Волжский университет имени В.Н. Татищева

ВЕСТНИК ПО БЕЗОПАСНОСТИ

№12 декабрь 2019

В НОМЕРЕ:

ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск двенадцатый

Тольятти 2019

УДК: 004+007+009+070+34+33+502/504+556+57/58+80/82+882
ББК: 004.00+20.1+32+33.00+34.00+57.00+65+67+76+80/84

Материалы Всероссийской научно-практической конференции по безопасности. Вестник по безопасности. Выпуск двенадцатый. – Тольятти: ВУиТ, 2019. - 128 с.

20-21 декабря 2019 года в Волжском университете имени В.Н. Татищева состоялась Всероссийская научно-практическая конференция по безопасности.

В настоящем издании публикуются материалы участников конференции.

Все материалы представлены в авторской редакции.

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

ПРАВОВАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ ИНТЕГРИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОРГАНАХ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Желюк П.С., студент
Научный руководитель: Пынчук В.А., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

В условиях стремительного нарастания информационного потока функционирование государственного надзорного органа невозможно без четкого налаживания процедур документационного обеспечения управления. Поэтому органами прокуратуры Российской Федерации ведется работа по развитию электронного документооборота и, соответственно, правовое обеспечение данного процесса, в первую очередь, обеспечение его безопасности [1]. Принимая во внимание опыт зарубежных стран, таких как Финляндия, США, Великобритания и Германия, в использовании технологий безбумажного документооборота в государственных органах уголовной юстиции, в России принята стратегия развития отрасли информационных технологий на 2014-2020 гг. и на перспективу до 2025 года [3]. Развитие безопасного электронного документооборота названо одной из основных задач совершенствования отрасли информационных технологий России.

Законодательство Российской Федерации в целом регулирует осуществление делопроизводства в органах прокуратуры. Приняты законодательные и иные нормативные акты, с помощью которых урегулированы вопросы создания и использования электронных документов наряду с созданием документов на бумажном носителе, а также вопросы безопасности доступа к информации, эксплуатации информационных систем, использования электронных документов и электронной подписи. Электронный документооборот несомненно имеет ряд преимуществ, среди которых можно выделить: упрощение порядка взаимодействия между структурными подразделениями и ведомствами; снижение рутинного труда при оформлении документов на бумаге; безопасность электронных документов выше, чем у документов на бумажном носителе, так как цифровая подпись, в отличие от обычной, заверяет не носитель (бумагу), а само содержание документа, то есть данные, информацию; сокращение времени прохождения обращений до исполнителя; сокращение издержек; применение и использование имеющихся технических средств, а также использование электронного документооборота в целом влияет на развитие экономики государства. Но электронный документооборот требует соответствующего уровня развития и использования инновационных информационных технологий, а также обеспечения безопасности данных в связи с переходом на безбумажную форму документооборота в органах прокуратуры Российской Федерации [7].

В настоящее время идет активный процесс формирования единой платформы электронного документооборота и взаимодействия в органах прокуратуры РФ. Программное обеспечение, которое уже существует, прежде всего автоматизированный информационный комплекс «Надзор» [5], созданный для оптимизации и систематизации делопроизводственной и надзорной деятельности, морально и функционально устарел, в том числе, в силу отсутствия некоторых необходимых функциональных возможностей.

Органы прокуратуры Российской Федерации в том числе призваны обеспечить информационную безопасность в области государственной безопасности [2]. Фактически текущее состояние безопасности информационных систем служебных процессов прокуратуры требует не только внедрения новых средств их автоматизации, но и комплексной цифровой трансформации. В целях компетентного и оперативного решения данной проблемы органы прокуратуры Российской Федерации первыми из силовых ведомств вошли в государственную программу

«Цифровая экономика» [4]. Органы прокуратуры всех уровней объединены посредством ЕЗСПД (единая защищенная сеть передачи данных), создается суперсервис «Подача заявлений в правоохранительные органы онлайн», внедрена система непрерывного повышения квалификации работников надзорного ведомства по использованию новейших информационных технологий защиты информации в практической деятельности в системе Интернет и работе с большими данными, совершенствуется федеральная государственная информационная система «Единый реестр проверок» и государственная автоматизированная система правовой статистики.

Принятые меры позволят в значительной мере перевести большую часть документооборота из бумажной формы в электронную и повысить эффективность деятельности органов прокуратуры в сфере защиты информации. Система электронного документооборота будет способна наиболее полно и оперативно удовлетворять информационные потребности функционирования органов прокуратуры всех уровней, а также создаст условия для удобного и прозрачного взаимодействия с прокуратурой граждан и общества.

Для реализации целей цифровой трансформации электронного документооборота в органах прокуратуры РФ в ряду приоритетных направлений установлено обеспечение защищенного информационного взаимодействия органов прокуратуры всех уровней между собой, а также с автоматизированными информационными системами и базами данных, которые созданы в других органах государственной власти и ведомствах; разработка системы управления нормативно-справочной информации, требований в архитектуре и стандартам построения цифровой платформы системы электронного документооборота органов прокуратуры.

Учитывая развитие законодательства, которое регулирует перевод документооборота в электронную форму в органах и организациях прокуратуры РФ, а также права, обязанности, ответственность всех участников информационного взаимодействия и совершенствования профессиональных навыков работников прокуратуры в рамках выполнения должностных обязанностей можно выделить следующие общие тенденции: совершенствование систем электронного документооборота; востребованность электронной подписи с разным уровнем защиты; изменение программно-аппаратной среды документационного обеспечения деятельности надзорного органа. При этом необходимо провести мероприятия по разработке нормативно-правовой базы регулирования вопросов цифровой трансформации и информационной безопасности делопроизводства органов и организаций прокуратуры [6].

Кроме того, комплексная оптимизация деятельности ведомства, в частности, формирование среды электронного взаимодействия, преимущественное использование данных в цифровой форме, развитие цифровой инфраструктуры и формирование новой технологической основы деятельности органов прокуратуры будет основываться на российских технологиях, что, в свою очередь, серьезно повысит уровень защиты информации системы ведомственного делопроизводства.

Библиографический список

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС «Консультант Плюс» (дата обращения 10.11.2019).

2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности в Российской Федерации» // СПС «Консультант Плюс» (дата обращения 10.11.2019).

3. Распоряжение Правительства РФ «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 — 2020 годы и на перспективу до 2025 года» от 01.11. 2013 № 2036-р // СПС «Консультант Плюс» (дата обращения 10.11.2019).

4. Паспорт национальной программы «Цифровая экономика Российской Федерации»: утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16 // СПС «Консультант Плюс»

(дата обращения 10.11.2019).

5. Приказ Генеральной прокуратуры РФ от 29.12.2011 г. № 450 «О введении в действие Инструкции по делопроизводству в органах и учреждениях прокуратуры Российской Федерации» // СПС «Консультант Плюс» (дата обращения 10.11.2019).

6. Приказ Генеральной прокуратуры РФ от 14.09.2017 г. № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // СПС «Консультант Плюс» (дата обращения 10.11.2019).

7. Кудряшов, Е.Ю., Мышко, Ф.Г. Основные аспекты развития системы электронного документооборота в органах прокуратуры Российской Федерации / Е.Ю. Кудряшов, Ф.Г. Мышко // Государственная служба и кадры. - 2019. - № 1. - С. 161-163.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ОХРАНЫ ОКРУЖАЮЩЕЙ СРЕДЫ

Журавлева Д., студент
Научный руководитель: Галеева Г.Р., к. ю. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Глобальные экологические проблемы, влияние которых на развитие земной цивилизации в целом и каждого государства в отдельности постепенно осознано подавляющим большинством населения планеты, обусловливают необходимость укрепления международного сотрудничества в области охраны окружающей среды. В этих условиях происходит формирование международного экологического права как одного из инструментов решения таких проблем и формы реализации международного сотрудничества.

Международное экологическое право возникло во второй половине XX столетия как закономерная реакция международного сообщества на глобальные экологические проблемы - загрязнение атмосферного воздуха, вызывающее трансграничные последствия, опасные изменения климата, связанные с выбросами парниковых газов и сокращением лесов, особенно тропических, разрушение озонового слоя, загрязнение морей и континентальных трансграничных вод, деградация животного и растительного мира, сокращение биологического разнообразия на Земле и др.

В последней четверти XX в. в условиях экологического кризиса, охватившего всю планету, объективной необходимостью стало международное сотрудничество в области природопользования и охраны окружающей природной среды.

Такая потребность вызвана:

- глобальным (общепланетарным) характером многих экологических проблем (например, сохранение озонового слоя);
- трансграничным переносом загрязняющих окружающую природную среду веществ воздушными течениями, круговоротом воды, биологической миграцией по трофическим цепям;
- международным статусом природных систем и объектов (Мировой океан, воздушный бассейн Земли, околоземное космическое пространство, Антарктида);
- невозможностью решить все проблемы организации рационального природопользования и охраны окружающей природной среды силами одной страны.

Таким образом, важнейшим направлением международного сотрудничества является международная правовая охрана окружающей среды, а основным инструментом – международное экологическое право, т.е. система правовых норм, регулирующих межгосударственные отношения, политику мирового сообщества в области охраны окружающей среды, обеспечения экологической безопасности и устойчивого социально-

экономического развития общества.

Конституция РФ закрепляет общепризнанные принципы и нормы международного права и международные договоры РФ в качестве составного элемента ее правовой системы, устанавливая приоритет норм международного права над национальным правом. Данное положение находит свое отражение и в законодательстве об охране окружающей среды. Так, ст. 82 Федерального закона «Об охране окружающей среды» установлено, что в случае противоречия международного договора РФ в области охраны окружающей среды нормам указанного федерального закона применяются правила, установленные международным договором. Закрепление данного положения в национальном законодательстве является неотъемлемым элементом функционирования правового государства.

Ведущую роль источников играют международные договоры (конвенции, соглашения). В зависимости от содержания можно выделить:

- договоры политического характера;
- договоры непосредственно экологического характера.

Международные договоры играют важную роль в правовом регулировании экологических отношений в стране. В соответствии со ст.15 Конституции РФ общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора. Российская Федерация является участницей более 80 многосторонних экологических договоров, которые согласно упомянутой статье не только являются источниками экологического права, но и обладают верховенством по отношению к российскому законодательству. Международный договор может применяться прямо для регулирования экологических и иных отношений, в том числе для рассмотрения судами гражданских, уголовных или административных дел, за исключением случаев, когда для его реализации требуется принятие внутригосударственного акта

В международных договорах политического характера вопросы природопользования и охраны окружающей среды рассматриваются наряду с вопросами мира, безопасности и т.п. Центральное место в данной группе договоров занимает Заключительный акт Совещания по безопасности и сотрудничеству в Европе 1975 г. Данный правовой акт провозглашает приоритет международного сотрудничества в сфере охраны окружающей среды, а также закрепляет основные области, формы и методы такого сотрудничества.

Международные договоры непосредственно экологического характера полностью посвящены вопросам правового регулирования природопользования и охраны окружающей среды. Договоры, относящиеся к данной группе, подразделяются на:

- международные договоры эколого-комплексного направления;
- международные договоры эколого-ресурсного направления.

Среди договоров эколого-комплексного направления можно выделить Договор об Антарктике 1959 г. (с Протоколом от 4 октября 1991 г.).

Необходимо отметить, что с момента начала межгосударственного экологического сотрудничества страны-участники международного сообщества проявляют особый интерес к вопросу обеспечения экологической безопасности. Решению именно этого вопроса были посвящены первые соглашения, затрагивающие проблемы окружающей среды.

Подводя итог вышесказанному, можно сделать вывод, что регулирование экологических отношений между государствами и другими субъектами международного права пока характеризуется довольно высокой степенью фрагментарности и отсутствием системного подхода. В этой области пока нет единого кодифицирующего акта, хотя попытки по его подготовке предпринимаются. В нормотворческой деятельности доминирует пообъектный подход, когда принимаются соглашения, направленные на охрану и использование отдельных природных объектов - животного мира, вод, атмосферного воздуха и др. В некоторых случаях пообъектное регулирование уже достигло высокого уровня

развития. Особенно это касается охраны животного мира, где проведена кодификация в рамках Конвенции ООН о биоразнообразии. За последнее время принят ряд соглашений, направленных на комплексное решение отдельных экологических проблем, например проблемы опасных отходов, а также устанавливающих требования для источников экологически вредной деятельности.

ПОНЯТИЕ И СУЩНОСТЬ СТРАХОВАНИЯ ГРАЖДАНСКОЙ ОТВЕТСТВЕННОСТИ ВЛАДЕЛЬЦЕВ АВТОТРАНСПОРТНЫХ СРЕДСТВ

Казаков А.А., студент
Научный руководитель: Галеева Г.Р., к. ю. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Прежде чем приступить к раскрытию дефиниции Обязательного страхования автотранспортных средств, следует сказать несколько слов о самом понятии страхования.

Если обратиться к грамматическому толкованию понятия «страхования», то, в Толковом Словаре С.И. Ожегова оно понимается, как «…предохранение от чего-либо нежелательного»[1] или во втором своём значении - «…обеспечение от возможного ущерба путём периодических взносов специальному учреждению, которое выплачивает денежное возмещение в случае такого ущерба…»[2].

Нормативное толкование данного понятия будет следующим:

В самом Гражданском Кодексе Российской Федерации, в главе 48, которая затрагивает отношения по страхованию, мы не сможем найти чёткой дефиниции, которая бы отражала смысл данного вида правоотношений.

Однако в науке гражданского права сложилось множество точек зрения, которые позволяют определить понятие страхования с разных сторон. К примеру, С.А. Суханов рассматривал страхование как экономическую категорию – «…механизм, основанный на принципе распределения (разложения, расклада) убытка, понесенного в одном случае, между некоторым множеством других, которые подвержены аналогичной (однородной) опасности. Обеспечивая таким образом восстановление имущественной сферы отдельного (частного) хозяйства или определенного лица, а тем самым гарантируя и их экономические интересы….»[3].

Е.Н. Пименова определяет страхование – как многоаспектную категорию, и делит её на три подвида: «…Страхование – социально-экономический институт, суть которого заключается в защите имущественных интересов граждан, предприятий, учреждений; смягчении негативных последствий случайных событий, путём разложения тяжести данных последствий на многие единицы, которым угрожают данные события; организация за счет уплачиваемых гражданами страховых взносов, страховых фондов, предназначенных для возмещения убытков и выплаты страховых сумм при наступлении страхового случая.

Страхование – научная дисциплина, которая охватывает вопросы экономики страхового дела.

Страхование – объект воздействия нормотворческой деятельности государства, объект правового регулирования…»[4].

Отсюда следует, что дефиниция страхование – многогранная, но, если говорить о страховании автотранспортных средств, то оно будет иметь более узкий смысл, так как данный вид страхования может применяться только к отдельным категориям лиц –

[1] Ожегов С.И. Словарь русского языка: Ок 57000 слов / Под ред. чл.- корр. АН СССР Н.Ю. Шведовой - 18-е изд., стереотип. [Текст] / С.И. Ожегов – М.: Рус. яз, 1986 - С. 671.

[2] Там же. С. 671.

[3] http://jurisprudence.club/pravo-grajdanskoe/strahovanie-kak-ekonomicheskaya.html

[4] Пименова Е.Н. Страховое право. Учебное пособие. [Электронный ресурс] – Режим доступа: http://thelib.ru/books/elena_nikolaevna_ pimenova/ strahovoe_pravo_uchebnoe_posobie-read-2.html#n_14

автомобилистам. Помимо понятия необходимо обратиться к сущности страхования в целом.

Для понимания его значения следует отметить, что «…С вступлением в силу Федерального Закона от 25.04.2002 № 40-ФЗ страхование гражданской ответственности стало обязательным для всех автовладельцев. До издания этого закона заключение договора зависело только от усмотрения сторон. Отношения по страхованию гражданской ответственности владельцев транспортных средств оформляются договором по которому страховщик обязуется за обусловленную договором плату (страховую премию) при наступлении предусмотренного в договоре события (страхового случая) возместить потерпевшим причинённый вследствие этого события вред их жизни, здоровью или имуществу, т.е. (осуществить страховую выплату) в пределах определённой договором суммы (страховой суммы)…»[1].

Как справедливо отмечает С.Е. Герштейн в своей работе «Административно-правовое регулирование обязательного страхования гражданской ответственности владельцев транспортных средств как меры обеспечения безопасности в сфере дорожного движения»[2], «…сущность обязательного страхования ответственности владельцев транспортных средств определяется совокупностью его признаков, к которым относятся: обязательный характер; отсутствие автономии воли сторон при определении условий страхования; ответственность за невыполнение обязанности владельца транспортного средства по обязательному страхованию гражданской ответственности; непосредственная связь с владением и управлением транспортным средством, являющимся источником повышенной опасности; направленность на обеспечение безопасности в сфере дорожного движения…»[3]. Все данные признаки тесно взаимосвязаны, и не могут существовать по отдельности друг от друга. Их следует раскрыть:

1) Обязательный характер. Признак закреплён в статье 4 ФЗ «Об обязательном страховании гражданской ответственности владельцев транспортных средств»[4], который означает, что ущерб причинённый водителям, пассажирам, пешеходам и иным участникам движения будет возмещён, что является следствием гарантии компенсации вреда.

2) Отсутствие автономии воли сторон при определении условий страхования.

Автономия воли сторон – это возможность для сторон устанавливать, по своему усмотрению содержание договора, его условия в пределах, установленных правом, свободное волеизъявление сторон, вступление в гражданско-правовые отношения в своей воле и в своём интересе.

Данная возможность распространяется на выбор применимого права, если отношения осложнены иностранным элементом. В нашем случае, условия страхования будут определяться только российским правом и никаким больше.

3) Ответственность за невыполнение обязанности владельца транспортного средства по Обязательному Страхованию Автомобильной Гражданской Ответственности.

Согласно части 2 статьи 4 Закона, «…владелец транспортного средства обязан застраховать свою гражданскую ответственность до регистрации транспортного средства, но не позднее чем через десять дней после возникновения права владения им…»[5]. В противном случае, владелец несет административную ответственность в соответствии со статьёй 12.37 Кодекса об Административных Правонарушениях Российской Федерации: «Несоблюдение

[1] Дешалыт Л.Б. и др. О договоре обязательного страхования гражданской ответственности владельцев транспортных средств // Научно-практический журнал «Современное право». 2006, № 9 – стр.79.

[2] Диссертация Герштейн С.Е. «Административно-правовое регулирование обязательного страхования гражданской ответственности владельцев транспортных средств как меры обеспечения безопасности в сфере дорожного движения» [Электронный ресурс] – Режим доступа: http://www.susu.ru/sites/default/files/ dissertation/dissertaciya_gershteyn_s.e_0.pdf

[3] Там же. С. 10-11.

[4] Федеральный закон от 25.04.2002 N 40-ФЗ (ред. от 29.10.2019) "Об обязательном страховании гражданской ответственности владельцев транспортных средств" СПС КонсультантПлюс [Электронный ресурс] – Режим доступа: http://www.consultant.ru/ document/ cons_doc_LAW_36528/

[5] Федеральный закон от 25.04.2002 N 40-ФЗ (ред. от 29.10.2019) "Об обязательном страховании гражданской ответственности владельцев транспортных средств" СПС КонсультантПлюс .

требований об обязательном страховании гражданской ответственности владельцев транспортных средств»

4) Непосредственная связь с владением и управлением транспортным средством, являющимся источником повышенной опасности.

ОСАГО будет являться охранительным институтом в случае причинения ущерба самому автомобилисту-собственнику, в результате неправомерного завладения его автомобилем (угон), а также в случае дорожно-транспортного происшествия самим автовладельцем с другими участниками движения.

5) Направленность на обеспечение безопасности в сфере дорожного движения.

Каждый из данных принципов является неотъемлемой частью сущности ОСАГО, которая в свою очередь является его своеобразным фундаментом.

Библиографический список

1. Ожегов, С.И. Словарь русского языка: Ок 57000 слов / Под ред. чл.- корр. АН СССР Н.Ю. Шведовой - 18-е изд., стереотип. [Текст] / С.И. Ожегов – М.: Рус. яз, 1986.

2. Страхование как экономическая категория. [Электронный ресурс] – Режим доступа: http://jurisprudence.club/pravo-grajdanskoe/strahovanie-kak-ekonomicheskaya.html

3. Пименова, Е.Н. Страховое право. Учебное пособие. [Электронный ресурс] – Режим доступа: http://thelib.ru/books/ elena_nikolaevna_pimenova/strahovoe_pravo_uchebnoe_posobie-read-2.html#n_14

4. Дешалыт, Л.Б. и др. О договоре обязательного страхования гражданской ответственности владельцев транспортных средств // Научно-практический журнал «Современное право». 2006, № 9 – стр.79.

5. Герштейн, С.Е. «Административно-правовое регулирование обязательного страхования гражданской ответственности владельцев транспортных средств как меры обеспечения безопасности в сфере дорожного движения» / дис. … канд. юрид. наук. [Электронный ресурс] – Режим доступа: http://www.susu.ru/sites/default/files/dissertation/ dissertaciya_gershteyn_s.e_0.pdf

6. Федеральный закон от 25.04.2002 N 40-ФЗ (ред. от 29.10.2019) «Об обязательном страховании гражданской ответственности владельцев транспортных средств» СПС КонсультантПлюс.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРЕДПРИНИМАТЕЛЬСТВА КАК МЕРЫ ПОВЫШЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Карпенко И.И., студент
Научный руководитель: Сыропятова С.Б., к. э. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Сложность реализации вопросов национальной безопасности заключается, в первую очередь, в регулировании и контроле за деятельностью хозяйствующих субъектов, в том числе, и лицами, осуществляющими предпринимательскую деятельность.

Законы, регулирующие предпринимательскую деятельность, многочисленны, в связи с чем их исчерпывающее перечисление затруднительно и нецелесообразно. Поэтому определим в качестве критерия классификации сферу предпринимательства и группу вопросов, подлежащих регулированию.

К первой группе отнесем законы, устанавливающие требования к осуществлению предпринимательской деятельности, например, Конституция, ГК, ТК, НК «О государственной регистрации юридических лиц и индивидуальных предпринимателей», «О предпринимательской деятельности».

Ко второй группе - законы, регулирующие правовое положение участников предпринимательской деятельности и их объединений, например, «Об обществах с

ограниченной ответственностью», «О производственных кооперативах», др.

В третью, отдельную группу следует определить законы, регулирующие отдельные виды предпринимательской деятельности, например, «О рекламе», «Об аудиторской деятельности», «Об организации страхового дела в РФ»

Осуществление любой законной предпринимательской деятельности сопровождается заключением гражданско-правового договора. Поэтому, данный аспект должен, с одной стороны, четко регулироваться законодательством, с другой – предоставлять возможность выбора.

