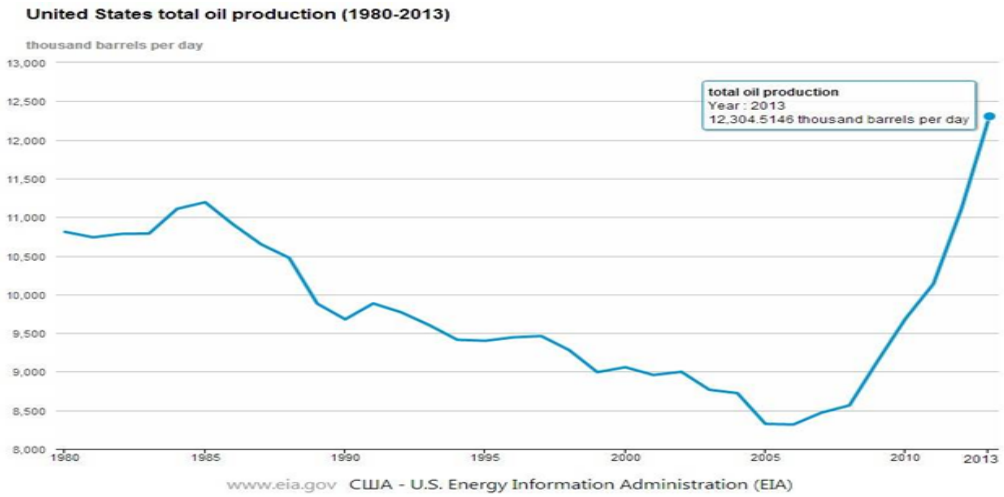


Рисунок 1 - Общая добыча нефти в США

Им нужно находить рынки сбыта, а самым перспективным является европейский рынок, но 1/3 поставок нефти в Европу обеспечивается российскими компаниями. Ситуация связанная с конфликтом на Украине позволила найти формальный повод для введения санкций против РФ, в результате упали цены на нефть с 99 долларов за баррель в 2014 году до 47 долларов за баррель в 2015 году [2].

При этом эффект низких цен оказал существенную поддержку глобальному спросу на нефть, который согласно Агентству энергетической информации США (EIA) по итогам прошлого года увеличился на 1,33 млн. барр./сут., и стал рекордным показателем за последние 5 лет. В частности, оживлению спроса в странах ОЭСР способствовал рост потребления бензина в США. Несмотря на снижение цен на нефть и сохраняющийся санкционный режим для нефтяной отрасли, добыча жидких углеводородов в России в 2015 г. выросла на 1,4% по сравнению с 2014 г. (рис. 2).

Основные векторы налагаемых санкций в нефтяной отрасли следующие:

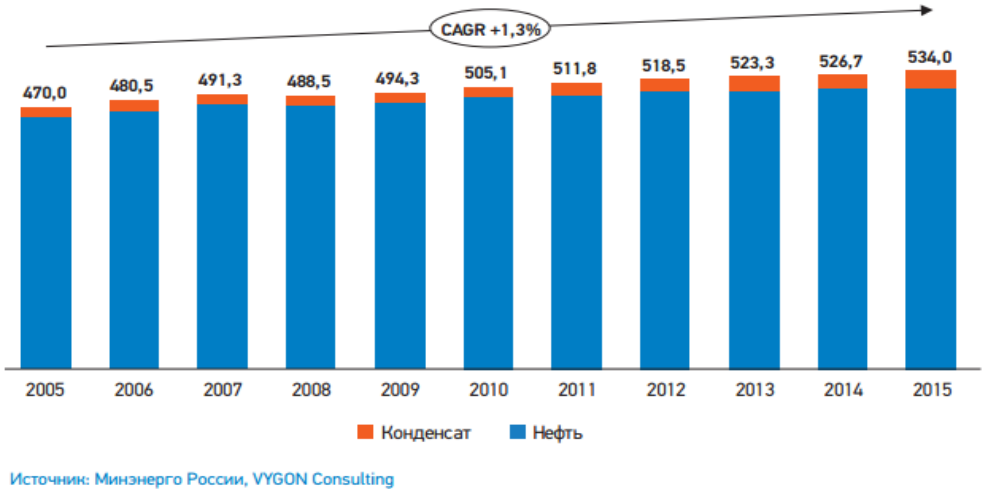
– санкции против российских нефтяных компаний и их дочерних предприятий;

– запрет на экспорт в Россию технологий нефтедобычи и нефтепереработки;

– отказ от совместных проектов в нефтяной сфере и инвестирования перспективных проектов.

Проанализируем санкции в газовой отрасли против РФ. Россия является крупнейшим в мире производителем природного газа. Монополистом в российской газовой сфере является компания «Газпром», которая ежегодно покрывает треть потребности Европы в газе. В 2015 году доля газа компании в европейском потреблении достигла рекордного значения – 31% [3].

Начиная с 2000-годов американские компании стали инвестировать огромные средства в разработку нетрадиционных источников газа. Начиная с 2006 года, в США отмечается стремительный рост производства газа. Сланцевый бум в 2010 году привел к избыточному предложению газа на внутреннем рынке, а в 2012 году к обвалу цен на газ в США (рис. 3).



Источник: Минэнерго России, VYGON Consulting

Рисунок 2 - Динамика добычи жидких углеводородов в России, млн. т.

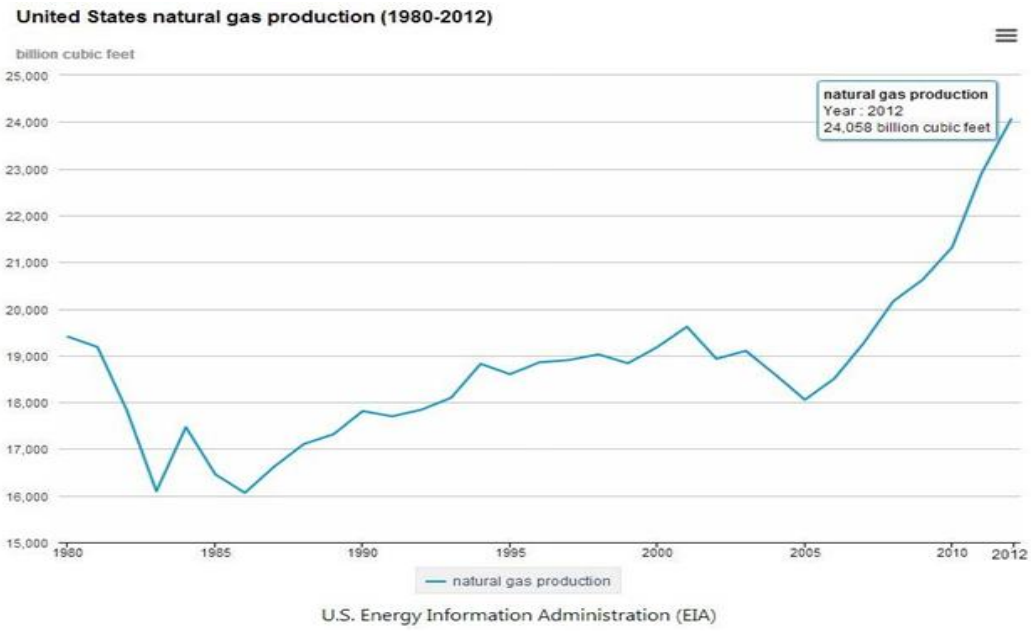


Рисунок 3 - Добыча природного газа в США

В этой связи американские компании в ближайшей перспективе будут испытывать потребность в крупных рынках сбыта, прежде всего – Европы и Азии. Однако на данных рынках США в настоящее время ограничены тремя основными факторами:

1. Отсутствие достаточного количества в Европе регазификационных СПГ – терминалов;
2. Отсутствие экспортных СПГ – терминалов в США;
3. Текущие долгосрочные контракты с Газпромом на поставку российского газа в ЕС.

Однако ввиду отсутствия технической возможности альтернативных поставок газа в ЕС в настоящее время санкции в отношении Газпрома вряд ли будут применены. Но поскольку рынок Европы является наиболее перспективным для американских и британских компаний, то налагаемые санкции будут направлены на все перспективные проекты Газпрома.

Анализ санкций показывает, что они направлены на ограничение присутствия российских компаний в различных сегментах мирового и, прежде всего, европейского рынка, на долю которого приходится половина внешнеторгового оборота РФ. Отсюда ситуация с Украиной послужила удобным формальным поводом к практическим действиям против РФ в этом направлении.