Гражданский Кодекс РФ является основным источником, регулирующим отношения между лицами, осуществляющими предпринимательскую деятельность, или с их участием, исходя из того, что предпринимательской является самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке.

Он определяет, что «гражданин вправе заниматься предпринимательской деятельностью без образования юридического лица с момента государственной регистрации в качестве индивидуального предпринимателя».

Один из важнейших вопросов безопасности бизнеса – договорные отношения, также регулируется гражданским кодексом РФ. Для повышения уровня безопасности, при заключении договором необходимо проверить информацию о полномочиях представителя юридического лица. Как известно, вопрос о полномочиях руководителя (представителя) юридического лица определяется его уставом либо другим документом, аналогичным уставу. Так вот, во всех случаях при подписании любого договора следует изучить Устав своего контрагента.

Все дело в том, что многие общества (ООО, ЗАО, ОАО и т.д.) в своих уставах стараются ограничить полномочия руководителя, а тем более его заместителя, по совершению сделок. Так, например, в текст своих уставов такие общества записывают «трафаретные» пункты примерно следующего содержания: «Генеральный директор вправе единолично, без согласия других участников общества подписывать договоры по совершению сделок на сумму, не превышающую 300000 деноминированных рублей. Для подписания сделки на сумму более 300000 рублей генеральный директор обязан истребовать письменное разрешение не менее двух участников общества. Сделка, совершенная генеральным директором с превышением указанных полномочий, т.е. без письменного согласия двух участников общества, признается недействительной».

Законодатель «сконструировал» правовые нормы о юридических лицах таким образом, что предоставил возможность учредителям (соучредителям) в своих уставах самим решать вопрос об объеме полномочий и компетенции руководителя исполнительного органа.

Перед подписанием договора следует также проверить, вправе ли ваш партнер заниматься определенным видом деятельности, если он выступает в роли определенного исполнителя (продавца, изготовителя, подрядчика, перевозчика и т.п.), в тексте заключаемого договора следует также зафиксировать серию, номер и дату выдачи лицензии.

Стадия подписания договора как заключительная стадия оформления договора представляется самой важной стадией потому, что является законоутверждающей. Однако может таить множество неожиданностей. Рассмотрим их.

Как правило, подписание договора включает в себя собственноручную подпись первого лица предприятия или его полномочного представителя, а также оттиск печати этой организации. Печать на договоре - подтверждение полномочий лица, подписавшего договор. Наличие печати на договоре, подписанном неполномочным лицом, не делает договор действительным, в то время как отсутствие печати на подписи полномочного лица однозначно свидетельствует о заключении договора.

Существуют неписаные правила о факторах, которые могут существенно повлиять на содержание и сущность заключаемого договора:

1) подписи сторон должны быть сделаны полно и разборчиво, «крестики» и

«закорючки» на договоре в случае, если ваш контрагент оспорит свою подпись, могут повлечь за собой то, что судебная экспертиза не сможет дать однозначного ответа об авторстве подписи, и это может существенно вам помешать;

2) никогда не подписывайте чистых бланков, поскольку такими «чистыми» бумагами могут воспользоваться нечестные люди, если эти документы будут случайно потеряны;

3) после подписания договора, ни при каких обстоятельствах не отдавайте ваш подлинный экземпляр договора вашему контрагенту или иным посторонним лицам. Лучше всего снимите на ксероксе копию подлинного договора и в текущей работе пользуйтесь только ею. Подлинный экземпляр договора, во избежание возможной потери или хищения, лучше положить в сейф и использовать этот документ только в действительно необходимых случаях;

4) если текст договора составляет несколько страниц, необходимо их прошить, заклеить и удостоверить подписями и печатями сторон. Некоторые предприниматели используют и другой, также эффективный способ - они подписывают каждую страницу договора. Данное обстоятельство в случае спора может оградить вас от заявлений недобросовестного партнера, что "этот лист договора он в глаза не видел";

5) может случиться так, что ваш контрагент вдруг заявит, что при подписании договора его обманули, ввели в заблуждение, "подсунули" для подписания не тот экземпляр договора и т.д. Поэтому можно рекомендовать вам сохранять проекты договора с собственноручными исправлениями, замечаниями и вставками другой стороны. Такой документ в арбитражном суде может служить доказательством того, что ваш контрагент при заключении сделки вовсе ни в чем не заблуждался, а действовал разумно и обдуманно.

Для противодействия угрозам в сфере национальной безопасности необходимо создание и функционирование системы обеспечения региональной безопасности, которая образуется органами законодательной, исполнительной и судебной властей субъектов РФ, государственными, общественными и иными организациями и объединениями, гражданами, принимающими участие в обеспечении безопасности в соответствии с законом, а также законодательством, регламентирующим отношения в сфере региональной безопасности.

Библиографический список

1. Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 18.07.2019) (с изм. и доп., вступ. в силу с 01.10.2019).

2. Ахметова, И.Н. Риски в предпринимательской деятельности: юридические аспекты // Безопасность бизнеса. 2019. N 4. С. 11 - 16.

3. Право и экономическое развитие: проблемы государственного регулирования экономики: монография / В.К. Андреев, Л.В. Андреева, К.М. Арсланов и др.; отв. ред. В.А. Вайпан, М.А. Егорова. М.: Юстицинформ, 2017. 432 с.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ АТМОСФЕРНОГО ВОЗДУХА В ЗАКОНОДАТЕЛЬСТВЕ РОССИИ

Сергина Я.А., студент
Научный руководитель: Галеева Г.Р., к. ю. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти
Карлов В.В., магистрант
Санкт-Петербургский государственный университет
г. Санкт-Петербург

Согласно ст. 1 «Закона об охране атмосферного воздуха», под атмосферным воздухом понимается жизненно важный компонент окружающей среды, представляющий собой

естественную смесь газов атмосферы, находящуюся за пределами жилых, производственных и иных помещений[1].

Охрана атмосферного воздуха представляет собой систему мер, осуществляемых органами государственной власти РФ, органами государственной власти субъектов РФ, органами местного самоуправления, физическими и юридическими лицами в целях улучшения качества атмосферного воздуха и предотвращения его вредного воздействия на здоровье человека и окружающую природную среду.

Говоря о качестве атмосферного воздуха, отметим, что это совокупность физических, химических и биологических свойств атмосферного воздуха, отражающих степень его соответствия гигиеническим и экологическим нормативам качества атмосферного воздуха[2].

К сожалению, атмосферный воздух в большинстве городов России содержит вредные (загрязняющие) вещества, химические или биологические вещества, либо смесь таких веществ, которые содержатся в воздухе. Загрязнение атмосферного воздуха зависит от поступления в атмосферу или образования в нем вредных (загрязняющих) веществ в концентрациях, превышающих установленные государством гигиенические и экологические нормативы качества атмосферного воздуха. Кроме того, технический норматив выброса вредного (загрязняющего) вещества в атмосферный воздух устанавливается для передвижных и стационарных источников выбросов, технологических процессов, оборудования. Он отражает максимально допустимую массу выброса вредного (загрязняющего) вещества в расчете на единицу продукции, мощности, пробега транспортных или иных передвижных средств и другие показатели.

С учетом этого технического норматива, а также фонового загрязнения воздуха устанавливается норматив предельно допустимого выброса вредного (загрязняющего) вещества в атмосферу для стационарного источника загрязнения воздуха. Этот норматив устанавливается территориальными органами специально уполномоченного федерального органа исполнительной власти в области охраны атмосферного воздуха для конкретного стационарного источника выбросов вредных (загрязняющих) веществ в атмосферный воздух.

Закон «Об охране атмосферного воздуха» ввел понятие временно согласованного выброса, который представляет собой временный лимит выброса вредного (загрязняющего) вещества в атмосферу.

Кроме химического загрязнения атмосферного воздуха выделяют вредное физическое воздействие, под которым подразумевают воздействие шума, вибрации, ионизирующего излучения, температурного и других физических факторов, изменяющих температурные, энергетические, волновые, радиационные и другие физические свойства атмосферного воздуха, на здоровье человека и окружающую среду.

Согласно ст. 14 «Закона об охране атмосферного воздуха», выброс вредных (загрязняющих) веществ в атмосферный воздух стационарным источником допускается на основании разрешения, выданного специально уполномоченным государственным органом. При этом разрешением на выброс таких веществ в атмосферный воздух устанавливаются предельно допустимые выбросы и другие условия, которые обеспечивают охрану атмосферного воздуха. Вредные физические воздействия на атмосферный воздух также допускаются на основании разрешений.

В соответствии со ст. 21 Закона об охране атмосферного воздуха, юридические лица, имеющие источники выбросов вредных (загрязняющих) веществ в атмосферный воздух и источники вредных воздействий на атмосферный воздух, а также количество и состав выбросов вредных (загрязняющих) веществ в атмосферный воздух, виды и размеры вредных физических воздействий на него подлежат государственному учету.

Статья 24 Закона об охране атмосферного воздуха устанавливает, что государственный контроль за охраной атмосферного воздуха призван обеспечить соблюдение: условий,

[1] Федеральный закон "Об охране атмосферного воздуха" от 04.05.1999 N 96-ФЗ (от 26.07.2019 N 195-ФЗ).

[2] Статья 11 Федеральный закон "Об охране атмосферного воздуха" от 04.05.1999 N 96-ФЗ (от 26.07.2019 N 195-ФЗ).

установленных разрешениями на выбросы вредных (загрязняющих) веществ в атмосферный воздух и на вредные физические воздействия на него; стандартов, нормативов, правил и иных требований охраны атмосферного воздуха, в том числе проведения производственного контроля за охраной атмосферного воздуха; режима санитарно-защитных зон объектов, имеющих стационарные источники выбросов вредных (загрязняющих) веществ в атмосферный воздух.

Регламентация контрольных действий специально уполномоченных государственных органов изложена в Положении о государственном контроле за охраной атмосферного воздуха, утвержденном постановлением Правительства РФ от 15.01.2001 № 31[1], а также в постановлении Правительства РФ от 28.11.2002 № 847 «О порядке ограничения, приостановления или прекращения выбросов вредных (загрязняющих) веществ в атмосферный воздух и вредных физических воздействий на атмосферный воздух»[5].

Государственное управление в области охраны атмосферного воздуха согласно ст. 4 Закона об охране атмосферного воздуха осуществляется Правительством РФ непосредственно или через специально уполномоченный федеральный орган исполнительной власти (Ростехнадзор), а также органами исполнительной власти субъектов РФ. Принципами государственного управления в рассматриваемой сфере являются, в том числе:

недопущение необратимых последствий загрязнения атмосферного воздуха для окружающей среды;

обязательность государственного регулирования выбросов вредных (загрязняющих) веществ в атмосферный воздух и вредных физических воздействий на него;

гласность, полнота и достоверность информации о состоянии атмосферного воздуха, его загрязнении;

научная обоснованность, системность и комплексность подхода к охране атмосферного воздуха и охране окружающей среды в целом;

обязательность соблюдения требований федерального законодательства в области охраны атмосферного воздуха, ответственность за его нарушение.

Глава 3 Закона об охране атмосферного воздуха устанавливает требования к охране атмосферного воздуха, среди которых следует выделить:

запрет на внедрение новых техники, технологий, материалов, веществ и другой продукции, а также на применение технологического оборудования и других технических средств, если они не отвечают установленным законодательством требованиям охраны атмосферного воздуха;

обязательность при производстве и использовании топлива наличия сертификатов, подтверждающих соответствие топлива требованиям охраны атмосферного воздуха;

запрет на выброс в атмосферный воздух веществ, степень опасности которых для жизни и здоровья человека и для окружающей среды не установлена;

допустимость действий, направленных на изменение состояния атмосферного воздуха и атмосферных явлений только при отсутствии вредных последствий для жизни и здоровья человека и окружающей среды;

недопустимость превышения нормативов качества атмосферного воздуха при проектировании, размещении, строительстве, реконструкции и эксплуатации объектов хозяйственной и иной деятельности, при застройке городов и иных поселений;

запрет на размещение и эксплуатацию объектов хозяйственной и иной деятельности, которые не имеют предусмотренных правилами охраны атмосферного воздуха установок очистки газов и средств контроля за выбросами вредных (загрязняющих) веществ в

---

[1] Постановление Правительства РФ от 15.01.2001 N 31 (ред. от 21.04.2010) "Об утверждении Положения о государственном контроле за охраной атмосферного воздуха" // СПС «КонсультантПлюс».

[5] Постановление Правительства РФ от 28.11.2002 N 847 (ред. от 22.04.2009) "О порядке ограничения, приостановления или прекращения выбросов вредных (загрязняющих) веществ в атмосферный воздух и вредных физических воздействий на атмосферный воздух"// СПС «КонсультантПлюс».

атмосферный воздух;

запрет на производство и эксплуатацию транспортных и иных передвижных средств, содержание вредных (загрязняющих) веществ в выбросах которых превышает установленные технические нормативы выбросов;

запрет на хранение, захоронение и обезвреживание на территориях организаций и населенных пунктов загрязняющих атмосферный воздух отходов производства и потребления, в том числе дурнопахнущих веществ, а также на сжигание таких отходов без специальных установок и др.

Нарушители законодательства об охране атмосферного воздуха в зависимости от его характера могут нести дисциплинарную, материальную, гражданско-правовую, административную и уголовную ответственность.

КоАП РФ предусматривает наступление административной ответственности за:

нарушение правил охраны атмосферного воздуха (ст. 8.21);

выпуск в эксплуатацию механических транспортных средств с превышением нормативов содержания загрязняющих веществ в выбросах либо нормативов уровня шума (ст. 8.22);

эксплуатацию механических транспортных средств с превышением нормативов содержания загрязняющих веществ в выбросах либо нормативов уровня шума (ст. 8.23).

Субъектами РФ также может устанавливаться административная ответственность за нарушение законодательства об охране атмосферного воздуха.

УК предусматривает уголовную ответственность за совершение преступлений, предусмотренных ст. 251 (загрязнение атмосферы).

Рассматривая актуальную проблему загрязнения атмосферного воздуха, хочется обратить внимание и на наш родной город Тольятти. Отметим, что здесь сконцентрирована деятельность ведущих химических и нефтехимических производителей России. К сожалению, высокая производительность на должных предприятиях сопровождается выбросами отходом производства в атмосферный воздух.

Многочисленные жалобы граждан и общественных организаций почему-то игнорируются администрацией города. Прокуратура г. о. Тольятти осенью 2019 года обратилась в Центральный районный суд города, с целью привлечь к ответственности один из химических предприятий города за нарушения установленных нормативов при выброске отходов производства в атмосферный воздух.

Каждый гражданин России имеет право на благоприятную окружающую среду, атмосферный воздух является жизненно важным ее компонентом, поэтому хочется верить, что охрана окружающей среды задача не только граждан, но и ответственность юридических лиц и задача государства.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Гасс П.А., студент
Тольяттинский социально-экономический колледж
Иванов А.В., Корсаков Е.А., студенты
Волжский университет имени В.Н. Татищева
Научный руководитель: Плюснина Е.В.
г. Тольятти

Реализация мер по разработке защищенного программного обеспечения (ПО) на всех этапах жизненного цикла (SDLC - Secure Software Development Lifecycle) является предпосылкой конкурентоспособности на рынке для компаний, занимающихся разработкой ПО.

Программное обеспечение является объектом защиты из-за сложности и сложности восстановления его производительности, важности программного обеспечения для работы информационной системы.

Целью защиты программного обеспечения является:

1. Ограничение несанкционированного доступа к программам или их преднамеренного уничтожения и кражи;

2. Исключение несанкционированного копирования (репликации) программ.

Программный продукт и базы данных должны быть защищены от воздействия несколькими способами:

1. Кража человеком информации на машинные носители и программной документации; нарушение производительности программного продукта и т. д.;

2. Аппаратное соединение с компьютером для чтения программ и данных или физического их уничтожения;

3. Специализированные программы - приведение программного продукта или базы данных в нерабочее состояние (например, заражение вирусом), несанкционированное копирование программ и баз данных и т.д.

Самый простой и доступный способ защиты программных продуктов и баз данных - это ограничение доступа. Контроль доступа к программному продукту и базе данных устанавливается:

- защищать программы, когда они запускаются с паролем;
- использование ключевой дискеты для запуска программ;
- ограничения программных модулей или данных, доступных для пользователей, функций обработки и т. д.

Криптографические методы также могут использоваться для защиты информации базы данных или головных программных модулей.

Разработка защищенного программного обеспечения регламентируется ГОСТ Р 56939-2016. Этот стандарт устанавливает список и описание угроз информационной безопасности, которые могут возникнуть при разработке программного обеспечения. В целом, стандарт описывает 23 меры, каждая мера четко описывает цели, результат внедрения, а также требования к реализации меры (то есть, что именно должно быть сделано). Рассмотрим один из них:

Меры по разработке безопасного программного обеспечения, реализуемые при выполнении квалификационного тестирования программного обеспечения:

1. Функциональное тестирование программы.

2. Тестирование на проникновение.

3. Динамический анализ кода программы.

4. Фаззинг-тестирование программы.

Visual Studio позволяет контролировать безопасность запущенных приложений.

Политика безопасности - это настраиваемый набор правил, которым следует CLR при определении разрешений, предоставляемых коду. Администраторы устанавливают политику безопасности, а среда выполнения применяет ее. Среда выполнения гарантирует, что код может получить доступ только к ресурсам, разрешенным политикой безопасности, и вызвать только код, разрешенный ею.

Безопасность важна на всех этапах разработки приложений. Он начинается с анализа и выполнения правил написания безопасного кода.

Для написания эффективных приложений, нацеленных на CLR, вы должны быть знакомы со следующими принципами контроля доступа к коду.

- строго типизированный код;
- императивный и декларативный синтаксис;
- безопасные библиотеки классов;
- прозрачный код.

NET Compiler Platform SDK предоставляет инструменты для создания пользовательских предупреждений для кода C #. Анализатор содержит код, который распознает нарушения правил. Исправление файла кода содержит код, который исправляет эти нарушения.

Анализатор информирует пользователя о любых объявлениях локальных переменных, которые могут быть преобразованы в локальные константы.

Чтобы определить, можно ли изменить переменную на постоянную, вы используете синтаксический анализ, анализ константы из выражения инициализатора и анализ потока данных, чтобы убедиться, что переменная не записана. Платформа компилятора .NET предоставляет API для упрощения такого анализа. Сначала вам нужно создать новый проект анализатора C # с исправлением кода.

1.В Visual Studio последовательно выберите **Файл > Создать > Проект**, чтобы открыть диалоговое окно "Новый проект".

2.В разделе **Visual C# > Расширяемость** выберите **Analyzer with code fix (.NET Standard)** (Анализатор с исправлением кода (.NET Standard)).

3.Присвойте проекту имя и нажмите кнопку "ОК".

Анализатор с шаблоном исправления кода создаст три проекта: один, содержащий анализатор и исправление кода, второй проект модульного тестирования и третий проект VSIX.

Шаблон создает анализатор, который выдает предупреждение для каждой декларации типа, где имя типа состоит из строчных букв, как показано на рисунке 1.

```
namespace ConsoleApp1
{
    0 references
    class Program
    {
        0 references
        static void Main(string[] args)
        {
            Console.WriteLine("Hello World!");
        }
    }
}
```

Рисунок 1 – Шаблон

Шаблон также содержит исправление кода, которое заменяет любые строчные буквы в имени типа на заглавные буквы. Предлагаемые исправления можно просмотреть, щелкнув значок лампочки рядом с предупреждением. После того, как вы примете изменения, имя

типа и все ссылки на тип будут обновлены.

Расширение .NET Compiler Platform, выполняет анализ кода в режиме реального времени, находит проблемы и быстро их исправляет.

Библиографический список

1. ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования. Дата актуализации: 10.10.2019.

2. C#documentation: [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/ dot-net/csharp/

3. Крылов, Е.В. Техника разработки программ. В 2 книгах. Книга 1. Программирование на языке высокого уровня / Е.В. Крылов, В.А. Острейковский, Н.Г. Типикин. - М.: Высшая школа, 2011.

4. Крылов, Е.В. Техника разработки программ. В 2 книгах. Книга 2. Технология, надежность и качество программного обеспечения / Е.В. Крылов, В.А. Острейковский, Н.Г. Типикин. - М.: Высшая школа, 2013.

5. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

6. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

ИСПОЛЬЗОВАНИЕ СРЕДСТВ БИОМЕТРИЧЕСКОЙ ЗАЩИТЫ В ОТКРЫТЫХ СЕТЯХ

Дьяконов О.В., студент
филиал Самарского государственного технического университета
г. Сызрань
Митусов А.М., студент
Волжский университет имени В.Н. Татищева
г. Тольятти
Научный руководитель: Горбачевская Е.Н., к. п. н., доцент

Проблема идентификации личности при допуске к закрытой информации или объекту всегда была ключевой. Магнитные карты, электронные пропуска, кодированные радиосообщения можно подделать, ключи можно потерять, при особом желании даже внешность можно изменить. Но целый ряд биометрических параметров является абсолютно уникальным для человека. Биометрический принцип является одним из самых надежных способов аутентификации пользователя. Для снятия биометрических показателей необходимо использование специальных устройств, которые должны быть установлены на компьютерах высших уровней защиты. Проверка ритма работы на клавиатуре при вводе информации производится на обычной клавиатуре компьютера и по результатам проведенных в этой области экспериментов является достаточно стабильным и надежным. Даже при подглядывании за работой пользователя, набирающего ключевую фразу, не будет гарантирована идентификация злоумышленника при его попытке скопировать все действия при наборе фразы.

Признаки, делающие человека уникальным, могут быть разными.

В качестве биометрических характеристик, которые могут быть использованы при аутентификации субъекта доступа, достаточно часто применяют следующие:

- отпечатки пальцев;
- геометрическая форма рук;
- узор радужной оболочки и сетчатки глаз;
- форма и размеры лица;
- особенности голоса;
- биомеханические характеристики почерка;

- биомеханические характеристики «клавиатурного почерка».

Очень часто выбор метода зависит от длительности распознавания. Так, при большом потоке людей распознавание отпечатков пальцев удобнее сканирования радужной оболочки, которое занимает гораздо больше времени. Вместе с тем на принятие решения влияют аспекты стоимости и безопасности. Системы с высокими требованиями к безопасности, как правило, комбинируют распознавание двух признаков или одного биометрического метода и применения смарт-карт. И не последним критерием является положительное отношение пользователей.

Тому, что примерно 44% всех биометрических решений составляют системы распознавания отпечатков пальцев, есть логичное объяснение: они сканируются быстро и удобно, проверка не требует много времени и больших затрат, поэтому данный метод более охотно принимается населением. Отрасль накопила уже богатый опыт, технология довольно зрелая и хорошо принимается. На данный момент уже существуют обширные базы данных с отпечатками пальцев; кроме того, на рынке представлено множество недорогих и надежных устройств для широкого спектра применения.