При сохранении и расширении текущих санкций, можно ожидать уменьшения доли российских компаний на нефтяном, а в перспективе и на газовом рынке Европы и замещение их британскими и американскими компаниями.

Зависимость России от поставок сырья на рынок ЕС рано или поздно должно было обнажить негативные стороны такого сотрудничества. Отсюда диверсификация рынков сбыта становится приоритетной задачей для экономики РФ.

Анализируя прогноз, который был дан Всемирным Банком в январе 2015 года, рост ВВП России в 2016 году должен был увеличиться в среднем на 0,1%. Однако, при условии, что санкционная политика в отношении России сохранится, уровень ВВП в 2016 году по последним прогнозам, скорее сократится на 0,3% [4]. Однако, одним из условий реализации данного прогноза является сохранение рекордно низкой мировой цены на нефть, в пределах 53 долларов США за баррель. Именно в этом случае доступ российских банков и иных финансовых корпораций будет находиться в режиме жесткого ограничения к мировым финансовым рынкам. Падение инвестиций в российскую экономику, при условии сохранения санкционного режима, может затянуться вплоть до 2018 года.

При ограничении или прекращении торговых связей с Европой экономика России может получить толчок для возрождения и развития как промышленности, так и сельского хозяйства, которое именно из-за введения санкций стало развиваться более быстрыми темпами.

Санкции России против ЕС закрыли для большинства продуктов питания из стран Евросоюза доступ на Российский рынок, что естественным образом вызвало непропорциональное повышение предложения в самом ЕС, которое давит на цены. В зависимости от типа продукта, санкции могут ощутить в большой мере поставщики киви (10 % экспорта в Россию), груш (8 %) и яблок (7%). Почти незаметен эффект от эмбарго будет для производителей моркови и свеклы (по 1% экспорта).

Санкции против России и ответные меры РФ принесли странам ЕС убытки в 5 млрд. евро, а не входящей в ЕС Норвегии – убытки в 1 млрд. евро. Согласно Австрийскому институту экономических исследований, продление санкций составит потери до 90 млрд. евро экспортной выручки и более двух миллионов рабочих мест в 2016 году в странах ЕС.

По итогам 2015 года отечественное сельское хозяйство стало лидирующим сектором по росту производства – производство сельхозпродукции увеличилось на 3,5%. За последние 3-4 года Россия сократила затраты на закупки продуктов питания за рубежом почти в 2 раза: с 42-44 млрд. долл. в 2012 году до 23-24 млрд. долл. в 2015 году.

Сельское хозяйство является отраслью стратегического значения, развитие которой направлено не только на получение коммерческой прибыли, но и обеспечение продовольственной безопасности России.

В настоящее время в России происходит импортозамещение многих товаров, ввоз которых прекратился из-за санкций – даже тех, которые раньше в России не производились. Например, в Свердловской области стали производить мясной деликатес – хамон. В 2015 году во Владикавказе, начали производить итальянские сыры – моцареллу и рикотту. Производство сыров в РФ в 2014 году выросло почти на 15%, а в 2015 еще на 35%, однако качество импортозамещаемой продукции серьезно уступает аналогам в большинстве случаев [5]. Причины этого следующие:

- не хватает натурального сырья и новейших технологий для производства сыров;
- отсутствуют особенности культуры сыроварения.

Столкнувшись с частичной экономической блокадой в Европе, Россия во многом изменила курс внешней политики на Восток, где главным союзником стал Китай. Товарооборот с 2011 по 2014 гг. показал существенный рост, однако в первой половине 2015 года уровень торговли между двумя странами снизился на 28,3 % по сравнению с первой половиной 2014 года (табл. 1).

Влияние на снижение товарооборота между двумя странами оказывает дисбаланс структуры двусторонней торговли. Основными статьями экспорта Китая в Россию являются машиностроительная продукция и электроника, а экспорт России в Китай состоит в основном из энергоносителей и сырьевой продукции. Таким образом, резкое снижение цен на нефть в конце 2014 года привело к уменьшению стоимости российской нефти, экспортируемой в Китай, что, в свою очередь, снизило объемы двустороннего товарооборота.