Гораздо реже используется распознавание лица — лишь в 19% случаев. Обычно оно применяется вместе с проверкой фотографии в паспорте, к примеру, на пропускных пунктах на границе. Вполне вероятно, что скоро технологии сканирования лица получат значительный технологический толчок: трехмерные методы распознавания активно развиваются, и их применение должно значительно ускорить процедуры проверки.

Хотя распознавание радужной оболочки глаз считается наиболее точным методом, на него приходится лишь 7% биометрического рынка. Причина в том, что в большинстве случаев процедура проверки неприятна и довольно сложна. Так, пользователю приходится в течение секунды смотреть на источник яркого света, нагибаться или наоборот вставать на цыпочки, чтобы дотянуться до жестко закрепленного устройства. Кроме того, технология довольно дорога.

Наряду с утвердившимися методами имеются экзотические варианты, которым на биометрическом рынке отводится второстепенная роль. Распознавание геометрии ладони, сканирование глазного дна (сетчатки), распознавание голоса, ДНК или формы ушей пока еще рассматриваются как футуристические технологии. Они используются параллельно с другими системами, когда требуется обеспечить особый уровень безопасности.

Биометрические системы практически никогда не хранят непосредственные биометрические образы пользователей (например, отпечатки пальцев) и не выполняют сравнение с ними биометрических образов, предъявляемых на этапе аутентификации. Предъявляемый пользователем биометрический образ, как правило, преобразуется модулем регистрации в вектор биометрических признаков, который и обрабатывается в дальнейшем. Данный вектор содержит признаки, наиболее полно, не избыточно и уникально характеризующие предъявляемый биометрический образ. Например, в качестве одной из составляющей вектора биометрических признаков при использовании в качестве биометрической характеристики геометрической формы рук, можно использовать длины пальцев руки человека.

Одним из важнейших вопросов при проектировании биометрических систем является вопрос совмещения вектора биометрических характеристик пользователя, проходящего аутентификацию, с эталонным вектором, хранимом в базе данных эталонов.

Отличительная черта человека считается хорошей с точки зрения биометрики, если она обеспечивает получение для каждого человека набора уникальных значений измерений (измерения хорошо кластеризуются). Если схожие результаты измерений получаются для многих людей, то биометрика уязвима в плане успешности маскировки под законного пользователя.

Достаточно часто для совмещения векторов биометрических характеристик используют некоторую метрику в векторном пространстве, например, расстояние по Хэммингу или расстояние по Евклиду.

Принятие решения о прохождении либо не прохождении аутентификации пользователя принимается системой идентификации и аутентификации по результатам анализа расстояния между вектором биометрических характеристик, предъявленным пользователем, и эталонным вектором биометрических характеристик для данного пользователя. При этом очень важным является вопрос о выборе порогового расстояния, определяющего границу между легальным и нелегальным входом. Выбор порогового расстояния во многом определяет соотношение между ошибочными отказами и ошибочными подтверждениями для биометрической системы.

Главный принцип биометрических приложений довольно прост: сначала устанавливается и регистрируется личность пользователя на основе его биометрических данных, к примеру, отпечатков пальцев — этот процесс называется регистрацией. Для этого сканер проверяет приложенный палец трижды. Считанные биометрические особенности сохраняются централизованно или децентрализовано — на смарт-карте, в частности.

Затем в зависимости от установленной системы выбирается один из двух вариантов для опознания человека — идентификацию или верификацию. В первом случае, при идентификации, пользователь не сообщает свои личные сведения. После приложения пальца к специально предназначенной для этого поверхности начинается поиск аналогичного отпечатка. Эта процедура применяется для осуществления авторизованного доступа к связанным с обеспечением безопасности системам или зданиям, причем чаще всего в корпоративном секторе.

В случае верификации, напротив, пользователь сообщает идентификационную информацию при помощи смарт-карты, пароля или удостоверения. Система сопоставляет их с распознанными признаками — с тем же отпечатком пальца. Примером может послужить биометрическое удостоверение, когда система сравнивает владельца удостоверения с сохраненными на документе данными. Преимущества такого подхода заключаются в том, что он позволяет обеспечить как всеобъемлющую защиту личных данных, так и высокий уровень безопасности.

Биометрическая аутентификация к 2020 г. будет внедрена в 86% компаний в Северной Америке и Европе. Такие данные приводят аналитики ИТ-сети Spiceworks по итогам опроса 500 своих членов в этих регионах. Итоги исследования свидетельствуют о том, что 62% компаний уже внедрили такой способ аутентификации, а еще 24% придут к этому в ближайшие два года. По данным доклада «Вера в технологии», подготовленном в мае 2017 года HSBC, страны Азии и Ближнего Востока опережают Запад в вопросе внедрения биометрических технологий. Возглавляет список стран с наибольшим распространением средств биометрической идентификации Индия, жители которой в три раза чаще (9%) использовали «распознавание по радужной оболочке глаза» для идентификации, чем жители любой другой страны (3%), принявшей участие в исследовании.

В России единая биометрическая система начала работать 30 июня 2018 года. Она создана по инициативе Центрального банка Российской Федерации и Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и является одним из ключевых элементов механизма удаленной идентификации, которая позволяет гражданам дистанционно получать финансовые услуги. Сегодня зарегистрироваться в системе можно в более чем 10 000 отделений банков, расположенных в 800 городах России. В Татарстане насчитывается 122 отделения банков, где можно сдать биометрию, всего в Приволжском федеральном округе — 2079 отделений 54 банков, регистрирующих биометрию.

Это цифровая платформа, которая является одним из ключевых элементов механизма удаленной идентификации человека по его биометрическим характеристикам. Указанная система создается по инициативе Министерства связи и массовых коммуникаций Российской Федерации и Центрального банка Российской Федерации.

При разработке Единой биометрической системы были заданы повышенные требования к безопасности и комфорту граждан при дистанционном получении услуг

Биометрия, в отличие от других методов удаленной идентификации, является уникальным «ключом», который нельзя потерять и крайне сложно подделать. Все другие способы идентификации недостаточно надежны - всегда остается возможность потери или взлома пароля или token-а.

В 2017 году Правительство РФ приняло программу «Цифровая экономика Российской Федерации», в соответствии с которой государство уделяет большое внимание развитию новых цифровых платформ и услуг, а также систем информационной безопасности для обеспечения их надежной работы. Создание системы является частью программы реализации «Цифровая экономика РФ».

Тем не менее, биометрические средства защиты имеют ряд недостатков:

1. Необходимость обучения биометрической системы для конкретных пользователей, зачастую, достаточно длительного.
2. Возможность ошибочных отказов и ошибочных подтверждений при аутентификации пользователей.
3. Необходимость использования специальных технических устройств для чтения биометрических характеристик, как правило, достаточно дорогостоящих (за исключением, быть может, аутентификации по клавиатурному подчерку).

Возможность ошибочных отказов и ошибочных подтверждений связан с несовершенством техники. Поскольку “предъявление” для проверки какого-либо биометрического параметра происходит, как правило, с помощью обычного смартфона, а качество их бывает разным, то вероятны ложноотрицательные результаты. Система может отказаться признать подлинность истинного хозяина учетной записи – например, из-за пореза на пальце сочтет этот отпечаток “чужим”. В случае, когда используется мультифакторная аутентификация и биометрические данные служат лишь одним из ее компонентов, идентификация сможет осуществиться с помощью OTP. Если же применяется вариант 2FA, при котором не одноразовые пароли, а именно биометрия является вторым фактором, то пользователь так и не сможет войти в аккаунт из-за этого ложного срабатывания. Также, стоит помнить о том, что злоумышленники быстро осваивают последние технологические новинки. Например, несколько лет назад появилась программа, позволяющая наложить на видео виртуальный слепок с фотографии человека в режиме реального времени. С ее помощью можно предоставить сканеру не просто статичное фото объекта, в чей аккаунт осуществляется вход, а динамичный, движущийся клон. С отпечатками пальцев – та же беда. Их несложно подделать, изготовив объемный латексный слепок или перчатку. Для исходного образца достаточно даже фотографии ладони потенциальной жертвы в высоком разрешении. Плюс ко всему, скомпрометированные данные очень трудно восстановить. Если перехвачен пароль – его можно поменять за пару минут. Украденную кредитку или OTP токен восстановить будет чуть дольше, но тоже возможно. В том же случае, когда скомпрометированными оказываются биометрические параметры, присущие человеку от рождения, практически происходит похищение личности. А ее не поменяешь так же легко, как пароль или электронную карту.

При всем вышесказанном, с учетом того, что мы вступаем в век носимой электроники, а телеметрия движется вперед семимильными шагами, вполне вероятно, что в недалеком будущем появятся новые технологии биометрической идентификации, лишенные тех недостатков, которые присущи существующим.

Библиографический список

1. Биометрия, личная безопасность, гражданская идентификация - Выпуск No_84. [Электронный ресурс] – Режим доступа: https://subscribe.ru/archive /state.politics.civil/200710/12184657.html

2. Мэнди Кюн. Защита доступа биометрическими методами. Журнал сетевых решений/ LAN. 2007. № 09. [Электронный ресурс] – Режим доступа: https://www.osp.ru/lan/2007/09/4376021/

3. Современные биометрические методы идентификации. Все плюсы и минусы биометрической системы защиты. [Электронный ресурс] – Режим доступа: https://eto-zhizn.ru/modern-biometric-identification-methods-all-the-pros-and-cons-of-the-biometric-protection-system.html

4. В России запущена Единая биометрическая система. 09 июля 2018. [Электронный ресурс] – Режим доступа: http://www.vsp.ru/2018/07/09/v-rossii-zapushhena-edinaya-biometricheskaya-sistema/

КИБЕРБЕЗОПАСНОСТЬ: ИССЛЕДОВАНИЕ ПРЕДСТАВЛЕНИЙ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ О СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВОЗМОЖНЫХ УГРОЗ

Исаков Р.О., учащийся
МБУ г. о. Тольятти «Лицей № 19»
Научный руководитель: Есина Н.В., учитель информатики и ИКТ
г. Тольятти

В современном мире все большую актуальность приобретает проблема обеспечения защиты информации от несанкционированного доступа, умышленного изменения, кражи, уничтожения, негативного психологического воздействия на человека и других преступных действий. Защита информации становится делом не только профессионалов, но и всех пользователей сети Интернет.

Анализ литературы, Интернет-источников, материалов СМИ показал, что в настоящее время любой пользователь сети Интернет может легко найти информацию по защите от киберугроз. Рекомендации, которые даются пользователям Интернет по безопасной работе, доступны и понятны для человека любого возраста.

Мы предположили, что современные пользователи сети Интернет, независимо от возраста, пола и места жительства, хорошо информированы о существующих угрозах кибербезопасности и принципах безопасной работы в сети Интернет; не верят в эффективность современных средств защиты от киберугроз; нарушают принципы безопасной работы в сети.

Для проверки выдвинутой гипотезы нами была разработана анкета, состоящая из трех разделов. В первом разделе анкеты размещена информация, объясняющая цели и задачи исследования. Основная часть анкеты включала 15 вопросов по проблеме исследования. Вопросы направлены на выяснение наличия или отсутствия аккаунтов в социальных сетях и электронной почты у респондентов; на выяснение того, кому или чему респонденты приписывают источник угроз: людям или вредоносным программам; на изучение поведения респондентов при защите информации от угрозы социальной инженерии при помощи паролей; на выяснение отношения респондентов к защите информации при помощи антивирусных программ, а также вопросы о принципах защиты от угрозы мошенничества. В заключительной части анкеты размещены вопросы о респондентах (пол, возраст, место жительства).

Исследование представлений пользователей сети Интернет о способах защиты информации от возможных угроз проводилось нами в ноябре 2019 года. В нем приняли участие 104 человека из Российской Федерации и стран ближнего и дальнего зарубежья. Граждане Российской Федерации составили 64% респондентов, граждане зарубежных стран – 36%.

Возрастной состав респондентов разнообразен, представлены все возрастные категории, однако более половины участников исследования составляют возрастную группу до 20 лет.

Нам необходимо было выяснить насколько активно участники исследования пользуются электронной почтой и социальными сетями, т.е. насколько активно они

используют сеть Интернет для обмена информацией. Нами было заданы два вопроса: «У Вас есть адрес электронной почты?» и «В каких социальных сетях у Вас есть аккаунты?». Результаты представлены на рис. 1 и 2.

Из диаграмм видно, что 97% респондентов активно используют сеть Интернет для обмена сообщениями и информацией. Это подтверждает и ответ на следующий вопрос о целях использования социальных сетей (рис. 3).

Поскольку основную часть респондентов составили люди в возрасте до 20 лет, то ожидаемо наибольшей популярностью у них пользуются такие социальные сети как ВКонтакте, Instagram, на третьем месте YouTube. Более половины участников опроса (57%) имеют несколько адресов электронной почты. Лишь 7% респондентов указали, что у них есть личная и публичная почта. Это означает, что одно из правил кибербезопасности, а именно, не размещать адрес личный электронной почты в социальных сетях, для регистрации на сайтах – нарушается. Это приведет к таким негативным последствиям как спам и фишинг.

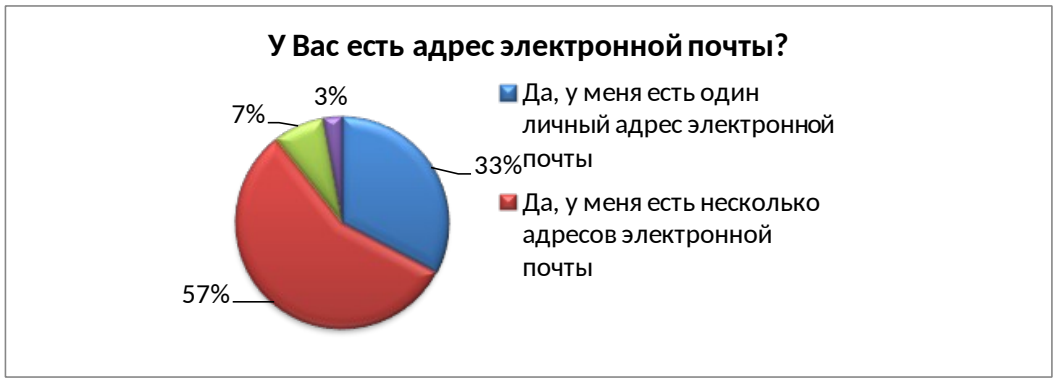

Рисунок 1 - Анализ наличия электронной почты у респондентов

Рисунок 2 - Анализ наличия аккаунтов в социальных сетях у респондентов

Рисунок 3 - Цели использования социальных сетей респондентами

Далее мы выяснили представления участников исследования об источнике угроз кибербезопасности. Результаты ответов на вопрос «Что из перечисленного ниже представляет наибольшую угрозу для сохранности информации (может быть несколько вариантов ответов)?» представлены на рис. 4.

Из диаграммы видно, что основной источник угроз сохранности информации респонденты приписали вредоносным программам и вирусам, не смотря на то, что разработчиками данных программ являются люди (хакеры, кибермошенники, кибертеррористы). Нам показалось интересным и распределение баллов по шкале «Источник угроз Человек». Чем выше степень социальной опасности (хакер → кибермошенник → кибертеррорист), тем меньшую угрозу в нем видят респонденты (57% - 45% - 29% соответственно).

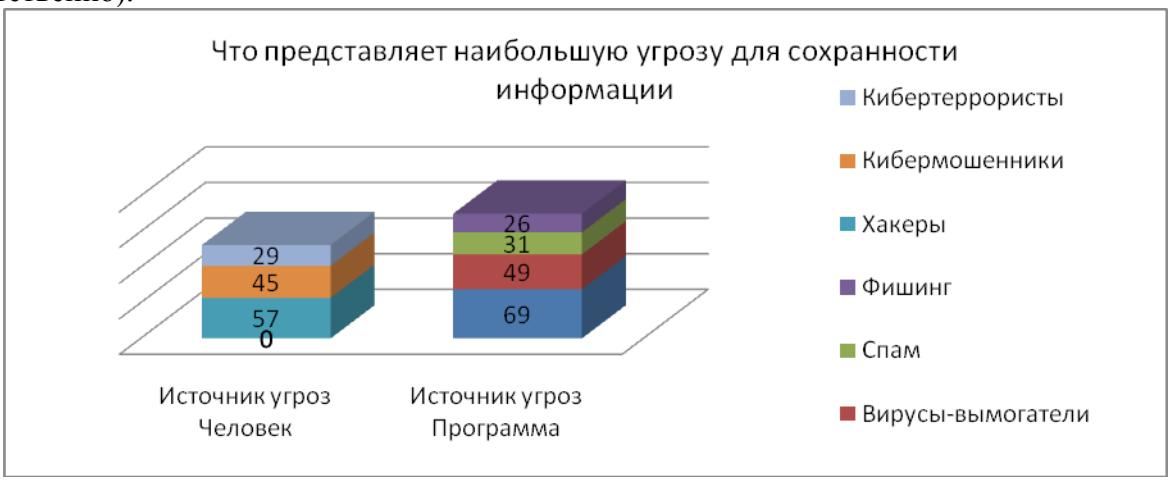

Рисунок 4 - Источники угроз кибербезопасности

Следующим этапом нашего исследования стало изучение отношения респондентов к такому средству защиты информации как пароль.

92% респондентов отметили, что для входа в аккаунты социальных сетей в ящики электронной почты необходимо иметь разные пароли. Это означает, что участники исследования хорошо знают это правило кибербезопасности и понимают последствия нарушения этого правила.

Далее участникам исследования были заданы три вопроса о том, какие пароли наиболее надежны, какие пароли легче всего взломать, и какие пароли использовал респондент хотя бы однажды. Результаты представлены на рис. 5.

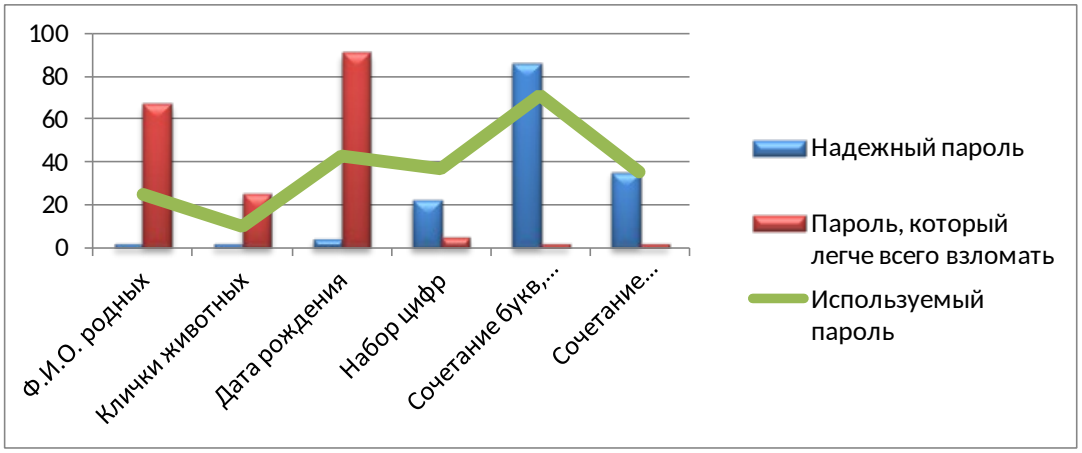

Рисунок 5 - Оценка респондентами надежности паролей

Из диаграммы видно, что респонденты хорошо знают, что нельзя использовать в

качестве паролей личную информацию, такую как фамилии и имена, даты рождения, клички животных, т.е. ту информацию, которую злоумышленники могут легко найти в социальных сетях. Также респонденты знают, что самым надежным является пароль, в котором есть сочетание и букв, и цифр, и знаков. 71% респондентов использует именно такой тип паролей. Однако, как мы и предполагали, 43% респондентов использовали в качестве пароля дату рождения, 25% - фамилии и имена. 37% респондентов в качестве паролей используют набор цифр. Не исключено, что это набор цифр 12345678 или 111111.

Учитывая тот факт, что почти половина респондентов (49%) вообще не меняют пароли и почти четверть респондентов (24%) меняют пароли не чаще, чем раз в год, говорит о том, респонденты не сильно заботятся о сохранности своей конфиденциальной информации. В этой части исследования наше предположение о том, что люди знают правила безопасности, но их нарушают – подтвердилось.

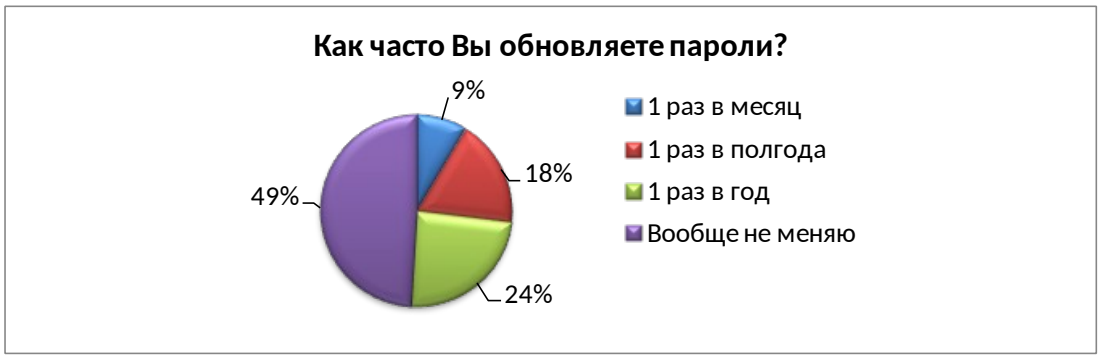

Рисунок 6 - Периодичность обновления паролей

Следующий этап нашего исследования посвящен изучению защиты от вредоносных программ и вирусов. Как мы выяснили ранее именно вредоносные программы и вирусы, по мнению наших респондентов, представляют наибольшую угрозу безопасности. Следовательно, респонденты особенно тщательно должны были бы защищать свои ПК и мобильные устройства от данных угроз, тем более, что в настоящее время антивирусные программы постоянно совершенствуются.

Респондентам были заданы три вопроса: о наличии антивирусных программ на устройствах респондентов, об оценке их пользы, об обновлении данных программ.

Результаты представлены на рисунках 7-9.