Таблица 1- Товарооборот между Россией и Китаем за 2011-2015 гг. (млрд. $) [7]

	2011	2012	2013	2014	Январь - июнь 2014 г.	Январь - июнь 2015 г.
Оборот	83,5	87,5	88,8	88,4	**42,9**	**30,6**
Темпы роста в %	140,8	105,2	101,6	99,5		71,3
Экспорт	35,2	35,7	35,6	37,5	**19,1**	**14,6**
Темпы роста в %	173,4	102	99,6	105,7		76,5
Импорт	48,3	51,8	53,1	50,9	**23,9**	**16**
Темпы роста в %	123,9	107,6	102,9	95,7		67,2
Сальдо	-13,1	-16,1	-17,5	-13,4		-1,4

Несмотря на сокращение двустороннего товарооборота, в торгово-экономическом сотрудничестве Китая и России отмечаются новые тенденции развитии. Ожидается, что благодаря совместным усилиям правительств двух стран и активной внешнеэкономической деятельности, цель достижения двустороннего товарооборота до 200 млрд. долл. будет достигнута к 2020 году. Кроме того, китайские и российские эксперты считают, что снижение товарооборота между двумя странами не окажет серьезного влияния на стабильное долгосрочное торгово-экономическое сотрудничество двух стран.

Исходя из всего вышеизложенного, можно сделать вывод от санкций страдают обе стороны как ЕС, так и РФ. Но для России введение санкций со стороны запада сыграло немаловажную роль в понимании нынешней экономической ситуации, в которой наиболее важные отрасли хозяйствования сильно зависят от иностранных поставщиков. Это, такие стратегически важные товары как, продовольствие, лекарства, технологии и комплектующие для машин. Однако России, в первую очередь, необходимо развивать импортозамещение товаров сельского хозяйства и фармакологии, что увеличит ее независимость от иностранных поставщиков, поскольку на данный момент, крупнейшие европейские поставщики занимают 71,8% российского фармацевтического рынка [6].

Таким образом, в условиях давления на РФ со стороны ряда зарубежных стран в форме санкций, российские власти изменили курс политики на импортозамещение, что позволяет в нынешних условиях отечественным производителям сельскохозяйственной продукции развиваться. России необходимо и дальше развивать политику импортозамещения и обеспечивать независимость страны, в первую очередь от иностранных поставщиков продуктов питания и медикаментов, что позволит обеспечить более высокую экономическую безопасность страны.

Библиографический список

1. http://weic.info/ekonomicheskie_stati/ekonomicheskie_sankcii_protiv_rossii_rf_prichiny_analiz_spiski_posledstviia;
2. http://ru.investing.com/commodities/brent-oil;
3. http://www.gazprom.ru/about/marketing/europe/;
4. http://altaempresa.ru/ekonomicheskie-sanktsii-v-2016-godu-prognoz-i-realnost/;
5. http://ruxpert.ru/;
6. http://refleader.ru/rnaqasyfsbew.html;
7. http://moluch.ru/archive/106/25163/.

ФАКТОРЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ МАЛОГО БИЗНЕСА В РОССИИ

Мелёхин Д.М., студент
Научный руководитель: к.т.н., доцент В.М. Ильичев
ОАНО ВО «Волжский университет имени В.Н. Татищева»
г. Тольятти, Россия

В настоящее время Россия столкнулась с проблемой экономической безопасности, это способность реагировать на внешние и внутренние факторы, а так же поддерживать основные показатели экономики на уровне достаточном для функционирования и развития. Для экономической безопасности большое значение имеют пороговые значение основных показателей. Пороговые значения - это величины, несоблюдение которых приводит к формированию различных внутренних и внешних рисков, которые в свою очередь отрицательно влияют на экономическую безопасность. Пороговые значения основных показателей экономической безопасности представляют собой барьер, выход за который несет отрицательные последствия экономической стабильности хозяйствующего объекта. Например, к основным показателям экономической безопасности страны относятся: уровень падения

ВВП; доля ВВП государственных ассигнований на науку; доля в экспорте продукции обрабатывающей промышленности; доля импортных продуктов питания и другие показатели, определяющие конкурентоспособность страны [1].

Перспективы развития малого бизнеса в России определяются необходимостью развития конкурентной среды, повышения качества товаров и услуг, уровня производительности труда. В масштабах страны роль малого бизнеса нельзя недооценивать, так как малое и среднее предпринимательство являются важным фактором структурной модернизации экономики России. Малое предпринимательство охватывает, достаточно большой круг лиц и тем самым борется с безработицей и с социальной напряженностью в обществе. В целях объективной оценки следует отметить, что малое предпринимательство по накопленному в нем человеческому потенциалу, неисчерпаемому запасу идей, масштабам рынка, который ему предстоит освоить, призвано стать важнейшим фактором ускорения рыночных преобразований и обеспечения достойных условий жизни миллионов граждан [2, 3]. Это дает основание говорить о том, что состояние, развитие и устойчивая динамика малого предпринимательства во многом предопределяет экономическую безопасность государства. Оказывая сильнейшее воздействие на экономику, политику, социальную сферу малое предпринимательство зависит от многочисленных внешних (экономических, политических, организационных и др.) факторов. От характера факторов внешней среды зависит успешное развитие малого предпринимательства в рыночной экономике. С данных позиций формирование благоприятной внешней среды малого предпринимательства задача продуманной и стратегической государственной политики. Государство должно способствовать развитию малого бизнеса, постепенно освобождая его от непосильного налогового бремени, произвола бюрократии и власти мафиозных структур [4]. Для поддержания состояния экономической безопасности субъектов малых форм хозяйствования следует придерживаться стратегии, обеспечивающей достаточный уровень и наращивание социально-экономического потенциала, устойчивое развитие и подготовленность к возможным нежелательным изменениям. Вероятность осуществления угрозы (уязвимости) бизнес-деятельности, перехода ее из потенциальной в реальную характеризует понятие «предпринимательские риски». Риски имманентны малому бизнесу, поскольку природа последних всецело основана на рыночных законах с присущими им стихийностью, непредсказуемостью и неопределенностью. Поэтому, каким бы ни было экономическое поведение хозяйствующего субъекта, они всегда существуют. Поэтому, невозможно достичь полной экономической безопасности бизнес-деятельности. Задача хозяйствующего субъекта – минимизировать предпринимательские риски, обеспечивая тем самым устойчивую динамику развития малых бизнес-структур и фактически исключая возможность экономических потрясений [5].

Подводя итог, можно отметить, что, несмотря на трудности, идёт рост числа предпринимателей. И нужно рассматривать экономическую безопасность государства необходимо рассматривать с одной стороны, как материальную основу национальной безопасности, а с другой - как целостную, единую, целенаправленную систему.

Библиографический список

1. Современная модель эффективного бизнеса: монография / Н.Ю. Величко, Н.А. Гончарова, Н.В. Заболоцкая и др./Под общ. ред. С.С. Чернова. Книга 10. - Новосибирск: ООО «Агентство «СИБПРИНТ», 2012. -189 с.

2. Экономика: мировой исторический опыт и современные проблемы монография. Книга 3/под ред. М.М. Скорева. Ставрополь: Логос, 2014. С. 2761.

3. Гусаков, Н.П. Концептуальные подходы к разработке новой Стратегии экономической безопасности / Н.П. Гусаков, И.В. Андронова // Нац. интересы: приоритеты и безопасность. - 2014. С. 341.

4. http://smb.gov.ru/mediacenter/expertopinions/17734.html.

5. http://www.fundamental-research.ru/ru/article/view?id=39817.

ДОСТАТОЧНОСТЬ ЗАЛОГА КАК ФАКТОР ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО БАНКА

Рогачева Т.Л., студент
Научный руководитель: к.э.н., доцент Н.В. Таратухина
ОАНО ВО «Волжский университет имении В.Н. Татищева»
г. Тольятти, Россия

Проблема достаточности залогового обеспечения является крайне актуальной для российских банков, поскольку довольно часто стоимость залога имеет тенденцию к снижению, и при реализации

залога банк может потерпеть убытки. Это в свою очередь ведет к снижению общего уровня финансовой безопасности кредитной организации и возникновению риска потери платежеспособности.

Согласно ст.1 ФЗ «О залоге», залог – это способ обеспечения обязательства, при котором кредитор-залогодержатель приобретает право в случае неисполнения должником обязательства получить удовлетворение за счет заложенного имущества преимущественно перед другими кредиторами за изъятиями, предусмотренными законом.