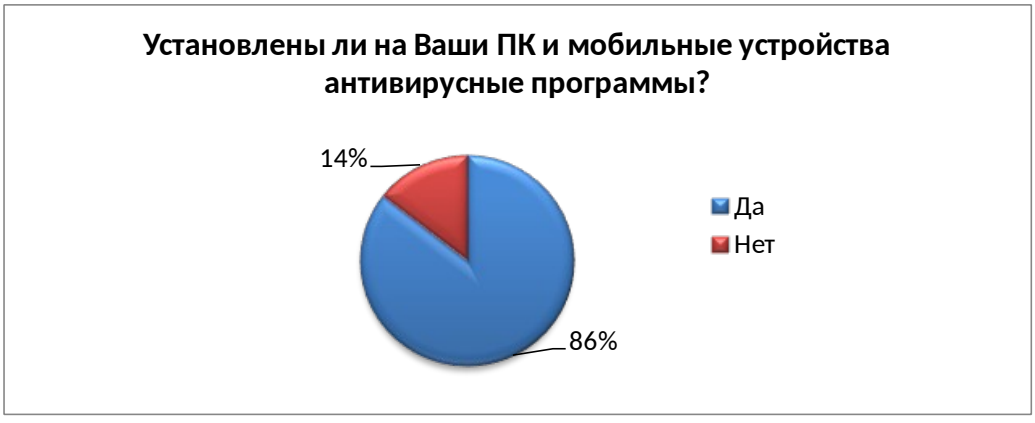

Рисунок 7 - Наличие антивирусных программ у респондентов

Рисунок 8 - Оценка эффективности антивирусных программ

Из представленных диаграмм видно, что 86% респондентов пользуются антивирусными программами, лишь 62% респондентов верят в их эффективность, и только 22% респондентов регулярно их обновляют.

Рисунок 9 - Периодичность обновления антивирусных программ

15% респондентов, осознавая наличие угрозы проникновения на ПК вредоносного программного обеспечения и вирусов, вообще не используют антивирусных программ. 17% респондентов, осознавая, что вредоносное ПО постоянно совершенствуется, что разрабатываются все новые вирусы, не обновляют антивирус. В этой части исследования наша гипотеза также нашла свое подтверждение.

В заключительной части опроса мы предложили респондентам две возможные ситуации и попросили рассказать об их предполагаемом поведении. В первой ситуации мы описали одну из самых популярных техник кибератаки, которая заключается в обмане пользователя путем отправки поддельных электронных писем - фишинг.

Из диаграммы (рис. 10) видно, что 13% респондентов могут стать «жертвами фишинга».

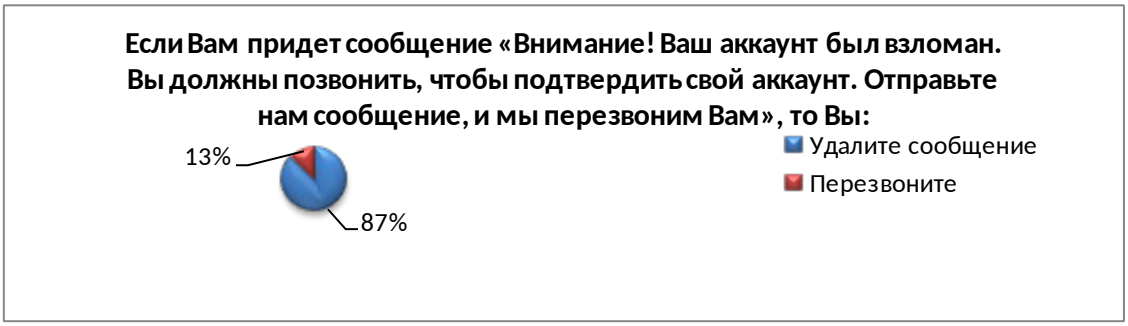

Рисунок 10 - Фишинг. Поведение респондентов

Вторая ситуация связана с взломом аккаунта в социальной сети, которая, к сожалению, в настоящее время не редкость.

Многие из нас с подобной ситуацией сталкивались и не раз, поэтому научились критично относится к сообщениям с аккаунтов друзей, с просьбой перечислить денег, и перепроверять подобную информацию. Результаты, представленные на рис. 11, свидетельствуют о том, что лишь 1% респондентов мог пострадать от действий мошенников.

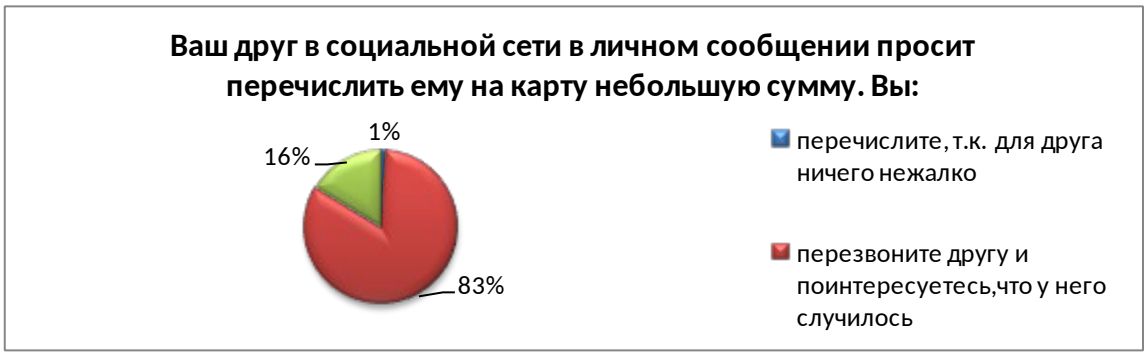

Рисунок 11 - Взлом аккаунта. Поведение респондентов

В ходе проведенного исследования, мы выяснили, что все наши респонденты являются активными пользователями сети Интернет. 98% респондентов пользуются электронной почтой и социальными сетями для обмена сообщениями, а значит, могут стать потенциальными жертвами кибератак со стороны злоумышленников. Все респонденты хорошо информированы о возможных киберугрозах, о способах защиты информации от данных угроз, о правилах безопасной работы в сети Интернет. Однако, как мы и предполагали, респонденты не всегда придерживаются правил кибербезопасности. Таким образом, наша гипотеза о том, что современные пользователи сети Интернет, независимо от возраста, пола и места жительства хорошо информированы о существующих угрозах кибербезопасности и принципах безопасной работы в сети Интернет; не верят в эффективность современных средств защиты от киберугроз; нарушают принципы безопасной работы в сети Интернет - подтвердилась.

Библиографический список

1. Горбачевская, Е.Н. Защита информации: учебное пособие [Текст] / Е.Н. Горбачевская. – Тольятти, 2016. - 307 с.

2. Кибербезопасность: вопросы, проблемы и угрозы безопасности. [Электронный ресурс] / URL: http://withsecurity.ru/kiberbezopasnost-voprosy-problemy-i-ugrozy-bezopasnosti.

3. Колесникова, К. Фильтруй контент! Нужны ли школьникам уроки кибербезопасности // Российская газета - Федеральный выпуск № 48(6619) [Электронный ресурс] / URL: https://rg.ru/ 2015/03/10/kontent.html.

4. Тонких, И.М., Комаров, М.М., Ледовской, В.И., Михайлов, А.В. Основы кибербезопасности. Описание курса для средних школ, 2-11 классы. - Москва, 2016.

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ДЕСТРУКТИВНЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ «ANDROID»

Карлова А.В., студент
Научный руководитель: Молодцова Ю.В., к. т. н., доцент
Национальный исследовательский университет Московский государственный технический университет им. Н.Э. Баумана
г. Москва

Аннотация: *популярность мобильных устройств с каждым годом увеличивается. В то же время появились уязвимости и вредоносные программы, влияющие на новую*

мобильную среду. Чтобы выявить и обезвредить эти угрозы, необходимо, чтобы существующие методы и средства безопасности адаптировались к новой ситуации. В результате современные методы, инструменты и процессы для проведения криминалистического анализа в сетях и системах должны охватывать также мобильные платформы. Статья посвящена выявлению алгоритма по исследованию вредоносного программного обеспечения в операционной системе «Android».

Ключевые слова: *судебная экспертиза, мобильное устройство, операционная система «Android», деструктивное приложение, вредоносное программное обеспечение.*

За последние несколько лет «Android» стал самой широко используемой операционной системой для смартфонов. Поскольку все больше и больше пользователей используют мобильные устройства с поддержкой «Android» и могут устанавливать сторонние приложения с официальных и альтернативных сайтов. Безопасность как устройств, так и сети становится серьезной проблемой как для конечного пользователя, так и для его поставщика услуг.

В последние годы пользователи стали свидетелями появления различных вредоносных программ для «Android». Связанные угрозы варьируются от простого отслеживания пользователя и раскрытия личной информации до продвинутого мошенничества и подписки на SMS-услуги премиум-класса, или даже неоправданного участия в бот-сетях. Хотя большинство пользователей в настоящее время знают, что персональные компьютеры могут быть атакованы вредоносным программным обеспечением (далее - ПО), очень немногие понимают, что их смартфон подвержен такой же опасной угрозе.

Чтобы оценить угрозу ПО, загруженного из сети Интернет [1], проницательные пользователи полагаются на результаты сканирования, полученные антивирусными продуктами. К сожалению, у каждого производителя антивирусов есть свой секретный рецепт того, как и почему он решает назначить метку вредоносного ПО данному приложению. Таким образом, различные антивирусные продукты могут по-разному оценивать приложение, что приводит к путанице.

На территории РФ киберпреступность, к которой можно отнести и распространение деструктивных программных продуктов, имеет тенденцию к устойчивому росту.

Компьютерные программы (или программное обеспечение или программы для ЭВМ) представляют собой один из объектов интеллектуальной собственности [2]. Законодательство РФ относит ПО к объектам авторского права [3, 4].

Что же такое программное обеспечение? Программное обеспечение (ПО) - совокупность программных средств, которые реализуют функции накопления, обработки, анализа и хранения информации, а также предоставления к ней доступа пользователям информационной системы. ПО с позиций предназначения и распространения можно разделить на три больших класса:

- универсальное ПО (отсутствие привязки к конкретной предметной области) - системы обработки текстов, средства распознавания образов, системы управления базами данных (СУБД), офисные системы, операционные системы, сетевое ПО, развлекательные компьютерные игры и т.д.;
- специализированное ПО (рассчитано на определенную группу пользователей, которые связаны с определенной предметной областью): системы автоматизированного проектирования, бухгалтерские, банковские и корпоративные системы, справочные и информационно-поисковые системы;
- уникальное ПО, разрабатывается по индивидуальному заказу для решения конкретной задачи и предназначено для использования организацией или лицом, которое сделало заказ.

С позиций функционального назначения ПО можно подразделить на:

- системное (включает сетевое) – совокупность средств, которые обеспечивают вычислительные процессы и поддерживают хранение, сбор и обработку информации;

- прикладное ПО – рассчитано на решение конкретных прикладных задач по автоматизации определенных действий;
- развлекательное ПО (компьютерные игры, аудио- и видеоплееры и т.д.) - разработано для удовлетворения потребностей пользователей в компьютерном досуге;
- справочное ПО – обеспечивает потребность пользователя в справочной информации.

Еще ПО можно разделить по основным категориям пользователей на следующие виды:
- корпоративное деловое ПО - предназначено для одновременного использования многими сотрудниками организации;
- автономное деловое ПО - используется индивидуально одним специалистом;
- групповое обучающее или развлекательное ПО - предназначено для проведения занятий в компьютерных классах или использования в компьютерных клубах;
- домашнее ПО - предназначено для использования в личных целях пользователя на домашних компьютерах.

Исследованием программного обеспечения в рамках раскрытия, расследования и предупреждения преступлений занимается судебная компьютерно-техническая экспертиза (далее - СКТЭ).

Так, 30 января 2019 года стало известно, что компания «Check Point Software Technologies Ltd.» выпустила первую часть отчета 2019 «Security Report», который раскрывает основные тренды и методы вредоносного ПО, которые исследователи «Check Point» наблюдали в 2018 году. Согласно документу, 33% организаций по всему миру подвергались атакам мобильного вредоносного ПО, причем три основных угрозы были направлены на ОС «Android». В 2018 было несколько случаев, когда мобильное вредоносное ПО было предварительно установлено на устройствах, а приложения, доступные в магазинах приложений, фактически оказались скрытым вредоносным ПО [5].

Для того, чтобы признать компьютерную программу вредоносной, необходимо доказать наличие совокупности следующих признаков, что данная программа:

1. Способна уничтожить, блокировать, модифицировать или копировать компьютерную информацию или нейтрализовать средства ее защиты;
2. Не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий;
3. Не запрашивает согласие (санкции) собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети на реализацию своего назначения (алгоритма) [6].

Исходя из вышеперечисленных требований, по нашему мнению, если у компьютерной программы отсутствует хотя бы один признак, то она является не вредоносной.

Так в рамках исследования деструктивного программного обеспечения переде экспертом стоят задачи по выявлению всех вышеуказанных в пунктах 1-3 признаков для того, чтобы ответить на вопрос о деструктивности данного программного обеспечения.

На современном этапе развития для решения задач, которые поставлены перед экспертом или специалистом при исследовании деструктивного программного обеспечения, активно используются программно-аппаратные комплексы, которые входят в автоматизированное рабочее место («Мобильный Криминалист», «Encase», «AutoPsy» и др.). Все они могут помочь эксперту при исследовании предположительно деструктивного программного обеспечения.

Таким образом, предмет судебно-экспертного исследования деструктивного программного обеспечения составляет выявление алгоритма работы вредоносной программы.

Задачи исследования любой предположительно вредоносной программы схожи вне зависимости от той платформы, на которой она используется. Общая методика исследования предположительно деструктивного программного обеспечения состоит из нескольких этапов:

1. Установление информации о дате и времени примерного появления данного программного обеспечения на устройстве.

2. Выявление антивирусными средствами данное программное обеспечение.

3. Проверка исследуемого файла антивирусной программой.

4. При срабатывании антивирусной программы убедиться в наличии кода в файле. Возможно ложное срабатывание антивирусной программы.

5. Определить форму представления кода (наличие зашифрованных фрагментов). Если код не зашифрован, то можно перейти к этапу 7.

6. Расшифровать код.

7. Проанализировать алгоритм работы программы и выявить источник происхождения предположительно вредоносной программы (сетевые адреса, номера телефонов, адреса электронной почты и др.).

Таким образом, при исследовании предположительно деструктивного программного обеспечения должны решаться следующие задачи:

1. Обнаружение признаков и следов работы предположительно вредоносной программы.

2. Сопоставление признаков, определенных выше для вредоносной компьютерной программы, с выявленными, решение вопроса о признании данного программного обеспечения деструктивным.

3. Анализ структуры предположительно вредоносной программы.

4. Расшифровка зашифрованных элементов исходного кода предположительно деструктивного программного обеспечения, если таковые имеются.

5. Анализ алгоритма работы программы, выявление источника происхождения предположительно деструктивного программного обеспечения [7].

Далее рассмотрим некоторые из самых популярных типов деструктивных приложений для мобильный устройств:

1) Банковское вредоносное ПО.

Такое ПО находится на подъеме, поскольку злоумышленики стремятся скомпрометировать пользователей, которые предпочитают вести весь свой бизнес - включая денежные переводы и платежи по счетам - со своих мобильных устройств. В третьем квартале 2018 года было обнаружено более 1,6 миллиона вредоносных инсталляционных пакетов, многие из которых были троянами, предназначенными для проникновения на устройства и последующего развертывания, собирая данные логина и пароля банка, которые затем отправлялись обратно на сервер управления и контроля.

2) Мобильные «вымогатели».

Первоначально ставшие популярными на ПК, «вымогатели» «блокируют» важные пользовательские данные, такие как документы, фотографии и видео, шифруя эту информацию, а затем требуя выкуп, выплачиваемый производителям вредоносных программ. Если выкуп не выплачивается вовремя, то все файлы удаляются или просто блокируются [8, 9].

3) Мобильные шпионские программы.

Они следят за всей активностью, записывают местоположение и извлекают важную информацию, такую как имена пользователей и пароли для учетных записей электронной почты или сайтов электронной коммерции. Во многих случаях шпионское ПО «соединено» с другим, казалось бы, безопасным ПО и незаметно собирает данные в фоновом режиме. Пользователь может даже не заметить наличие шпионских программ, пока производительность устройства не снизится или не запуститься антивирусный сканер [10].

4) Мобильное рекламное ПО.

Рекламное программное обеспечение прошло долгий путь: от раздражающих всплывающих окон до программ для сбора данных. Для многих производителей рекламного ПО доход зависит от количества кликов и загрузок, которые они получают, и, согласно «ZDNet», некоторые из них уже создали код «вредоносной рекламы», который может заразить и устройство, заставляя его загружать определенные типы рекламного ПО и позволяя злоумышленникам красть персональные данные.

Исходя из всего вышесказанного, деструктивное ПО - один из видов информационного оружия. По мнению отдельных исследователей, это специальное оружие, которое основано на использовании разрушающего программного воздействия на аппаратное обеспечение, ПО, компьютерную информацию, в том числе на средства защиты. Под разрушающим программным воздействием следует понимать целенаправленное изменение функций ПО, компьютерной системы или сети, которое порождает потенциальные или реальные опасные последствия.

Подводя итог, на основе предложенной системы научных положений о вредоносных программах и следах их применения необходимо усовершенствовать уже имеющиеся и разработать новые приемы, методы и средства обнаружения, фиксации, предварительного исследования и последующего использования в целях раскрытия, расследования и предупреждения преступлений.

Библиографический список

1. An attitude of citizens to state control over the internet traffic, Akhmadieva R.S., Ignatova L.N., Bolkina G.I., Soloviev A.A., Gagloev D.V., Korotkova M.V., Burenina V.I., Eurasian Journal of Analytical Chemistry. 2018. Т. 13. № 1b. С. em82.
2. Буренина, В.И. Система законодательства, регулирующего научно-техническую деятельность: проблемы и противоречия. Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2013. № 9-1 (35). С. 19-24.
3. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018) // «Парламентская газета», N 214-215, 21.12.2006.
4. Буренина, В.И. Авторские права в учебно-методическом обеспечении системы высшего образования, В книге: Управление качеством инженерного образования. Возможности ВУЗов и потребности промышленности Тезисы докладов второй международной научно-практической конференции. 2016. С. 217.
5. Вредоносная программа (зловред) [Электронный ресурс]. URL: http://www. tadvis-er.ru/index.php/ Статья:Вредоносная_программа_(зловред) (дата обращения 22.10.19).
6. Вехов, В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. – М.: Академия Следственного комитета Российской Федерации, 2015. № 2. – С. 43-46.
7. Нехорошев, А.Б., Шухнин, М.Н., Юрин, И.Ю., Яковлев, А.Н. Практические основы компьютерно-технической экспертизы. – Саратов: Науч. кн., 2007. – 266 с.
8. Арсенькина, Л.С. Нормативное регулирование использования аппаратных блокираторов в рамках судебной компьютерно-технической экспертизы в российской федерации. В сборнике: Источники частного и публичного права Сборник научных трудов по материалам VII ежегодной международной научно-практической конференции (с элементом школы молодого ученого для студентов юридических специальностей). 2017. С. 13-16.
9. Арсенькина, Л.С. Использование аппаратных блокираторов в судебной компьютерно-технической экспертизе при анализе накопителей на жёстких магнитных диска, Молодежный научно-технический вестник. 2017. № 3. С. 35.
10. Мобильные вредоносные программы [Электронный ресурс]. URL: https:// www.kaspersky.com/resource-center/threats/mobile (дата обращения 22.10.19).

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕДУРЫ ВЫБОРА И РЕГИСТРАЦИИ ДОМЕННОГО ИМЕНИ

Краснов С.С., инженер
Волжский университет имени В.Н. Татищева
г. Тольятти

При наличии больших пробелов не только в российском, но и в международном законодательстве, по поводу как определения самого доменного имени, так и формализации правоотношений, возникающих при его правоприменении, основными документами в этой области для нашей страны являются Правила регистрации доменных имен в доменах .RU и .РФ, разработанные АНО «Координационный центр национального домена сети Интернет» и являющиеся обязательными для всех администраторов доменных имен.

Домен в зоне .RU может состоять из букв латинского алфавита, цифр и знака дефиса «-» и «должен быть не менее 2 и не более 63 символов…» [3].

Доменное имя должно:

1. быть достаточно просто запоминаемым;
2. отражать по возможности, содержательную составляющую информационных ресурсов, которые предполагается размещать по этому адресу;
3. не должно противоречить общественным интересам, принципам гуманности и морали, особенно как показано в работе Белинда Айзек (Belinda Isaac) не совпадать с «именами известных авторов и знаменитостей…» [5];
4. не должно совпадать со специализированными обозначениями.

К специализированным обозначениям, обычно, относят несколько «групп:

- международные непатентуемые названия (INN) фармакологических препаратов;
- названия международных организаций;
- личные имена;
- фирменные наименования;
- географические названия и указания на происхождение…» [4];

5. быть «свободным».

Убедиться, что выбранное доменное имя свободно можно с помощью информационного сервиса WHOIS, по адресу https://whois.ru/, на котором находятся данные обо всех действующих доменах. Если выбранного доменного имени в данной базе нет, то его можно регистрировать.

На этом же сервисе можно оставить заявку на регистрацию уже освобождаемых доменов, если вам подойдут их имена.

Вместе с ростом числа организаций и фирм растет количество администраторов доменных имен, а, следовательно, и количество компаний - регистраторов. В зависимости от подходов к ведению бизнеса эти компании могут различаться и формой собственности, и внутренней организацией, и тарифами, и практикой ведения дел. Таким образом, выбор компании регистратора важный этап, при котором нельзя руководствоваться единственным критерием – стоимостью регистрации.

Остановимся на этом вопросе подробнее.

Если под зарегистрированным доменным именем размещаются какие-то ресурсы, то домен нужно привязать к определенным серверам DNS, которые связаны с конкретным доменом через общую, глобальную иерархию систем адресации.

То есть сам сервер, на котором размещен сайт, может работать бесперебойно, но, если откажут серверы DNS, то попасть на этот сервер по привычному адресу не получится. Таким образом, сайт просто исчезнет из пространства Интернета. Так что надежность серверов DNS играет важную роль в обеспечении доступности веб-сайтов и других онлайн-ресурсов, в том числе систем электронной почты. Часто услуга размещения DNS предоставляется хостинг-провайдерами.

Серверы DNS часто служат объектом атак со стороны хакеров, типа «отказ в обслуживании». Отказавшие DNS-серверы не смогут обслуживать запросы, и размещенные под соответствующим доменом ресурсы будут недоступны.

DNS-серверы могут быть взломаны хакером. В таком случае получивший доступ к серверу хакер сможет управлять и доменом или несколькими доменами, обслуживаемым этим DNS-сервером. Это означает, что хакер может перенаправить трафик с ресурсов администратора на какие-нибудь свои ресурсы. С точки зрения пользователя Сети, новые хакерские онлайн-ресурсы будут доступны под теми же самыми доменами, которые ранее соответствовали легальным сайтам или адресам электронной почты. Другими словами, происходит «угон» домена в интересах хакера.

Необходимо также учитывать, что устойчивая работа Интернета, возможна лишь при надежной работе телекоммуникационной инфраструктуры, функции «по управлению государственным имуществом и оказанию государственных услуг в сфере электросвязи…» соответствии с Постановлением Правительства Российской Федерации возложены на Федеральное агентство связи (Россвязь), которое через своего оператора связи должно обеспечить «пользователю возможность пользования услугами связи по передаче данных 24 часа в сутки…» [1].

Степень уверенности в том, что у компании-регистратора не возникнет серьезных проблем возрастает при учете следующих рекомендаций:

- использовать услуги по аренде DNS, предоставляемые крупными регистраторами или хостинг-провайдерами;
- одновременно использовать нескольких DNS-серверов, находящихся у разных провайдеров;
- страна, где зарегистрирована компания - Россия;
- как давно оказывает подобные услуги;
- количество клиентов;
- какой % рынка занимает;
- где территориально расположены сервера – наиболее предпочтительный вариант - Россия;
- существует и какой тестовый период;
- стоимостная политика;
- существует ли техническая поддержка;
- наличие положительных отзывов.

Данная информация доступна в интернете на сайтах фирм, публикующих рейтинг компаний - регистраторов и провайдеров.

Библиографический список

1. Постановление Правительства Российской Федерации от 30 июня 2004 г. № 320 «Об утверждении Положения о Федеральном агентстве связи».

2. Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных».

3. "Правила регистрации доменных имен в доменах .RU и. РФ" (утв. решением Координационного центра национального домена сети Интернет от 05.10.2011 N 2011-18/81) (ред. от 28.02.2019).

4. Дашян, М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет – М.: "Волтерс Клувер", 2007.

5. Belinda, Isaac. Personal Names and the UDRP: A Warning to Authors and Celebrities // Entertainment Law Review. Vol. 12, No. 2. 2001. p. 44.

ИНСАЙДЕРСКИЕ УТЕЧКИ ИНФОРМАЦИИ. СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Куваев В.Д., Арустамян А.М., Бадиков Д.О., студенты

Научный руководитель: Федосеева О.Ю., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Информационная безопасность (ИБ) – тема номер один во всем, что касается юридических и физических лиц в цифровом пространстве. И если все, что связано с технической стороной работы ИБ-систем широко обсуждается, то культуре работы с данными и влиянию человеческого фактора не уделяется заслуженного внимания. Инженер по облакам и безопасности компании Linxdatacenter Б. Меркулов рассказал о роли личности специалиста по ИБ в глобальной ИТ - истории: «В мировом рейтинге экономических угроз кибератаки находятся в топ-3. Ответом на эту ситуацию может стать только резкий рост грамотности людей в вопросах информационной безопасности. Мы живем в эпоху, в которой главным товаром является информация. Поэтому уже со школы детям необходимо формировать понимание, что такое персональные данные, конфиденциальная и секретная информация, а также как и почему необходимо обращаться с ней правильно.

В противном случае, общество рискует получить ещё несколько поколений, которые будут относиться к этим вопросам как большинство наших современников, т. е. реагируя на последствия инцидентов. Если говорить о том, какие шаги следует предпринимать на уровне организации, то это регулярное обучение, тренинги и лекции для лучшей осведомленности персонала по вопросам ИБ. В первую очередь нужно сделать так, чтобы люди осознавали ценность информации. Если человек не сталкивается с кражей персональных данных в обычной жизни, то он не будет задумываться, что его паспорт может кто-то продать/купить и как-то нелегально использовать. Необходимо регулярно напоминать коллегам о важности защиты персональной информации, повышать грамотность в этой области, говорить о том, что такие вопросы касаются не только интересов компании, но и жизни каждого из нас.

Необходимо обеспечить выполнение требований законодательства и регуляторов в области ИБ. Важно, чтобы сотрудник понимал ответственность за те или иные действия, а для этого необходимо доходчиво формировать политики, не делая их избыточными. Для каждой организации эти документы будут отличаться. Соблюдение требований регуляторов и выполнение законодательства вкупе с минимальным влиянием на бизнес-процессы организации является идеальным сочетанием. Немаловажным моментом является и периодический аудит соответствия требованиям безопасности. Нужно в первую очередь самостоятельно осуществлять контроль внутри организации для выполнения всех норм и регламентов.

Поскольку чисто технически сегодня возможно сделать так, чтобы единственным слабым звеном процесса оставался только человек, пропорционально возрастает важность ответственных за информационную безопасность кадров».

Исследование уровня ИБ в российских и зарубежных компаниях, которое «СёрчИнформ» проводила в 2018 году, показало: в 74% ИБ-инцидентов виноваты рядовые сотрудники (рисунок 1).

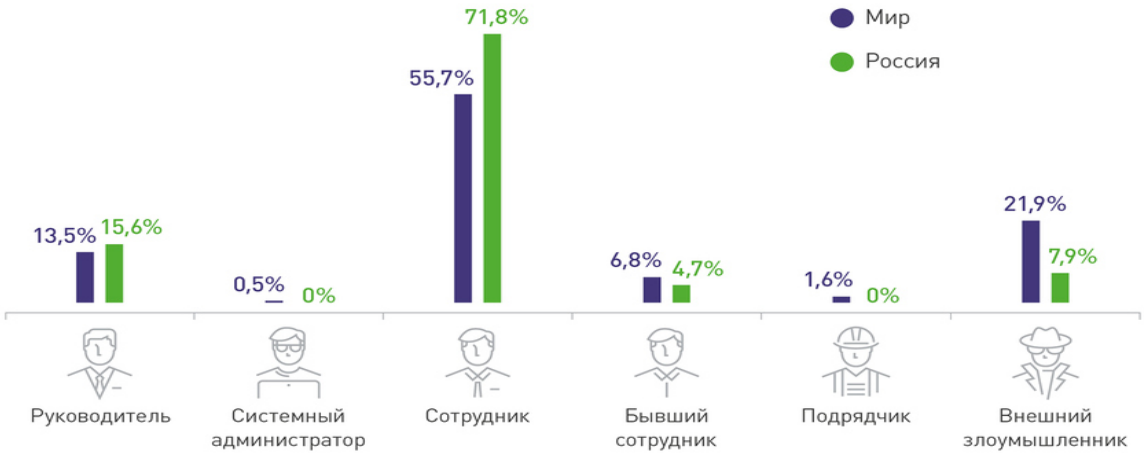

Рисунок 1 – Распределение мошеннических инцидентов с данными по виновникам, мир-Россия, 2018 год

С развитием информационных систем угрозы, исходящие от сотрудников организаций (инсайдеров), давно стали очень серьезными, а ущерб от их действий исчисляется десятками миллиардов долларов. Постоянно растет поток сообщений об инцидентах, связанных с нарушением своих обязательств и прав авторизованными пользователями, которые намеренно саботируют свою компанию и передают информацию конкурентам. Одновременно изменяется и бизнес-среда, которая все больше полагается на аутсорсинг, подрядные компании и сторонние технологические платформы, что приводит к тому, что ценная бизнес-информация становится доступной все большему количеству людей. В случае инсайдерских утечек контроль доступа и защита периметра не помогут, вредитель уже находится внутри периметра.

Умышленные утечки информации – это случаи преднамеренной утечки данных, когда пользователь, имеющий доступ к ценной информации, знал о возможных негативных последствиях своих действий, понимал, что такие действия носят противоправный характер.

В переводе с англ. inside – внутренняя сторона; внутренность; изнанка; внутренний; скрытый; секретный; insider – лицо, в силу служебного положения располагающее конфиденциальной информацией о делах фирмы; хорошо осведомленный человек; человек, посвященный в тайну.

В настоящее время термин «инсайдер» трактуется несколько в ином значении: это сотрудник компании, который сознательно способствует или осуществляет утечку информации для своей выгоды и во вред компании, в которой работает.

Инсайдерство - нелегальный вынос коммерчески важной информации за пределы компании, умышленное раскрытие секретной информации с целью продажи, порчи репутации компании или неумышленное, произошедшее по причине халатности персонала.

Инсайдерская атака – это утечка персональной и конфиденциальной информации, произошедшая вследствие инсайдерского инцидента. Среди прочих киберпреступлений инсайдерские атаки имеют самый высокий уровень латентности и самый низкий показатель раскрываемости.

Инсайдер остается самым распространенным виновником утечек данных в организациях. Доля инцидентов по вине внутреннего нарушителя в 2018 году увеличилась на три процентных пункта - до 63% от общего количества утечек за год, говорится в новом исследовании Аналитического центра компании InfoWatch. Каждый второй инцидент произошел по вине рядового специалиста, еще около десяти процентов случаев пришлись на "привилегированных" пользователей (руководители и системные администраторы), подрядчиков и бывших сотрудников компаний.

Сегодня большинство предприятий используют многоуровневые системы обработки информации – компьютеры, облачные хранилища, корпоративные сети и т. д. Все эти

системы не только передают данные, но и являются средой их возможной утечки. Утечка секретной информации – это процесс неконтролируемого разглашения ключевых для фирмы данных.

Коммерческая тайна – это информация об организации деятельности предприятия, технологии разработки продукции, данные о денежных потоках, интеллектуальная собственность и другие сведения, владея которыми фирма получает финансовую выгоду.

Существует несколько причин инсайдерской утечки информации.

Причина 1 – Персонал. Каждый сотрудник предприятия является потенциальной угрозой для безопасности информации. Часто люди забирают работу домой – перемещают рабочие файлы на свои флеш-носители, передают их по незащищенным каналам соединения, обсуждают информацию с сотрудниками конкурирующих компаний.

Действия персонала бывают умышленными и непреднамеренными. Непреднамеренные действия – это следствие незнания регламента работы с коммерческой информацией.

Риск утечки информации от персонала есть всегда, и его нельзя исключить полностью. Служба безопасности может принять меры, которые ограничат взаимодействие работников с конфиденциальной информацией:

- Разработка правил разграничения доступа. Правила представляют собой перечень четких прав и ограничений, которые должны соблюдаться каждым сотрудником. Их основной принцип – каждый работник взаимодействует только с теми данными, которые нужные для его работы. Таким образом, простой менеджер не сможет узнать технологию разработки продукции и другие важные данные, которые желает знать злоумышленник.

- Соблюдение норм документирования информации, которая содержит коммерческую тайну.

- Оперативное выявление сотрудников, которые несут угрозу разглашения данных.

Как выявить сотрудника, который разглашает данные конкуренту?

Вопросами контроля работы персонала с секретными материалами должен заниматься уполномоченный сотрудник или отдел безопасности. Их задача – следить за деятельностью работников на протяжении всего рабочего дня и оперативно выявлять все случаи утечки информации.

На практике обнаружить человека, сливающего коммерческую тайну, можно по таким признакам:

- Сотрудник без предупреждения задерживается после работы на своем рабочем месте. В таком случае есть вероятность того, что он пытается получить доступ к секретной информации в момент, когда рядом нет контролирующих. На такого работника нужно обратить внимание и проследить, не является ли его целью разузнать тайные сведения. Контролировать время пребывания персонала на рабочем месте помогают специальные системы учета доступа. Начинать расследование нужно лишь в том случае, если стали известны конкретные факты утечки защищаемой информации.

- Сотрудник сохраняет на свой персональный компьютер или смартфон слишком много электронных документов компании. Такой вариант утечки можно отследить в компаниях, которые используют системы защиты файловой системы. Суть их работы заключается в создании общего сервера, который действует в рамках одной корпоративной или Wi-Fi-сети. Во время каждого открытия, копирования и перемещения данных на служебном ПК вся информация о процессах поступает на сервер. Таким образом, администратор безопасности может выявить, с какого ПК и в каком количестве была перемещена секретная информация.

- Сотрудник без необходимости копирует бумажную документацию, сведения в которой предназначены только для служебного использования.

Согласно нормам документирования, все физические папки и файлы с коммерческой тайной должны храниться в защищаемой части архива. Доступ к документам возможен только для уполномоченных работников. Все данные о получении документа с тайной на руки должны документироваться (с указанием имени работника и точного времени выдачи документа).

Если же секретный документ попал в руки недобросовестного сотрудника, отследить его несанкционированное копирование можно на сканере или ксероксе, который хранит отчет о последних действиях. Также существуют факсимильные аппараты, доступ к которым возможен только после правильного введения пары «идентификатор пользователя-пароль».

- Работник регулярно нарушает общие требования безопасности при работе с коммерческой тайной.

Если персонал регулярно пытается обойти систему запрета, просматривая запрещенные ресурсы, или использует личную технику для обработки секретных данных, необходимо внедрить дополнительные системы контроля пользователей. К примеру, DLP-системы. Их задача заключается в мониторинге всех переписок пользователей с коммерческой почты и других электронных ящиков, которые зарегистрированы в системе. Также модуль защиты запрещает установку стороннего ПО, а все действия сотрудника за компьютером видны администратору безопасности.

- Сотрудник был уличен в контактах со служащими конкурирующих компаний.

В больших компаниях работники часто общаются вне рабочего времени. Таким образом, они получают больше информации друг о друге и могут узнать о связях коллеги и работника конкурирующей организации. Вероятность обычных дружеских отношений между людьми тоже возможна, но лучше оповестить руководство компании об этом во избежание ненужных подозрений.

Причина 2 – Проблемы подбора кадров. Частая смена персонала, масштабные изменения в организации работы компании, понижение заработных плат, сокращения сотрудников – все это является частью «текучки» кадров. Такое явление часто становится причиной утечки секретной информации.

Кризис, нехватка средств для выдачи зарплат заставляют руководство ухудшать условия работы персонала. В результате повышается недовольство работников, которые могут уйти или же просто начать распространять секретные данные конкурентам. Проблема смены персонала особенно важна для руководящих должностей, ведь все управляющие должны иметь доступ к секретной документации.

Угрозу распространения тайны могут нести не только уже ушедшие сотрудники, но и текущие работники, уровень мотивации которых понижен.

Для предотвращения проблемы следует создать для работников максимально комфортные условия работы. В случае серьезного кризиса рекомендуется собрать персонал для обсуждения возможных путей выхода из сложной ситуации. Важно уведомлять сотрудников обо всех изменениях в начислении заработных плат заранее, а не по факту выплаты оклада.

Порой неблагоприятную атмосферу в коллективе создает один сотрудник. Система «ProfileCenter СёрчИнформ» анализирует переписку работников в электронной почте и мессенджерах и составляет их психологические портреты и определяет положительные и отрицательные стороны характера человека, что позволяет принимать верные управленческие решения.

Для устранения «текучки» важно выполнять следующие рекомендации:

- Наладить систему найма кадров. Все передовые организации имеют специальный отдел, который занимается вопросами найма, увольнения и поддержки сотрудников. Не следует искать работника на освободившуюся вакансию как можно быстрее. Хороший HR (специалист по подбору кадров) обязан прослушать несколько претендентов на должность, распространить информацию о свободной вакансии на всех популярных Интернет-площадках, провести итоговый конкурс, результаты которого определят наиболее подходящую кандидатуру.

- Внедрение системы вознаграждений. За успехи в работе, перевыполнение планов и заключение выгодных контрактов сотрудников нужно поощрять. Примерами поощрения могут быть повышение заработной платы, улучшение условий работы, продвижение по карьерной лестнице.

- Предоставление всем сотрудникам возможности профессионального роста, повышения квалификации. Хорошие компании всегда отправляют своих сотрудников на курсы повышения квалификация или же закупают онлайн-тренинги для более удобного прохождения обучения. Также рекомендуется организовывать тренинги от ведущих профессионалов отрасли.

- Контроль персонала. Если технические средства легко контролировать, то персонал является одним из самых опасных источников утечки. Человеческий фактор присутствует всегда, и даже сотрудники отдела безопасности не всегда могут установить, от какого работника может исходить угроза.

Как правило, поиск злоумышленника среди персонала выполняется уже тогда, когда стали известны первые случаи передачи данных конкурентам. Администраторы безопасности проверяют возможность перехвата информации по техническим каналам утечки, и, если все каналы надежно защищены, подозрение падает на работников.

Деятельность сотрудников организации контролируется с помощью систем учета рабочего времени. Это комплексное аппаратное и программное обеспечение, которое документирует точное время прибытия на работу, время ухода, деятельность персонала за компьютером, записывает переписки корпоративной почты, проводит видеонаблюдение и передает все эти данные руководству фирмы или главе отдела безопасности. Далее вся полученная информации анализируется и выявляется число работников, которые могли распространять коммерческую тайну.

Библиографический список

1. Утечки информации в России. [Электронный ресурс]. – Режим доступа: http://www.-tadviser.ru/index.php/
2. Нашумевшие утечки данных пользователей за январь — апрель 2019. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/ company/cloud4y/blog/452880/
3. Причины утечки информации. [Электронный ресурс]. – Режим доступа: https:// searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/prichiny -utechki-informatsii/
4. Исследование уровня информационной безопасности в компаниях России и мира за 2018 год. [Электронный ресурс]. – Режим доступа: https://searchinform.ru/research-2018/
5. Кривошапко, Ю. Утечки данных из организаций все чаще происходят по вине сотрудников. [Электронный ресурс]. – Режим доступа: https://rg.ru/2019/04/02/utechki-dan-nyh-iz-organizacij-vse-chashche-proishodiat-po-vine-sotrudnikov.html
6. Умышленные утечки информации. [Электронный ресурс]. – Режим доступа: https:// www.anti-malware.ru/threats/intentional-information-leaks
7. Инсайдеры и утечка информации. [Электронный ресурс]. – Режим доступа: http:// rus.safensoft.com/glossary/insider/

ИСТОРИЯ СТАНОВЛЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В США

Курганов А.В., студент
Научный руководитель: Федосеева О.Ю., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

На современном этапе развития информационного общества защита информации имеет огромное значение. Создание информационного пространства, включающего все сферы общественной жизни, не обходится без посягательств на информационную безопасность стран. Информация является такой же ценностью, как и другие ресурсы необходимые для развития стран. Перед всеми современными государствами встаёт задача создания системы защиты собственной информации, что напрямую связано с обеспечением государственной безопасности, сохранением независимости и целостности государства.

Каждое государство создаёт национальную систему защиты информации, исходя из собственных экономических и технологических ресурсов. Чем выше уровень развития страны, тем притягательней становится её информационная среда, тем современней и технологичной должна быть система информационной защиты.

Информационная структура является основой всех сфер жизни современного общества. Поэтому национальный информационный ресурс рассматривается, как главный источник экономической и военной мощи государства. С момента создания и распространения компьютеров и другой вычислительной техники связано возникновение такого направления, как индустрия производства, обработки и потребления информации, которая является неотъемлемой частью общественной жизни. Эти изменения повлекли за собой новые критерии уровня развития государства, именно развитие вычислительных средств определяет ведущую страну в мире. Информатизация военной, экономической и социально-политической деятельности страны повлекло бурное развитие информационных систем. Эти процессы сопровождаются постоянно растущим количеством попыток доступа к информации, как со стороны других государств, так и со стороны граждан, не имеющих доступа к ней, либо злоумышленниками. Информация приобретает конкретное политическое, материальное и стоимостное значение, так как проникает во все сферы деятельности государства. На этом фоне все более значимый характер приобретают вопросы обеспечения информационной безопасности страны как неотъемлемого элемента современной национальной безопасности, а защита информации становится одной из приоритетных задач государства. Данная обстановка выдвигает проблему информационной безопасности на первый план.

Рассмотрим и сделаем анализ системы информационной безопасности США. Эта страна представляет большой интерес для изучения ее системы безопасности, так как это одна из ведущих стран мира. Данная страна уделяет большое количество ресурсов на развитие собственной стратегии защиты информации. Система информационной безопасности, состоит из совокупности органов и исполнителей, используемой ими техники защиты, организованная и функционирующая по правилам, установленным правовыми, распорядительными и нормативными документами в области защиты информации.

Становление системы защиты связано с концом 19 века. В 1875 году было создано два комитета: комитет безопасности и комитет секретной корреспонденции, занимающиеся обеспечением защиты информации в военной и во внешнеполитической областях. Далее, в 1907 году было издано директивное распоряжение, согласно которому определяется порядок использования на документах грифа «конфиденциально». Документ с таким грифом сопровождался списком должностных лиц, имеющих доступ к данному документу [1].

Позже, в июле 1908 года было основано Федеральное Бюро Расследований (далее – ФБР) со следующими функциями: проверка государственных служащих на предоставление права доступа к информации, составляющей Государственную тайну. После, в 1911 году, был издан закон «о предотвращении раскрытия секретов национальной обороны». В нем впервые был введен термин “секреты национальной обороны”. Закон был направлен на предотвращение шпионажа. Также были приняты несколько ведомственных инструкций Министерства Обороны США, которые описывали порядок работы с документами с грифом «конфиденциально», «лично», «секретно» и с документами для использования одним должностным лицом.

После принятия данных инструкций, в 1917 году, был издан закон о шпионаже, который заменил закон 1911 года «о предотвращении раскрытия секретов национальной обороны». Согласно этому закону информация о шифрах, кодах и сигнальных книгах считалась секретной. Шпионаж наказывался смертной казнью. В 1935 г. вводится новый гриф - "ограниченный доступ". Применялся для конструкторской документации и исследовательских работ.

После создания инструкции Министерства Обороны (далее – МО) 1936 года осталось 3 типа секретной информации - "Секретно", "Конфиденциально" и "Ограниченный доступ".

Информация "для служебного пользования" была отнесена к категории "Ограниченного доступа". Данная система грифования применялась до 50-ых годов [2].

С 1946 по 1948 год в США рассматривалась и принималась новая директива под названием «Наши цели в отношении России», в которой описывались основные цели и стратегии в отношении России. Основой данной директивы послужил «План Даллеса». 18 августа 1948 года она была принята. По вопросам Защиты информации (далее – ЗИ) в вооруженных силах отвечал отдел службы безопасности армии, который в 1949 году был переименован в отдел службы безопасности вооружённых сил. В 1952 году его заменяет национальная службы безопасности [3].

В июле 1947 года был издан закон о национальной безопасности, согласно этому закону создается координирующий орган гражданской и военной разведки – Центральное Разведывательное Управление (далее – ЦРУ). Функции директора центральной разведки возложены на директора ЦРУ. Создаётся Совет национальной безопасности (далее – СНБ) при президенте США, реорганизованы военные ведомства, созданы единые министерство обороны, объединённый комитет начальников штабов, министерство ВВС. Но уже 1949 году принят закон о ЦРУ, как закон о национальной безопасности. В соответствии с этим законом более чётки определены задачи Центрального Разведывательного Управления:

- Добывание разведывательных сведений тайным и легальным путём.
- Тайная подготовка вмешательства в дела других государств, если затрагиваются интересы США.
- Обобщение информации, собранными другими ведомствами и подготовка выходных документов разведки.

В ноябре 1952 года было создано агентство национальной безопасности (далее – АНБ). Задачи агентства делились на 2 группы: наступательные и оборонительные. К наступательным относится добывание информации о иностранных государствах путём перехвата любых электромагнитных сигналов. К оборонительным относится защита от иностранного проникновения всех линий связи, по которым передавалась информация. Задачи агентства национальной безопасности:

- Создание и санкционирование шифров всех правительственных служб.
- Обеспечение сохранности передачи данных в каналах связи.
- Обеспечение безопасности связи для систем стратегического оружия.
- Создание личного шифра президента.