Залог – это эффективная демонстрация состоятельности намерений заемщика и гарантия его благонадежности. По данным Центрального Банка РФ более 63% активов ведущих российских банков – это кредиты населению и предприятиям различной формы собственности. Подобная значимость и объем кредитного портфеля свидетельствует о существенном и определяющем влиянии кредитной деятельности на рентабельность финансовых учреждений. Чтобы обезопасить свою деятельность, банки широко используют залоговое имущество как инструмент, повышающий ответственность заемщика. В течение всего срока кредитования залог для обеспечения финансовой безопасности кредитной организации выполняет еще ряд определенных функций:

- стимулирует возвратность кредитных средств, выданных банком;
- обеспечивает реальный возврат финансовых средств с помощью механизмов взыскания имущества, заложенного заемщиком в банковское учреждение;
- сдерживает рост кредитной задолженности у должника в других финансовых организациях;
- минимизирует риски досрочного вывода активов заемщика;
- корректирует резервы при возникновении просрочки платежа.

Актуальной проблемой применения механизма залога является проблема расчета объективной и максимально достоверной стоимости имущества, предоставляемого в обеспечение кредита. Необходимо отметить, что на Законодательном уровне не прописаны нормы, обязывающие проведение оценки стоимости залога в процессе проведения операций банковского займа и его погашения. Такое требование указано в Федеральных стандартах оценочной деятельности, которые обязательны для выполнения аккредитованными экспертными компаниями. Для банка оценка залога является четко обоснованным основанием для расчета суммы заемных средств, а для заемщика – объективным выражением фактической стоимости его материальных активов на момент проведения оценочных мероприятий. Поэтому в качественно выполненной оценке и ее достоверности заинтересованы обе стороны – и банковская структура, и ее потенциальный клиент, будущий заемщик.

Однако какой бы степенью надежности не обладал залог, его принятие неизбежно накладывает на коммерческий банк целый ряд рисков, снижающих общий уровень его финансовой безопасности. И прежде всего, риск невозвратности заемных средств, что отрицательно влияет на деятельность банка и на его экономическую безопасность в современных условиях.

Оценка залогов для банков состоит из специальной технологии расчета залоговой стоимости, равной определенной сумме, за которую можно реализовать данный актив, за минусом издержек и затрат, связанных с взысканием денежных средств и продажей предмета залога. Профессиональные эксперты оценивают залоговую стоимость имущества в несколько этапов:

1. На первом этапе определяется текущая рыночная стоимость предмета залога с помощью проведения подробного анализа аналоговых предложений в данном регионе и объектов с соответствующими характеристиками.

2. На основании полученной суммы проводится корректировка рыночной цены при помощи экспертного прогнозирования изменений стоимости залога на дату возможной продажи имущества.

3. Полученная прогнозируемая стоимость еще раз корректируется с учетом возможных издержек и затрат, экономических и юридических рисков, которые могут возникнуть во время процедуры взыскания и реализации залога.

К залоговому имуществу могут быть отнесены различные материальные ценности, обладающие существенной стоимостью, недвижимость и различные активы, которые на время проведения сделки по кредитованию передаются в банк. Профессиональная оценка залогов для банков выполняется независимым экспертом для определения реальной стоимости залогового имущества.

В качестве предмета залога могут выступать следующие активы: объекты недвижимости: здания, сооружения, частные дома, квартиры, земля и другие виды недвижимости, имеющие документы на право собственности; транспортные средства различной категории: автомобили, катера, грузовые машины, воздушный транспорт; технологическое оборудование и техника; промышленные и продовольственные товары с длительным сроком службы и хранения, включая активы, находящиеся в обороте предприятия; нематериальные активы: имущественные права и обязательства; акции, векселя и другие ценные бумаги.

Необходимо отметить, что в настоящее время самое ощутимое преимущество среди конкурентов имеют банки, использующие гибкий и всесторонний подход к оценочной деятельности и дисконтированию стоимости залога. Размер дисконта ставится в зависимость от надежности заемщика, финансовых и экономических показателей его деятельности.

Избежание рисков на сегодняшний день является широко применимым инструментом защиты коммерческим банком собственных интересов. Банк нацелен на предотвращение значительных потерь, то есть определяющей является оценка негативной стороны риска.

При этом уровень конкуренции на рынке ссудного капитала сегодня настолько велик, что в своем стремлении приобрести новых или сохранить старых клиентов, путем создания наиболее привлекательных условий, банки могут идти на ухудшение качества своего залогового портфеля. Возникает ситуация, в которой банк теряет рычаги воздействия на клиента, тем самым увеличивая вероятность возможного невозврата денежных средств. В свою очередь невозврат кредита при наличии залогового обеспечения выливается для банка в сверхубытки.