Классификация информации:

- Доставляемая ежедневно президенту.
- Доставляемая санкционированным потребителям в госучреждениях.
- Информация справочного характера, она вводится в автоматизированные информационные системы (АИС).
- Информация коммерческого характера.

После создания АНБ, в 1962 году было создано Разведывательное управление министерства обороны и Национальная космическая разведка, в 1981 году в него включено Национальное агентство картографии и изображений. Государственная политика в области защиты информации по национальной безопасности реализуется Разведывательным сообществом США [1].

В 60-70 годы в США приняты ряд федеральных законов, заложивших правовую основу для формирования и проведения Единой государственной политики в области информационных технологий и защиты информации.

Еще в марте 2001 года президент, перечислил главные угрозы безопасности Соединенных Штатов. На втором месте после терроризма в этом перечне значится информационная война и уже за ней - распространение оружия массового поражения и средств его доставки.

В начале 2008 года президент США Дж. Буш подписал две секретные директивы - № 54 (по национальной безопасности) и № 23 (по внутренней безопасности). В этих документах

спецслужбам страны, и прежде всего Министерству Внутренней Безопасности США (далее – МВБ), а также Агентству Национальной Безопасности даются указания по усилению контроля за компьютерными сетями, используемыми американскими федеральными структурами. Кроме того, заокеанские разведчики и контрразведчики должны расширить сферы мониторинга информации, поступающей в сети правительственных ведомств Соединенных Штатов через Интернет [4].

Новыми директивами Пентагону было разрешено разрабатывать планы проведения кибернетических контратак на информационные сети противников США. При установлении конкретного факта нападения и выявления сервера иностранного государства, с которого была осуществлена атака, специалисты Минобороны могут нанести по нему ответный удар для предотвращения новых атак на информационные сети американского правительства.

АНБ работает в тесном сотрудничестве с МВБ в вопросах обеспечения информационной безопасности. Так, в 2004 году подразделение кибернетической безопасности начало разработку учебного курса по информационной безопасности для центра повышения квалификации персонала агентства. В 2008 году в соответствии с президентской директивой АНБ было названо ведущей организацией по мониторингу и защите федеральных правительственных сетей от кибертерроризма [5].

Все вышеперечисленные организации руководствуются основными законами в области защиты информации. Правовая защита информации – защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая защита информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является основой для морально – этических норм в области защиты информации.

Законодательство США в сфере ИБ образует совокупность федеральных законов, законов штатов и нормативных актов, которые создают правовую основу для формирования и проведения государственной политики в сфере Информационной Безопасности. Американский законодатель значительное внимание уделил вопросам обеспечения безопасности информации в государственных компьютерных системах (законы США "О компьютерной безопасности" и "Об усовершенствовании информационной безопасности"), противодействия компьютерной преступности (законы "О компьютерное мошенничество и злоупотребление" и "О злоупотреблениях компьютерами"), регулирование соотношения прав граждан на получение информации (законы "О свободе информации" и "Об освещении деятельности правительства") и конфиденциальности их частной жизни (закон "Об охране персональных данных").

Рассматривая положения законодательства США в указанной сфере, можно сделать вывод о том, что оно направлено на обеспечение прав граждан на информацию и конфиденциальность их частной жизни, а с другой на национальную безопасности государства, то есть ориентирован на сохранение баланса интересов личности, общества и государства [1].

США – одна из развитых мировых держав, обладающая достаточными ресурсами и высоким уровнем экономического и политического развития. На протяжении исторического развития данной страны постепенно складывалась американская система защиты информации. Отличительными особенностями данной системы является всесторонний контроль над обеспечением секретности организаций и лиц, имеющих прямой доступ к информационным источникам. Система включает разветвлённую нормативно-правовую базу, которая охватывает различные стороны жизнедеятельности американского общества.

Библиографический список

1. Рытов, М.Ю., Аверченков, В.И. Системы защиты информации в ведущих зарубежных странах [Текст]: учебное пособие для вузов / Рытов М.Ю., Аверченков В.И.,

Кондрашин Г.В., Рудановский М.В. Брянск, 2007. – 225 - 227 с.

2. Алексеева, И.Ю. Информационные вызовы национальной и международной безопасности. [Текст] / Алексеева И.Ю., Федорова А.В., Цыгичко В.Н. Москва, 2009. – 23-25 с.

3. Барабанова, М.И., Кияев, В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях [Текст]: Учебное пособие. СПб., 2010. – 267-268 с.

4. Крутских, А.В. Технологический прогресс и современные международные отношения. [Текст]: Просвещение, 2014. – 448 - 450 с.

5. Леваков, А. Анатомия информационной безопасности США. [Текст]: Москва, 2002. - 39-51 с.

6. Пашков, В. Информационная безопасность США [Текст]: зарубежное военное обозрение. Москва, 2010. - 3-13 с.

7. Центральное разведывательное управление. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki. Дата обращения: 23.05.2019.

8. Организация защиты информации в США. [Электронный ресурс] – Режим доступа: https://studfiles.net/preview/848433/. Дата обращения: 25.05.2019.

9. Муравская, Н.Ю. Системы защиты информации в ведущих зарубежных странах. [Электронный ресурс] – Режим доступа: https://pandia.ru/text/78/544/54505-4.php. Дата обращения: 27.05.2019.

10. Особенности национальной защиты информации в США. [Электронный ресурс] – Режим доступа: https://tosaithe.wordpress.com/. Дата обращения: 29.05.2019.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Мартюшева Н.Ю., Исакова Т.С., студенты
Научный руководитель: Третьякова Т.И., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Интернет вещей (англ. internet of things, IoT) — концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Интернет вещей, как и любая быстроразвивающаяся технология, испытывает ряд «болезней роста», среди которых наиболее серьезной является проблема безопасности. Чем больше «умных» устройств подключается к сети, тем выше риски, связанные с несанкционированным доступом в IoT-систему и использованием ее возможностей злоумышленниками. Сегодня усилия многих компаний и организаций в сфере IT направлены на поиск решений, которые позволят минимизировать угрозы, тормозящие полноценное внедрение IoT.

«Умные», но уязвимые

Развитие концепции Интернета вещей и ее внедрение в различные сферы предусматривает наличие десятков миллиардов автономных устройств. По данным портала Statista в 2017 году их уже насчитывается более 20 млрд, а к 2025 году ожидается не менее 75 млрд. Все они подключены к Сети и передают через нее соответствующие их функционалу данные. И данные, и функционал являются мишенью для злоумышленников, а значит, должны быть защищены.

Для IoT-устройств безопасность заключается, прежде всего, в целостности кода, проверке подлинности пользователей (устройств), установлении правами владения (включая генерируемые ими данные), а также возможностью отражения виртуальных и физических атак. Но по факту, большинство из работающих сегодня IoT-устройств элементами защиты

не снабжены, имеют доступные извне интерфейсы управления, дефолтных пароли, т.е., имеют все признаки веб-уязвимости.

Все еще помнят события годичной давности, когда ботнет Mirai путем подбора комбинаций дефолтных логинов и паролей взломал большое количество камер и роутеров, которые были в дальнейшем использованы для мощнейшей DDoS-атаки на провайдерские сети UK Postal Office, Deutsche Telekom, TalkTalk, KCOM и Eircom. При этом «бутфорс» IoT-устройств осуществлялся при помощи Telnet, а роутеры взламывались через порт 7547 с использованием протоколов TR-064 и TR-069.

Но самой резонансной, пожалуй, была атака, положившая DNS-оператора DYN, а вместе с ним практически «пол-Интернета» США. Для атаки ботнетом был использован самый легкий путь через установленные по умолчанию логины и пароли устройств.

Указанные события наглядно продемонстрировали бреши в IoT-системах и уязвимость многих «умных» устройств. Понятно, что сбои чьих-либо «умных» часов или фитнес-трекеров особого вреда, кроме расстройства их хозяев, не принесут. Но вот взлом IoT-устройств, которые входят в системы и сервисы M2M, в частности, интегрированы в критическую инфраструктуру, чреват непредсказуемыми последствиями. В этом случае степень их безопасности должна соответствовать важности той или иной инфраструктуры: транспортной, энергетической или другой, от которых зависит жизнедеятельность людей и работа экономики. Также и на бытовом уровне — сбои и атаки на ту же систему «умный» дом могут привести к локальным коммунальным или иным аварийным и опасным ситуациям.

Безусловно, угрозы для инфраструктуры существовали и в «доинтернетовские» времена — например, из-за тех же стихийных бедствий или ошибок проектантов. Однако с появлением в ней подключенных к Сети устройств добавилась еще одна, и, наверное, на порядок серьезней — кибератака.

Сертификация устройств

Существующая проблема безопасности IoT-устройств возникла не из-за технической глупости или безалаберности их разработчиков. Здесь «торчат уши» трезвого расчета: быстрота выхода на рынок дает преимущество перед конкурентами, пускай и ненадолго, и даже за счет низкого порога защищенности.

Большинство производителей не заморачиваются тем, чтобы тратить время и деньги на разработки и тестирования кодов и систем безопасности своих «умных» изделий.

Одним из способов заставить их пересмотреть свое отношение к безопасности выпускаемых ими IoT-продуктов может стать сертификация. Идея не нова, но все же заслуживает на внимание, по крайней мере, это хоть какой-то путь решения проблемы. Процедура сертификации IoT-устройств не должна быть забюрократизированной и предоставлять покупателю гарантию, что оно имеет определенную степень защиты от хакерских атак. Для начала о необходимости наличия сертификата безопасности может быть указано при осуществлении государственных и корпоративных закупок.

Сегодня вопросами сертификации занимаются и несколько частных компаний. В частности, компания Online Trust Alliance (OTA) вышла с инициативой решения проблемы безопасности IoT на уровне государств и производителей, выпустив IoT Trust Framework — перечень критериев для разработчиков, производителей устройств и поставщиков услуг, который направлен на улучшение безопасности, конфиденциальности и жизненного цикла их IoT-продуктов. В первую очередь, он ориентирован на подключенные домашние, офисные и носимые устройства и является неким рекомендательным кодексом поведения и основой для нескольких программ сертификации и оценки рисков.

В текущем году независимым подразделением компании Verizon — ICSA Labs была запущена программа тестирования безопасности и сертификации IoT-устройств. Как утверждают ее разработчики, она является одной из первых в своем роде, и тестирует такие составляющие, как уведомление/протоколирование, криптография, аутентификация, связь, физическая безопасность и безопасность платформы. Устройства, которые прошли

сертификацию, будут отмечены специальным знаком одобрения ICSA Labs, указывающим на то, что они были тестированы, а обнаруженные уязвимости были устранены. Также прошедшие сертификацию устройства будут находиться под наблюдением и периодически тестироваться на протяжении всего их жизненного цикла для сохранения их безопасности.

В свою очередь программа тестирования и сертификации компании UL Cybersecurity Assurance (CAP) направлена на обеспечение безопасности продуктов и систем. Сертификация CAP удостоверяет, что продукт или система обеспечивают разумный уровень защиты от рисков, которые могут привести к непреднамеренному или несанкционированному доступу, изменению или сбою. Кроме того, CAP также подтверждает, что будущие патчи, обновления или новые версии ПО для сертифицированного продукта или системы не приведут к снижению уровня защиты, существующего на момент оценки.

Впрочем, многие эксперты по безопасности IoT считают, что наибольшая польза от таких программ сертификации будет при тестировании не только конкретного устройства, а всей экосистемы: используемой им инфраструктуры, приложений и т.д. Ведь протестированное и безопасное IoT-устройство может выйти из строя и в процессе взаимодействия внутри системы.

Имея безусловные плюсы для развития IoT, сертификационные программы имеют и обратную сторону. Один лишь факт прохождения устройством теста и наличие сертификата не может быть 100%-й гарантией его безопасности, поскольку, он, очень вероятно, все еще имеет определенные недоработки. Излишняя вера в сертификат безопасности может сыграть злую шутку с пользователями, у которых имеются индивидуальные потребности и различные варианты применения устройств, а значит, и собственные риски и угрозы. Ну и, конечно же, не исключена вероятность злоупотреблений. Наверняка найдутся производители, которые будут платить за «квазисертификацию», преследуя чисто коммерческие цели.

По всему выходит, что для глобального решения проблемы безопасности с помощью сертификации необходимо некое объединяющее решение, общий для всех производителей стимул выпускать защищенные устройства, а потребителям — не покупать те, безопасность которых ничем не подтверждается. Каким ему быть — законодательным, экономическим или карательным — еще предстоит решить. В конечном итоге, результатом должна стать безопасность глобальной системы Интернета вещей.

Блокчейн-технология

Безопасность Интернета вещей стала одной из первых сфер использования блокчейн-технологии. Благодаря технологии распределенного реестра появилась возможность обеспечивать высокий уровень безопасности IoT-устройств в сети и устранить существующие ограничения и риски для IoT, связанные с централизацией.

Она позволяет быстро и безопасно сохранять протоколы обмена и результаты взаимодействия различных IoT-устройств в децентрализованной системе. Именно распределенная архитектура блокчейна гарантирует достаточно высокую безопасность всей IoT-системы. Но если часть из устройств сети все же будет подвержена взлому, в целом, это не скажется на общей работе системы. Упомянутое использование ботнетами «умных» устройств, работающих в IoT-системах, стало возможным вследствие их слабой защищенности. Распределенный тип доверительных отношений позволяет избавиться от взломанного устройства без ощутимого ущерба для всей модели взаимодействия между «здоровыми» объектами.

В контексте безопасности сегодня блокчейн может использоваться в ряде сфер, в которых Интернет вещей развивается наиболее интенсивно. Например, это управление аутентификацией, проверка работоспособности разных сервисов, обеспечение неделимости информации и другие. В начале года ряд ведущих компаний, среди которых Cisco, BNY Mellon, Bosch, Foxconn и ряд других образовали консорциум, который будет находить решения по использованию блокчейна для увеличения безопасности и улучшения

взаимодействия IoT-продуктов. Главная задача, которую поставили перед собой его члены — разработка на основе блокчейн-технологии распределенной базы данных и протокола обмена информацией между IoT-устройствами.

Отметим, что в январе 2017 года DHS США начало использовать технологию блокчейн для защиты, передачи и хранения данных, которые собираются ведомством с камер видеонаблюдения и различных датчиков контроля. Технологию также тестирует и DARPA — подразделение Минобороны США, курирующее вопросы разработки новых технологий для армии. Кроме того, одно из агентств, ведущее исследования под крышей Пентагона, подписало контракт стоимостью несколько миллионов долларов с софтвер-компанией Galois, занимающейся разработками в сфере безопасности на базе блокчейна.

Сегодня уже очевидно, что реализовать все возможности, которые может предоставить пользователям концепция IoT без решения проблем с безопасностью и конфиденциальностью будет сложно. Указанные выше способы защиты IoT, конечно же, не являются исчерпывающими, над решением проблемы работают множество групп, компаний и энтузиастов. Но прежде всего высокий уровень безопасности устройств Интернета вещей должен быть основной задачей их производителей. Надежная защита должна изначально входить как часть функций изделия и стать новым конкурентным преимуществом, как для производителей, так и поставщиков комплексных IoT-решений.

Библиографический список

1. Википедия. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/
2. Леонид Черняк. Платформа Интернета вещей. Открытые системы. СУБД, №7, 2012. Открытые системы.
3. [Электронный ресурс] – Режим доступа: https://habr.com/ru/
4. Лагутенков, А. Тихая экспансия интернета вещей // Наука и жизнь. - 2018. - № 5. - С. 38-42.

ПОИСК И ИССЛЕДОВАНИЕ СЛЕДОВ КОМПРОМЕТАЦИИ, ЗАФИКСИРОВАННЫХ В ЛОГ-ФАЙЛАХ LINUX-СИСТЕМ

Ульянова М.А., студент Group-IB
Научный руководитель: Молодцова Ю.В., к. т. н., доцент
Национальный исследовательский университет Московский государственный технический университет им. Н.Э. Баумана
г. Москва

Аннотация: *статья посвящена исследованию лог-файлов в операционных системах семейства Linux. Так как операционные системы семейства Linux занимают одну из лидирующих позиций лидирующие позиции на рынке серверных систем то внимание к исследованию данных хранящихся в лог-файлах данных систем постоянно растет. В статье рассмотрены некоторые примеры базового и расширенного анализа содержимого лог-файлов операционной системы Linux при поиске и исследовании следов компрометации компьютерной системы.*

Ключевые слова: *получение доступа к данным, исследование лог-файлов, Linux, экспертиза.*

Исследование практики инцидентов компьютерной безопасности показало, что необходимо большое внимание уделять сбору максимального количества источников информации, поэтому особенную важность приобретает оптимизация механики алгоритма исследования. При этом лог-файлы, представляющие собой средство обеспечения журналирования событий компьютерной системы [1], являются одним из наиболее полных источников информации об инциденте, что обуславливает целесообразность их изучения. В

свою очередь операционные системы семейства Linux занимают лидирующие позиции на рынке серверных систем [2], чем объясняется акцентирование внимания на лог-файлах данных систем как объекте настоящего исследования.

Так как изначально файлы логирования предназначались для поиска системными администраторами произошедших в системе ошибок служб и приложений, в открытых источниках в основном содержится соответствующая общая информация. Однако перед специалистом в области информационной безопасности стоит несколько иная задача: поиск не только нештатных событий (процессов, завершившихся с ошибками), но и успешно завершенных (при этом нелегитимных) процессов. Тем не менее, на первоначальном этапе анализа и поиска [3] необходимо определить вектор поиска и сформировать перечень ожидаемых индикаторов компрометации в массиве иных событий, зафиксированных в лог-файлах. Для этого нами в рамках эксперимента были спланированы и проведены атаки на инфраструктуру собственной небольшой сети. При этом на каждом этапе фиксировались изменения, вносимые в файлы журналов операционной системы и различных сервисов, что позволило создать пул индикаторов компрометации, поиск которых целесообразно проводить в большинстве ситуаций. Так, была сконфигурирована сеть, состоящая из двух машин, на одной из которых были запущены серверные части служб SSH и TFTP, а также MySQL- ивеб-серверы. Описанная машина являлась атакуемой системой, как и wi-fi роутер, ставший точкой входа в инфраструктуру. Схема эксперимента представлена на Рисунке 1. Так, в центре расположена атакованная система, рядом с которой схематично изображены запущенные сервисы, прямыми стрелками обозначены направления подключения (атаки), волнистыми – механизм следообразования (лог-файлы, запись в которые происходит при совершении того или иного действия).

Таким образом, в случае использования злоумышленником основных векторов атаки (удаленная эксплуатация уязвимостей базовых серверных служб, подключение USB-устройства с целью выполнения с него произвольного кода), следы указанных действий фиксируются в перечне лог-файлов, представленном в таблице 1.

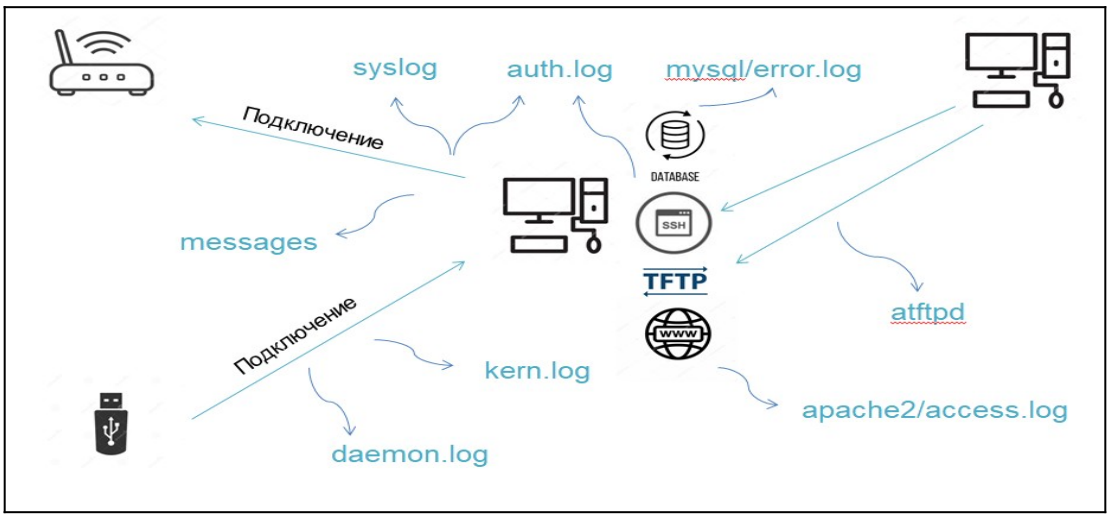

Рисунок 1 - Схема созданной инфраструктуры с отображением механики проведения эксперимента

Таблица 1 - Список целевых лог-файлов, расположенных в директории по умолчанию /var/log/

Файл	Описание
syslog, messages	Лог-файлы фиксации основных событий системы
auth.log	Лог-файл фиксации событий, связанных с попытками авторизаций в системе
btmp	Лог-файл фиксации неудачных попыток входа в систему
secure	Лог-файл фиксации событий, связанных с попытками авторизаций в

	системе (для RedHatCentOS)
boot.log	Лог-файл фиксации хода включения/выключения
mysql	Лог-файл сервера баз данных MySQL
cron	Лог-файл демона cron
maillogили mail.log	Лог-файл почтового сервера
proftpd, pureftpd.log	Лог-файл демона TFTP
samba	Лог-файлфайлового сервера Samba, который используется для доступа к общим папкам Windows и предоставления доступа пользователям Windows к общим папкам Linux.
apache2/access.log	Лог-файл веб-сервера Apache (для Ubuntu)
httpd	Лог-файл веб-сервера Apache (для RedHatCentOS)
yum.log, apt, pacman	Лог-файлы менеджеров пакетов Yum (CentOS), apt (Ubuntu), pacman (ArchLinux).

Так же в Linux-системах имеются лог-файлы, имеющие отдельное средство интерпретации. Вывод содержимого таких логов на экран осуществляется одноименной командой, если не указано иное.

Таблица 2. Список целевых лог-файлов одноименных служб, расположенных в директории по умолчанию /var/log/

Файл	Описание
tallylog	Лог-файл аудита неудачных попыток входа. Вывод на экран с помощью утилиты pam_tally2.
faillog	Лог-файл фиксации неудачных попыток входа в систему
dmesg	Лог-файл драйверов устройств
wtmp	Лог-файл фиксации попыток входа в систему. Вывод на экран командой utmpdump.

В силу того, что в лог-файлах высоконагруженной системы фиксируется колоссальное количество событий, оптимизация алгоритма поиска как средства минимизации времени становится одной из важнейших задач. При этом следует формировать запросы таким образом, чтобы выдача результата максимально коррелировала с типом события, однако не приводила к формированию перечня единичных событий (при анализе инцидента компьютерной безопасности интерес представляют связки событий/записей в лог-файлах). Обычно средства визуализации событий логирования содержатся в SIEM-системе, развернутой в сети компании. Однако расследование инцидента может проходить в сторонней организации, где такой системы не имеется, в связи с чем необходимо разрабатывать собственные механики фильтрации логированных событий. Так, нами были использованы регулярные выражения, которые могут быть использованы, к примеру, в связке с утилитой grep (стандартное средство поиска, имеющееся в Linux-системах).

Рассмотрим логику поиска индикаторов компрометации на примере эксплуатации службы SSH. В каждом случае с помощью утилиты grep возможно реализовать как полнотекстовый поиск (по вхождению строки), так и поиск окружения (за несколько строк до или после, поиск контекста). В случае анализа событий службы SSH предпочтителен второй вариант, так как, во-первых, синтаксис записей данной службы стандартен и для иных сервисов, а во-вторых, данная служба не имеет отдельного лог-файла, в связи с чем поиск ведется среди множества нерелевантных записей, которые не должны попадать в выдачу, мешая аналитику. Пример записей событий логирования службы SSH представлен на рисунке 2. Рамкой оранжевого цвета выделена запись, фиксирующая успешное подключение локального пользователя none; рамкой желтого цвета выделены записи, фиксирующие неудачные попытки подключения пользователей sshd, unknown, admin; рамкой красного цвета выделена запись, фиксирующая удачное подключение удаленного пользователя test.

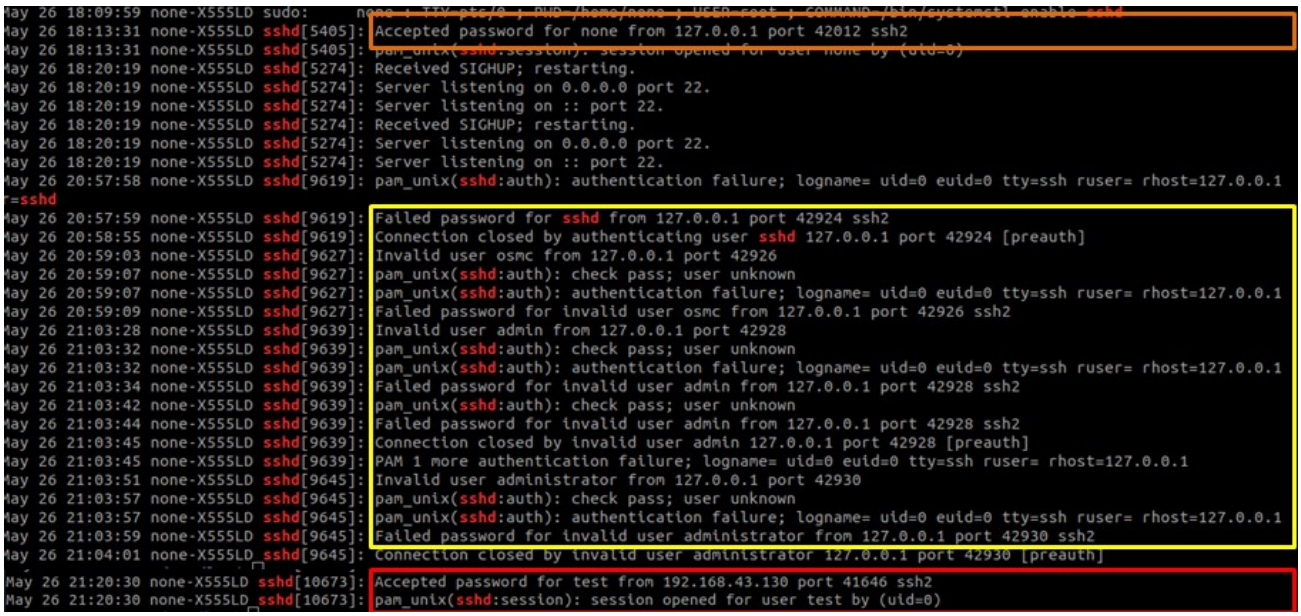

Рисунок 2 - Фрагмент окна эмулятора терминала Ubuntu с содержимым лог-файла «auth.log», относящимся к демону sshd

Так, для формирования перечня событий удачных попыток удаленного соединения с хостом посредством службыSSHнами использовано регулярное выражение следующего вида: «sshd.*192\.168.{,60}ses.*open», что будет соответствовать двум соседним записям лог-файла.

Для автоматизации поиска нами создавались скрипты и модули на языке программирования Python, так как регулярные выражения в данном случае компилируются в объекты шаблонов, имеющие методы для различных операций (например, поиск вхождения шаблона). Фрагмент кода подобного скрипта приведен в Листинге 1.

Листинг 1. Фрагмент кода скрипта для выполнения поиска событий удачных попыток удаленного соединения с хостом посредством службы SSH в лог-файле

```
>>>importre
>>>ssh_remote_locnet = re.compile(sshd.*192\.168.{,60}ses.*open ', re.DOTALL)
>>>printssh_remote_locnet
```

Так, в функции re.compile() указываются дополнительные аргументы, использующиеся для добавления особенностей синтаксиса. В данном случае был передан аргумент «re.DOTALL», при помощи которого метасимвол «.» соответствует в том числе и символу перевода строки.

Регулярное выражение передается re.compile() как строка. Регулярные выражения обрабатываются как строки, поскольку не являются частью языка Python, и нет никакого специального синтаксиса для их выражения. Вместо этого имеется модуль re, представляющий собой обертку модуля на C, подобно модулям socket или zlib [4].

Таким образом, лог-файлы являются одним из основных источников данных для анализа. Даже при базовом уровне логирования файлы журналов содержат большое количество информации, позволяющей установить факт и обстоятельства компрометации системы, что обуславливает значимость лог-файлов при расследовании компьютерных инцидентов.

Библиографический список

1. Логи: разбираемся с понятием лог файл [Электронный ресурс]: THELOCAL-HOST.RU. URL: http://thelocalhost.ru/log/ (Дата обращения: 20.10.2019).

2. Рейтинг серверных операционных систем. [Электронный ресурс]: TAGLINE. Рейтинги сервисов и технологий. URL: https://tagline.ru/server-operating-systems-rating/ (Дата обращения: 20.10.2019).

3. Development of general models of information analysis received during the conduct of in-

formation and analytical research. Molodtsova Y.V. Information Innovative Technologies: Materials of the International scientific – practical conference. (Czech Republic, Prague, 2019 April 22-26). M.: HSE, 2019. – Part 3: Innovative Information Technologies in Industry and Social-Economic Sphere. - P. 262-266.

4. iPython R Rapid Miner [Электронный ресурс]: pythonr.blogspot. URL: http://python-r.blogspot.com/2015/01/regular-expressions-python.html (Дата обращения: 20.10.2019).

5. An attitude of citizens to state control over the internet traffic. Akhmadieva R.S., Ignatova L.N., Bolkina G.I., Soloviev A.A., Gagloev D.V., Korotkova M.V., Burenina V.I. Eurasian Journal of Analytical Chemistry. 2018. Т. 13. № 1b. С. em82.

6. Буренина, В.И. Система законодательства, регулирующего научно-техническую деятельность: проблемы и противоречия. Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2013. № 9-1 (35). С. 19-24.

7. Арсенькина, Л.С. Нормативное регулирование использования аппаратных блокираторов в рамках судебной компьютерно-технической экспертизы в российской федерации В сборнике: Источники частного и публичного права Сборник научных трудов по материалам VII ежегодной международной научно-практической конференции (с элементом школы молодого ученого для студентов юридических специальностей). 2017. С. 13-16.

ОБЗОР РЕШЕНИЙ BREACH AND ATTACK SIMULATION ПО ПРАКТИЧЕСКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шамрицкий К.Г., студент
Научный руководитель: Третьякова Т.И., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Тест на проникновение является одним из наиболее распространенных вариантов оценить надежность систем защиты, показать возможные методы проведения атак, определить реально существующие проблемы безопасности. Однако такие тесты (пентесты) требуют значительной доли участия человека, предпринимаются с определенной частотой и в сжатые сроки. Результаты этих тестов отражают статичную картину, актуальную на момент проведения. Продукты по моделированию нарушений и атак (Breach and Attack Simulation или BAS) являются новым развивающимся рынком средств, которые выполняют автоматическое тестирование безопасности на регулярной основе. Рассмотрим внимательнее этот рынок и его драйверы, основные продукты данной области, а также прогнозы.

Последние оценки TAdviser в очередной раз показали, что рынок информационной безопасности в России растет. Этот рост в 2018 году составил порядка 10%. На мировом рынке ИБ так же отмечается стремительный рост. В следствии этого, бизнес уделяет все больше внимания задачам, направленным на защиту своих информационных активов увеличивая бюджет кибербезопасности. Внедряются новые аппаратные и программные средства. Однако для ИБ-департаментов по-прежнему остаются открытыми вопросы:

насколько хорошо защищена наша ИТ-инфраструктура сегодня?

какова вероятность подвергнуться атаке в будущем?

какие действия необходимо предпринять для увеличения эффективности мер борьбы с угрозами?

Для ответа на эти вопросы рынок предлагает относительно новый класс ИБ-решений — Breach and Attack Simulation (BAS). Это продукты, которые позволяют имитировать атаки на инфраструктуру по различным векторам, после чего на основе получаемых результатов делать выводы об эффективности принятых мер. Так же они позволяют оценивать риски вторжения и давать рекомендации по сокращению этих киберрисков. Они способны существенно дополнить комплекс ИБ-решений компании с помощью постоянного анализа

механизмов защиты.

Рынок BAS

Термин BAS (Breach and Attack Simulation) начал впервые использоваться в 2017 году после публикации компанией Gartner цикла зрелости (Hype cycle) различных классов решений в области информационной безопасности (рисунок 1).

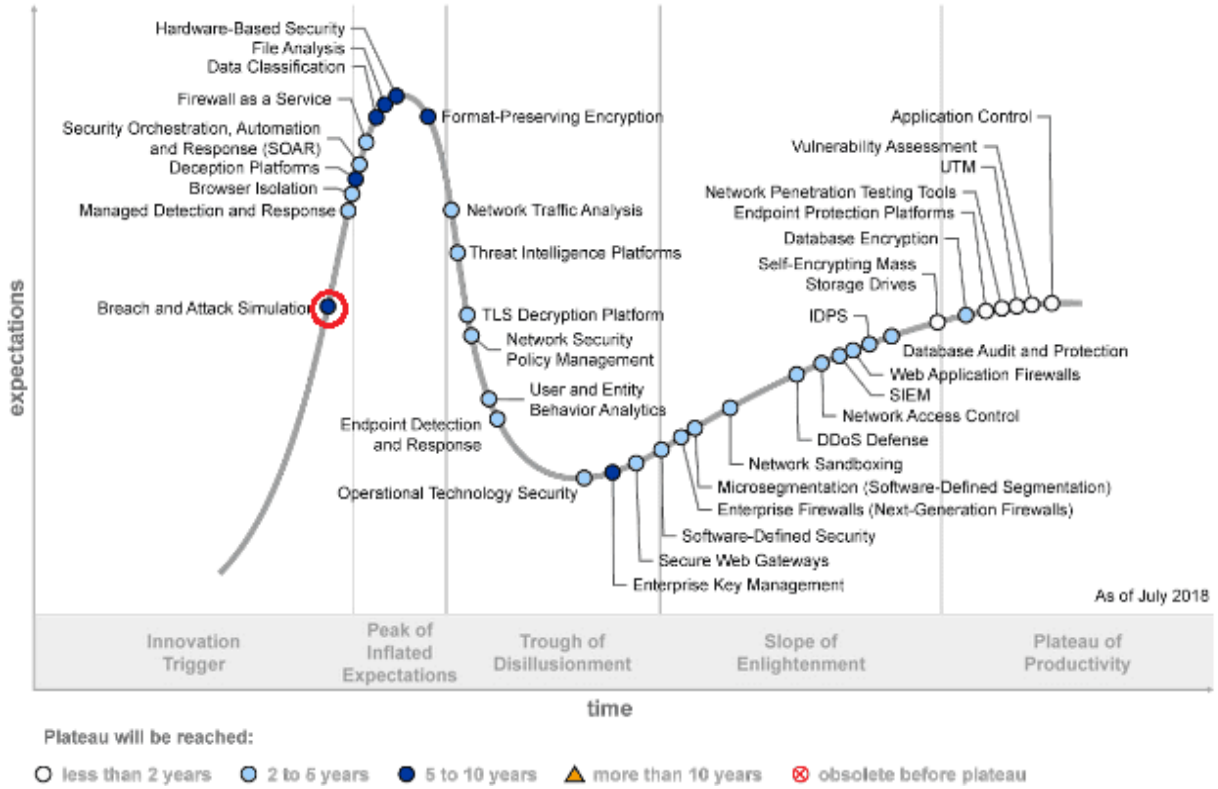

Рисунок 1- «Цикл хайпа» Gartner для решений по защите информации, 2018 год

Продукты класса BAS на сегодняшний день все еще находятся в стадии «технологического старта», на заре появления технологии. При этом рынок окончательно не сформирован, интерес к таким решениям растет, ожидается резкое увеличение их популярности. Среди причин такого роста рынка BAS можно выделить следующие:

возрастающие убытки от кибератак приводят к переходу от безопасности «на бумаге» к фактической защищенности, к необходимости построить максимально эффективную систему борьбы с угрозами;

компаниям необходимо выполнять существующие регуляторные требования по анализу защищенности;

большой выбор решений на рынке ИБ предполагает сложность выбора определенного продукта и к потребности объективно определять то, насколько эффективно защитные механизмы работают;

ИТ-инфраструктура - живой организм, она регулярно видоизменяется, при этом постоянно появляются новые угрозы и уязвимости, в связи с чем появляется необходимость регулярного тестирования безопасности;

услуги по непрерывному тестированию на проникновение или собственную команду Red Team может позволить себе не каждое даже крупное предприятие.

Возможности BAS и принцип его работы

Поскольку рынок BAS относительно новый, существующие решения довольно значительно отличаются друг от друга используемыми технологиями и функциональными возможностями: векторы моделируемых атак и их предопределённые шаблоны разнообразны, некоторые продукты позволяют оценить уровень риска, предлагают рекомендации по устранению обнаруженных угроз, учитывают соблюдение нормативных

требований (compliance). Большинство решений доступно в виде SaaS (англ. software as a service — программное обеспечение как услуга), некоторые разворачиваются локально. Некоторые продукты нуждается в установке агентов, другие работают без них и т.д. Однако есть схожий набор функций, который предоставляют все вендоры.

Продукты класса BAS позволяют компаниям самостоятельно и непрерывно определять степень своей защищённости, оценивать механизмы обеспечения безопасности, имитируя атаки по разным векторам. Примерами могут послужить фишинговые рассылки, моделирование случаев утечки конфиденциальной информации из внутренней сети, эмуляция сетевых атак, вредоносной активности. Большинство решений согласуется с платформой MITRE ATT&CK для тестирования по сценариям определенного типа.

Наглядные отчеты тестов позволяют определить текущий уровень информационной безопасности (как правило, по количественной шкале от 0% до 100%), оценить эффективность работы определенных средств защиты, принять правильное решение о том, какие меры необходимо реализовать в первую очередь.

Обзор наиболее популярных продуктов

Компания AttackIQ (https://attackiq.com) была основана в 2013 году группой экспертов с многолетним опытом работы в области консалтинга по безопасности, тестирования на проникновение, исследования угроз, моделирования атак, разработки продуктов и сопутствующих услуг. Штаб-квартира: Калифорния, США.

FireDrill является клиент-серверным приложением. Консоль управления может быть развернута как локально, на физическом или виртуальном сервере, так и облачно (рисунок 2). Необходима установка агентов. Библиотека содержит более 1200 предопределенных сценариев атак, каждый из которых может быть изменен пользователем.

Ценообразование зависит от количества агентов и начинается с 20 000 долларов.

Компания Cronus Cyber Technologies CyBot (https://cronus-cyber.com) основана в 2014 г. Штаб-квартира: Израиль.

CyBot Cronus определяет уязвимости и оценивает их приоритеты с точки зрения критичности для бизнес-процессов компании, а также строит вероятные сценарии атак с использованием методов машинного обучения, оценивает бизнес-риски. Имеет ядро решения (CyBot Pro) и 2 консоли управления — для MSSP и корпораций.

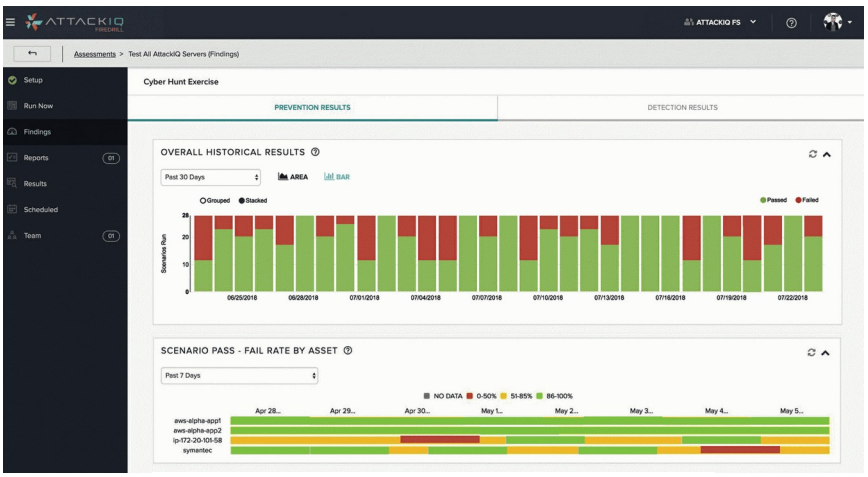

Рисунок 2 - Интерфейс AttackIQ FireDrill

Ценообразование — по запросу.

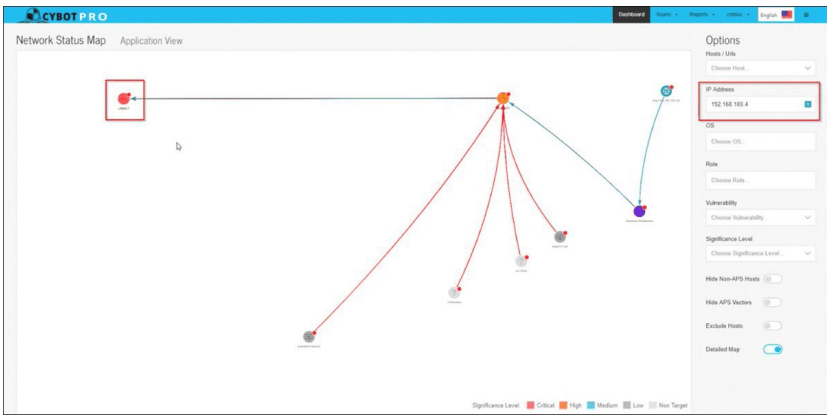

Рисунок 3 - Карта сети в CyBot Pro

Компания Cymulate (https://cymulate.com) была основана в 2016 г. элитной командой бывших офицеров разведки ИДФ, которая выявила разочаровывающую неэффективность своих операций по обеспечению кибербезопасности. Отсюда вытекает их миссия - расширять возможности организаций по всему миру и делать передовую кибербезопасность такой же простой и знакомой, как отправка электронной почты. Сегодня Cymulate доверяют сотни компаний по всему миру, в том числе ведущие банки и финансовые службы.

Решение типа SaaS, предлагает проверку средств защиты информации, сотрудников и процессов ИБ. Предоставляет возможности тестирования по 8 векторам атак, генерирует отчеты для руководителей и технического персонала, включающие практические рекомендации по устранению обнаруженных проблем. Необходимо установить один агент для выполнения симуляций и просмотра результатов (рисунок 4). Об особенностях реализации метода BAS на платформе Cymulate можно прочитать на нашем сайте.

Ценообразование: от 30 000 до 500 000 долларов в зависимости от размера компании и количества моделируемых векторов атак.

Компания Guardicore (https://www.guardicore.com/infectionmonkey) основана в 2013 г, штаб-квартира: Калифорния, США. Guardicore - это компания, занимающаяся центрами обработки данных и облачной безопасностью, которая защищает основные активы вашей организации, используя гибкие, быстро развертываемые и понятные средства управления микросегментацией. Наши решения предоставляют более простой и быстрый способ гарантировать постоянную и согласованную безопасность - для любого приложения, в любой ИТ-среде.

Infection Monkey - инструмент для моделирования атак с открытым исходным кодом, который оценивает устойчивость частных и общедоступных облаков к нападениям злоумышленников (рисунок 5). Позволяет проводить автоматическую симуляцию кражи учетных данных, неправильной конфигурации, компрометации активов и других видов вредоносной активности.

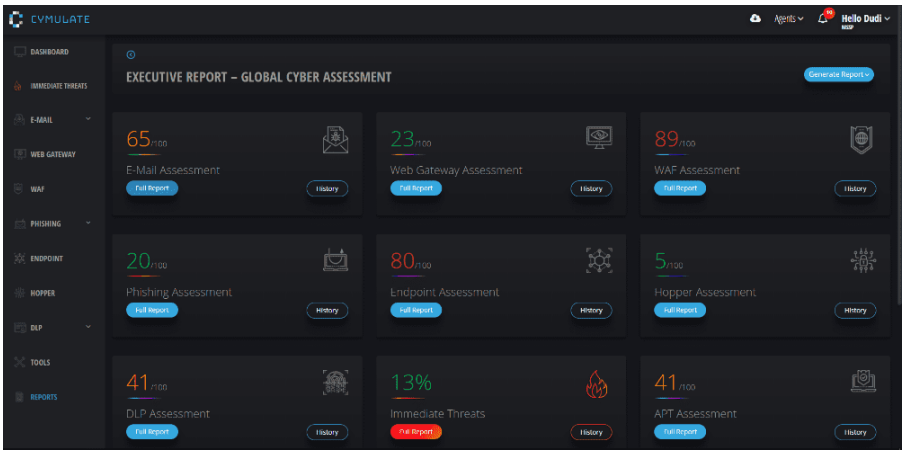

Рисунок 4 - Отчеты Cymulate

Guardicore Infection Monkey

Лицензируется как свободно распространяемое программное обеспечение.