В условиях понесенных убытков выходом будет являться ужесточение процедуры оформления приемлемого залогового обеспечения. Однако следствием чрезмерного ужесточения залоговой политики для коммерческого банка может стать снижение привлекательности предлагаемых им услуг в результате удорожания кредитов, а также сложностей в оформлении залогового обеспечения. Как следствие коммерческий банк имеет возможность потерять клиента еще до начала работы с ним.

Таким образом, эффективное функционирование коммерческого банка и обеспечение высокого уровня его финансовой безопасности возможно только при оптимальной оценке обеспечения возвратности кредита залогом. Чтобы залог был реально работающим инструментом кредитования, необходимо при оценке залога ставить перед экспертом, как основным исполнителем и главным ответственным лицом, четкие и определенные задачи по расчету стоимости залогового имущества. Нельзя ориентироваться только на рыночную стоимость предмета залога, так как это затрудняет выполнение дальнейших мероприятий по взысканию кредитных задолженностей и других обязательств.

Для предотвращения искусственного повышения рыночной стоимости залогов современные аналитики и экономисты предлагают ввести определенные ограничения на некоторые параметры оценочных расчетов. Оценщику сегодня необходимо более взвешенно и ответственно относиться к выявлению величины прибыли, дисконтированию денежных потоков и использованию ставки капитализации. Таким образом, можно повысить прозрачность полученных в отчете значений о стоимости залога на весь срок кредитования.

В целом, для поддержания высокого уровня финансовой безопасности в настоящее время рекомендуется при проведении оценки залогов для банка оперировать общепринятыми оценочными методами без увеличения стоимости объекта оценки, и непременно учитывать вероятность взыскания предмета залога, то есть его ликвидность, при невыполнении заемщиком своих обязательств.

СОДЕРЖАНИЕ

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ЭКСТРЕМИЗМ КАК ОДНА ИЗ УГРОЗ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ 4
Инкина А.Н.
«ПОТРЕБИТЕЛЬСКИЙ ЭКСТРЕМИЗМ» ИЛИ ЗЛОУПОТРЕБЛЕНИЕ ПРАВАМИ ПОТРЕБИТЕЛЯ 6
Подсеваткин В.С.
ПРАВОВОЕ РЕГУЛИРОВАНИЕ СУРРОГАТНОГО МАТЕРИНСТВА В РФ 8
Сочнев А.В.
СТ. 205.6 УК РФ КАК ГАРАНТИЯ БЕЗОПАСНОСТИ ГРАЖДАН РОССИИ: ЕЁ ПЛЮСЫ И МИНУСЫ 10
Учкин Т.А.
ТЕРРОРИЗМ КАК ГЛОБАЛЬНАЯ ПРОБЛЕМА ЧЕЛОВЕЧЕСТВА 12
Щеколдина О.А.
ОЦЕНКА СОЦИАЛЬНОЙ ТЕРПИМОСТИ (НЕТЕРПИМОСТИ) В ВУЗЕ (отчет по результатам НИРС юридического факультета Волжского университета имени В.Н. Татищева) 13
Алексеева А.М., Белова М.В., Ванькина И.А., Вдовкина Ю.С., Горбунова Т.А., Григорян Г.Г., Диасамидзе Л.Т., Дунин К.Ю., Иванов Г.Ю., Козубова Н.С., Коробкина Е.А., Краснобаев Н.И., Малолеткова Ю.В., Маркушина К.И., Медведев С.Е., Подсеваткин В.С., Пономарева Т.В., Савельева Е.А., Салейкин Н.Ю., Серебрянников В.И., Сочнев А.В., Строган О.А., Сутковой Г.О., Томшивер А.Я., Ульянов А.О., Федорова О.Ю., Ясакова Ю.В., Яшина Е.П.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПАНИИ ПРИ ИСПОЛЬЗОВАНИИ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ УДАЛЕННОГО ДОСТУПА СОТРУДНИКОВ К КОРПОРАТИВНОЙ СЕТИ 37
Андреев А.А.
ОСНОВНЫЕ ПОДХОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ 39
Аникеев В.М., Гуренков Е.В.
КЛАССИФИКАЦИЯ СОВРЕМЕННЫХ БИОМЕТРИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 42
Беляев П.С., Желтяков О.В.
СЕТЕВОЙ ПРОТОКОЛ SSH 45
Васильев Е.С.
ЗАКОНОДАТЕЛЬНОЕ ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ТЕРРОРИСТИЧЕСКИХ МАТЕРИАЛОВ В ИНТЕРНЕТЕ 47
Винокуров М.Ю.
ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ СВЯЗИ 48
Вяткин А.С., Юрцев Д.В.
ИСПОЛЬЗОВАНИЕ ПРОГРАММНО-МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ КАК ОРУЖИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ 53
Гужвенко В.Ю.
ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ 55
Евтеев А.В., студент, Плюснина Е.В.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЁ ОБЕСПЕЧЕНИЕ 59
Завьялов Д.Л.
УГРОЗЫ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ 65
Иванова А.В.
АНАЛИЗ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ДАННЫМ 66
Кошелева К.А.

СТРУКТУРА ГОСУДАРСТВЕННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ 69
Мустафаева С., Малкина С.
СПОСОБЫ РЕАЛИЗАЦИИ СТЕГАНОГРАФИИ 72
Пронин В.А.
ПРОБЛЕМЫ ЭКСПЕРТИЗЫ ИНФОРМАЦИОННЫХ МАТЕРИАЛОВ, СОДЕРЖАЩИХ ПРИЗНАКИ ИДЕОЛОГИИ ТЕРРОРИЗМА 74
Рожков Р.О.
ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ .. 75
Федосеев М.Ю.
ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ ВИРУСОВ 78
Калинин М.С.

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЭКОЛОГИЧЕСКИ БЕЗОПАСНОГО КОМПЛЕКСОНА ОЭДФ ДЛЯ ОПРЕДЕЛЕНИЯ МЕДИ МЕТОДОМ КОМПЛЕКСОНОМЕТРИЧЕСКОГО ТИТРОВАНИЯ 80
Глухова О.А., Вахрамеев В.В.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ПОТРЕБИТЕЛЬСКОГО КРЕДИТОВАНИЯ НАСЕЛЕНИЯ 82
Аринина Д.В.
ВЗАИМОСВЯЗЬ УСТОЙЧИВОГО РАЗВИТИЯ ГОСУДАРСТВА И ЕГО НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ 84
Безрукова Е.А, Бурундукова Д.В.
НЕДОИМКИ ПО НАЛОГАМ И СБОРАМ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 88
Ворушило Б.А., Уружбеков Р.Н.
ЗАРУБЕЖНЫЙ ОПЫТ В ОБЛАСТИ ПЕРЕРАБОТКИ ОТХОДОВ 91
Горшкова Ю.В.
ПРОБЛЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ МАЛЫХ ПРЕДПРИЯТИЙ В ОБЛАСТИ ФИНАНСОВОГО УЧЁТА И НАЛОГООБЛОЖЕНИЯ НА ПРИМЕРЕ ООО «УГЛЕРОД» 94
Данилина М.С.
«СИЛОВОЕ ДАВЛЕНИЕ» НА СРЕДНИЙ И МАЛЫЙ БИЗНЕС РОССИИ 97
Димакис М.А.
ВОЗМОЖНОСТЬ И БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ВИЧ-ИНФИЦИРОВАННЫХ ТРУДОВЫХ РЕСУРСОВ В ОРГАНИЗАЦИИ 98
Захаров И.В.
ВЗАИМОСВЯЗЬ ИМПОРТОЗАМЕЩЕНИЯ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 102
Килин А.В.
ФАКТОРЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ МАЛОГО БИЗНЕСА В РОССИИ 106
Мелёхин Д.М.
ДОСТАТОЧНОСТЬ ЗАЛОГА КАК ФАКТОР ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО БАНКА 107
Рогачева Т.Л.

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск девятый

Компьютерная верстка и дизайн И.А. Чиргадзе

Сдано в набор 14.12.2016.
Подписано к печати 16.12.2016.
Формат 60x84/16. Бумага офсетная.
Гарнитура Times ET.
Печать оперативная. Усл. п.л. 7,0. Уч.-изд. л. 6,5.
Тираж 25 экз. Заказ № 219.