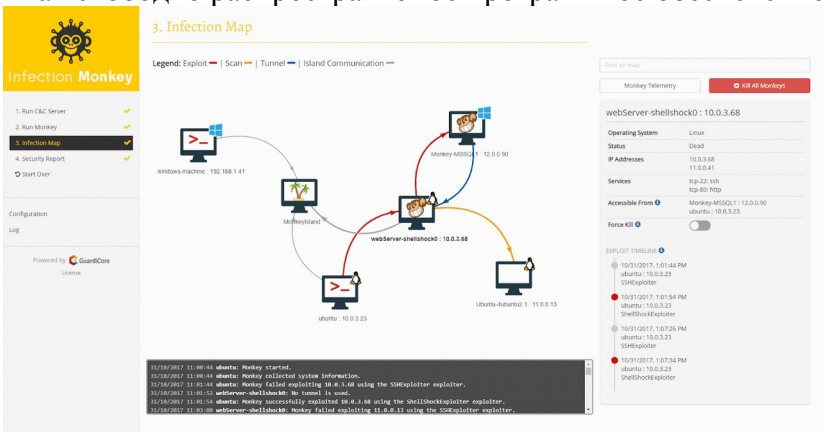

Рисунок 5 - Панель визуальной карты атак в Guardicore Infection Monkey

Компания SafeBreach Breach & Attack Simulation Platform (https://safebreach.com) основана в 2014 г., штаб-квартира: Кремниевая долина, США.

Платформа непрерывной проверки безопасности SafeBreach способна моделировать более 3600 способов атак по всей цепочке – от заражения электронной почты до компрометации конечных точек и всех промежуточных этапов. Включает серверную часть «Orchestrator», разворачиваемую в облаке, и клиентские симуляторы атак «Breach Simulators», которые устанавливаются локально (рисунок 6).

Ценообразование зависит от количества развернутых симуляторов: например, для десяти экземпляров цена составляет 50 000 долларов в год.

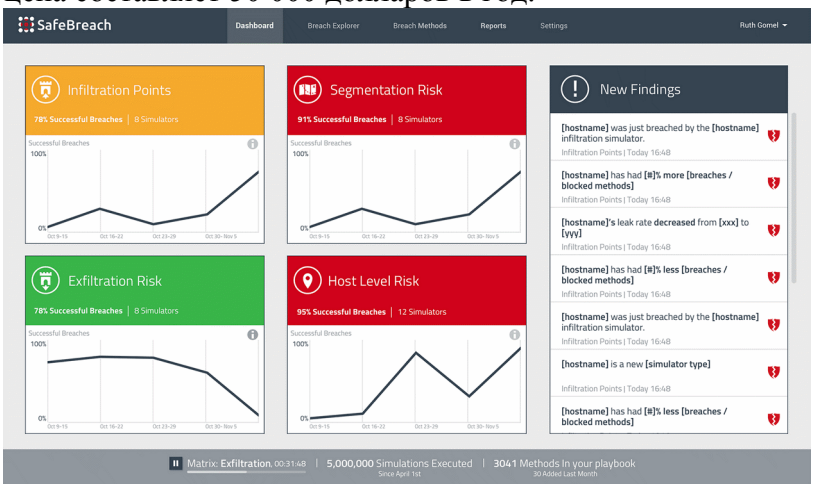

Рисунок 6 - Информационная панель SafeBreach Breach & Attack Simulation Platform

Компания XM Cyber HaXM (https://xmcyber.com) была основана в 2016 г., штаб-квартира: Израиль. XM Cyber была основана высокопоставленными сотрудниками службы безопасности из элитного разведывательного сектора Израиля. Вместе они приносят непревзойденный, проверенный послужной список в наступательном и оборонительном киберпространстве.

HaXM от XM Cyber позволяет имитировать атаки злоумышленников на ресурсы организации и предотвращать последствия в режиме 24×7 (рисунок 7). HaXM объединяет и автоматизирует действия команд нападающих (Red Team) и защитников (Blue Team), чтобы обеспечить, с одной стороны, полный реалистичный сценарий APT (Advanced Persistent Threat), а с другой - приоритетное восстановление.

Ценообразование - по запросу.

Рисунок 7 - Визуализация действий Red Team и Blue Team на сетевых ресурсах компании в XM Cyber HaXM

Компания Picus Breach & Attack Simulation Platform (https://www.picussecurity.com) основана в 2013 г., штаб-квартира: Сан-Франциско, США. Будучи пионером технологий Breach & Attack Simulation, Picus разработал новый и целостный подход к информационной безопасности: непрерывная проверка безопасности.

Независимо от какого-либо поставщика или технологии, беспрецедентная платформа Picus разработана для непрерывного измерения эффективности средств защиты с использованием новых образцов угроз в производственных средах. Созданная командой, которая работает вместе более 10 лет и доказала свою компетентность в области корпоративной кибербезопасности, Picus пользуется доверием многих крупных транснациональных корпораций и государственных учреждений.

Платформа симуляции атак от Picus является одной из первых на рынке технологий BAS(рисунок 8). Непрерывно моделирует киберугрозы в режиме реального времени, включает модули для симуляции атак по e-mail, HTTP/HTTPS, вредоносных действий против рабочих станций. Лаборатория Picus непрерывно пополняет собственную базу данных актуальных угроз.

Ценообразование также предоставляется по запросу (рисунок 8).

Компания Threatcare App (https://www.threatcare.com) основана в 2014 г., штаб-квартира: Техас, США. Threatcare представляет собой клиентское приложение, позволяющее активно сканировать систему и анализировать киберугрозы. Проводит оценку средств защиты, моделирование атак по расписанию и киберучения. С использованием агентов Threatcare позволяет планировать сценарии проведения атак одновременно в нескольких сетях (рисунок 9).

Ценообразование: от $33 в месяц за Pro-версию, также имеется бесплатная версия, доступная для скачивания на официальном сайте (рисунок 9).

Компания Verodin SECURITY INSTRUMENTATION PLATFORM (SIP) (https:// www.verodin.com) основана 2014 г., штаб-квартира: Вашингтон, США.

Инструментальная платформа безопасности Verodin использует ИТ-среды заказчика для проверки эффективности управления сетью, конечными точками, электронной почтой и облаком. SIP постоянно выполняет тесты и анализирует результаты, чтобы своевременно предупреждать о найденных угрозах. Предоставляет данные, которые показывают, действительно ли средства защиты обеспечивают желаемые результаты.

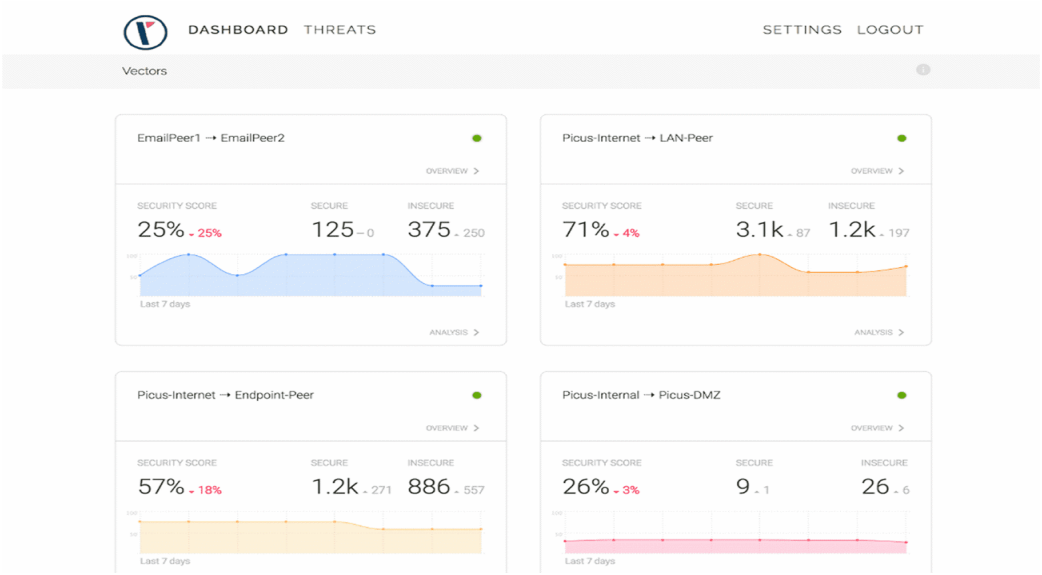

Рисунок 8 - Информационная панель Picus Breach & Attack Simulation Platform

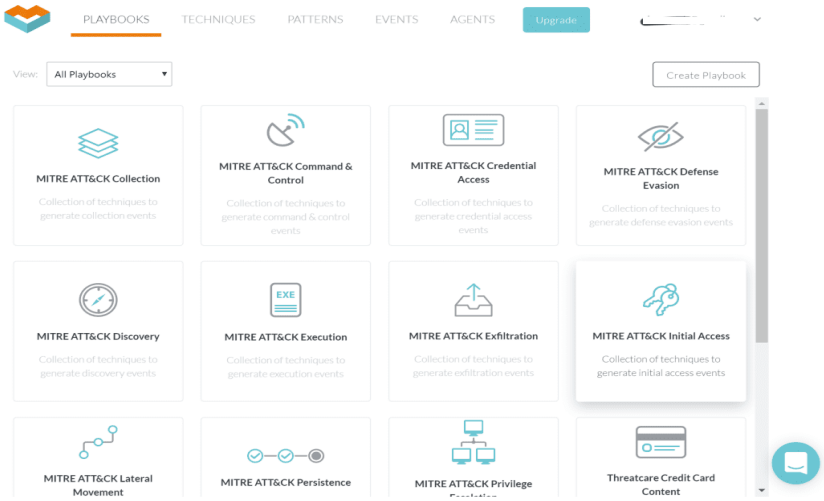

Рисунок 9 - Панель сценариев атак Threatcare App

Ценообразование — по запросу.

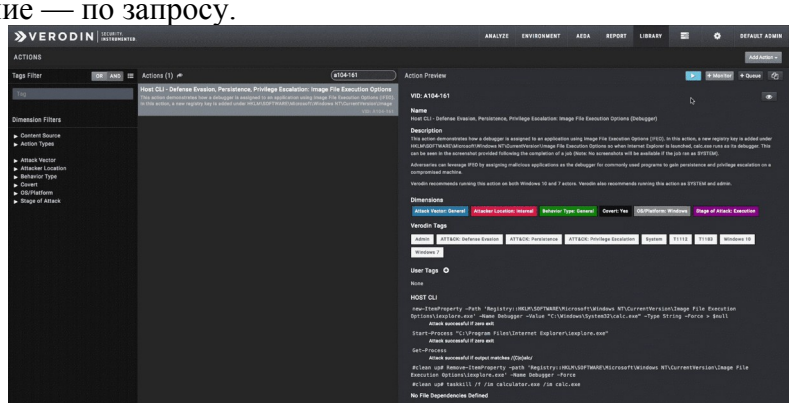

Рисунок 10 - Панель просмотра действий в Verodin SECURITY INSTRUMENTATION PLATFORM

Инструменты с открытым исходным кодом

Помимо описанных выше продуктов существует немало общедоступных инструментов, которые позволяют реализовать отдельные функции по симуляции атак и нарушений. К ним можно отнести, например, Metta от Uber, Atomic Red Team от Red Canary, Red Team Automation от Endgame и другие. Основным недостатком таких средств является высокий порог входа, поэтому они используются специалистами для решения локальных задач.

Кроме того, у этих разработок нет удобного пользовательского интерфейса и системы генерации отчетов.

Несмотря на возрастающую популярность решений для автоматической симуляции атак, BAS вряд ли сможет когда-либо полностью заменить классический пентест. Однако продукты данного типа способны существенно изменить рынок практической безопасности, так как предлагают более быстрый и дешевый способ оценки защищенности по сравнению с ручным тестированием на проникновение. По прогнозам CyberDB, мировой рынок средств автоматизации пентеста достигнет 1 миллиарда долларов к 2020 году.

Таким образом, использование BAS-решений для непрерывной оценки безопасности способно значительно повысить уровень фактической защищенности ИТ-инфраструктуры. А в комплексе с периодическим проведением классического пентеста компании смогут получить наиболее полную и объективную картину собственной защищенности и оценить свою готовность к отражению реальных кибератак.

Библиографический список

1. Данные TAdviser о выручке российских компаний на рынке ИБ в 2017-2018 годах. [Электронный ресурс] – Режим доступа: http://www.tadviser.ru/

2. Данные TAdviser со ссылкой на центр Canalys https://www.canalys.com/ по категориям продуктов информационной безопасности с наибольшими расходами на мировом рынке. [Электронный ресурс] – Режим доступа: http://www.tadviser.ru/index.php/

3. Данные по «циклу зрелости» (Hyper Cycle) от компании Gartner. [Электронный ресурс] – Режим доступа: https://www.gartner.com/en/documents/3762274

Информация с сайтов, реализующих свои продукты в сфере BAS:

4. AttackIQ FireDrill. [Электронный ресурс] – Режим доступа: https://attackiq.com

5. Cronus Cyber Technologies CyBot. [Электронный ресурс] – Режим доступа: https://cronus-cyber.com

6. Cymulate APT. [Электронный ресурс] – Режим доступа: https://cymulate.com

7. Guardicore Infection Monkey. [Электронный ресурс] – Режим доступа: https://www.-guardicore.com/infectionmonkey

8. SafeBreach Breach & Attack Simulation Platform. [Электронный ресурс] – Режим доступа: https://safebreach.com;

9. XM Cyber HaXM. [Электронный ресурс] – Режим доступа: https://xmcyber.com;

10. Picus Breach & Attack Simulation Platform. [Электронный ресурс] – Режим доступа: https://www.picussecurity.com;

11. Threatcare App. [Электронный ресурс] – Режим доступа: https://www.threatcare.com

12. Verodin SECURITY INSTRUMENTATION PLATFORM (SIP). [Электронный ресурс] – Режим доступа: https://www.verodin.com.

13. Данные прогноза компании CyberDB по объему мирового рынка средств автоматизации пентеста. [Электронный ресурс] – Режим доступа: https://www.cyberdb.co/.

ЭКОЛОГО-ОРИЕНТИРОВАННЫЙ ПОДХОД КОМПЛЕКСНОЙ ОЦЕНКИ УСЛОВИЙ ТРУДА ЭЛЕКТРОГАЗОСВАРЩИКА

Антипова А.Ю., студент
Научный руководитель: Богатова И.Б., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Комфортные и безопасные условия труда - один из основных факторов, влияющих на производительность и безопасность, здоровье работников.

Актуальность данной работы определяет растущий уровень опасности рабочих мест на предприятиях, в основном из-за усложнения технологий и вредности материала и сырья. Изучение и решение проблем, связанных с обеспечением здоровой и безопасной среды, в которой осуществляется человеческий труд, является одной из важнейших задач производственных систем и предприятий. Экологическую оценку можно охарактеризовать как соответствующий анализ экологического последствия и рисков работы по специальности на конкретном рабочем месте с целью обеспечения экологической безопасности с установлением степени ее опасности и предложением обеспечительных мер.

Цель данного исследования: Дать оценку условий труда электрогазосварщика на предприятии (на примере АО« Аком-Индастриал ») и разработать предложения по повышению безопасности труда.

Для достижения этой цели, поставлены задачи:

- Изучить документацию в области экологической безопасности условий труда;
- Выявить вредные и опасные факторы, воздействующие на электрогазосварщика;
- Провести специальную оценку труда;
- Сформулировать предложения по улучшению условий труда электрогазосварщика.

Предмет исследования - комплексная оценка условий труда электрогазосварщика.

Объект исследования - рабочее место (зона) электрогазосварщика на предприятии «Аком-Индастриал».

Условия труда - совокупность факторов рабочей среды и трудового процесса, влияющих на работоспособность и здоровье работника. Специальная оценка условий труда представляет собой единый комплекс последовательно реализуемых мер по выявлению вредных и (или) опасных факторов рабочей среды и процесса труда (далее также называемых вредными и (или) опасными производственными факторами) и оценки уровня их влияние на работника с учетом отклонения их фактических значений от норм, установленных федеральным органом исполнительной власти, уполномоченных Правительством Российской Федерации (гигиенические нормативы) условий труда и использования средств индивидуальной и коллективной защиты работников [1].

Безопасность — это состояние деятельности, при которой с определенной вероятностью исключаются потенциальные опасности, влияющее на здоровье человека [2].

По результатам проведения специальной оценки условий труда устанавливаются классы условий труда, которые указывают на вредность или опасность для работника. Результатами установления класса условий труда могут быть разработка и реализация мероприятий, направленных на улучшение условий, а так же расчёт льгот и компенсаций для работников [1].

Обязанность проводить специальную оценку установлена ст. 212 ТК РФ и Федеральным законом «Об особой оценке условий труда» № 426-ФЗ от 28 декабря 2013 г.

Проведение специальной оценки условий труда регламентировано:

- федеральным законом "О специальной оценке условий труда" от 28.12.2013 № 426-ФЗ (далее ФЗ 426) [1].

- приказом Минтруда РФ от 24.01.2014 №33н, которым утверждены "Методика проведения специальной оценке условий труда"; "Классификатор вредных и (или) опасных производственных факторов"; "Отчет о проведении специальной оценки условий труда"; "Инструкция о заполнении формы данного отчета".

- приказом Минтруда РФ от 07.02.2014 № 80н, которым утверждены "Форма и порядок подачи декларации соответствия условий труда государственным нормативным требованиям охраны труда"; "Порядок формирования и ведения реестра деклараций соответствия условий труда государственным нормативным требованиям охраны труда".

- приказом Минтруда РФ от 24.01.2014 №32н, которым утверждены: "Форма сертификата эксперта на право выполнения работ по специальной оценке условий труда, технические требований к нему"; "Инструкция по заполнению бланка сертификата эксперта на право выполнения работ по специальной оценке условий труда"; "Порядок формирования и ведения реестра экспертов организаций, проводящих специальную оценку условий труда".

Специальная оценка проводится работодателем совместно с организацией, проводящей специальную оценку условий труда. Частота проведения такой оценки 1 раз в 5 лет.

В целях проведения специальной оценки условий труда исследованию (испытанию) и измерению подлежат следующие вредные и (или) опасные факторы производственной среды:

1. Физические факторы – аэрозоли преимущественно фиброгенного действия, шум, инфразвук, ультразвук воздушный, вибрация общая и локальная, неионизирующие излучения (электростатическое воле, постоянное магнитное поле, в том числе гипогеомагнитное, электрические и магнитные поля промышленной частоты (50 Герц), переменные электромагнитные ноля, в том числе радиочастотного диапазона и оптического диапазона (лазерное и ультрафиолетовое), ионизирующие излучения, параметры микроклимата (температура воздуха, относительная влажность воздуха, скорость движения воздуха, инфракрасное излучение), параметры световой среды (искусственное освещение (освещенность) рабочей поверхности);

2. Химические факторы – химические вещества и смеси, измеряемые в воздухе рабочей зоны и на кожных покровах работников, в том числе некоторые вещества биологической природы (антибиотики, витамины, гормоны, ферменты, белковые препараты), которые получают химическим синтезом и (или) для контроля содержания которых используют методы химического анализа;

3. Биологические факторы – микроорганизмы-продуценты, живые клетки и споры, содержащиеся в бактериальных препаратах, патогенные микроорганизмы – возбудители инфекционных заболеваний.

В целях проведения специальной оценки условий труда исследованию (испытанию) и измерению подлежат вредные и (или) опасные факторы трудового процесса:

1. Тяжесть трудового процесса – показатели физической нагрузки на опорно-двигательный аппарат и на функциональные системы организма работника;

2. Напряженность трудового процесса – показатели сенсорной нагрузки на центральную нервную систему и органы чувств работника[3].

Далее выводят гигиенические критерии для каждого производственного фактора, гигиенические критерии - это показатели, характеризующие степень отклонений параметров факторов рабочей среды и трудового процесса от действующих гигиенических нормативов [4]. Исходя из степени отклонения фактических уровней факторов рабочей среды и трудового процесса от гигиенических нормативов, условия труда по степени вредности и опасности условно подразделяются на 4 класса: оптимальные, допустимые, вредные и опасные [5].

Исследование проводилось на аккумуляторном производстве ООО «АКОМ-Индастриал», это перспективное предприятие группы компаний. Первый резидент Территории перспективного развития (ТОР) г. Тольятти.

В процессе работы проведен анализ и выполнена оценка вредных и опасных факторов

рабочего места газоэлектросварщика. Итоги специальной оценки труда на рабочем месте электрогазосварщика на предприятии ООО «АКОМ-Индустриал» по всем факторам:

- Химический фактор: класс условий труда 3.1;
- Аэрозоли преимущественно фиброгенного действия: класс условий 3.1;
- Шум: класс условий 3.2;
- Локальная вибрация: класс условий 2;
- Неионизирующее излучение: класс условий 3.1;
- Параметры микроклимата: класс условий 3.1;
- Тяжесть трудового процесса: класс условий 2.

Итоговый класс, обозначается по самому вредному выявленному фактору, в данном случае – шум. Итоговый класс (подкласс) условий труда 3.2. Это такие условия труда, при которых на работника воздействуют вредные и (или) опасные производственные факторы, уровни воздействия которых способны вызвать стойкие функциональные изменения в организме работника, приводящие к появлению и развитию начальных форм профессиональных заболеваний или профессиональных заболеваний легкой степени тяжести возникающих после продолжительной экспозиции. Правовые последствия такой работы выражается в повышенной оплате труда, ежегодном дополнительном отпуске, выдаче молока или других равноценных пищевых продуктов, а так же льготное пенсионное обеспечение.

Рекомендуемые мероприятия по улучшению условий труда на рабочем месте электрогазосварщика:

1. Для снижения вредного воздействия химического фактора использовать средства индивидуальной защиты органов дыхания, например респиратор. Так же сохранить за работником право на льготы и спец. питание (молоко). В перерывах выходить на свежий воздух. Так же обеспечить правильную и частую чистку очистительных сооружений в помещении;

2. Шум, являясь общебиологическим раздражителем, оказывает влияние не только на слуховой анализатор, но действует на структуры головного мозга, вызывая сдвиги в различных функциональных системах организма. Для ограничения вредного воздействия шума использовать средства индивидуальной защиты органов слуха (противошумные наушники, беруши), применение звукоизоляции, звукопоглощения, демпфирования и глушителей шума, введение регламентированных дополнительных перерывов;

3. Для нормальной жизнедеятельности человека необходимы как чистый воздух и свет, так и ультрафиолетовое излучение. Однако, длительное воздействие больших доз ультрафиолетового излучения может привести к поражению глаз и кожи. Для снижения вредного воздействия ультрафиолетового излучения использовать спецодежду с длинными рукавами и капюшоном, противосолнечные экраны, окраска помещений водными составами (меловым и известковым), очки со стеклами, содержащими оксид свинца и другие спецсредства защиты лица и рук, не пропускающих излучение, так же кремы для кожи;

4. Микроклимат производственных помещений – это комплекс физических факторов, оказывающих влияние на теплообмен человека и определяющих самочувствие, работоспособность, здоровье и производительность труда. Жизнедеятельность человека может нормально протекать лишь при условии сохранения температурного гомеостаза организма. Категории работ разграничиваются на основе интенсивности энергозатрат организма, в ккал/ч (Вт). У электрогазоварщика газорезательные работы – категория работ IIа, Сварочные работы – категория работ IIа, и отдельно рабочее место электрогазосварщика - категория работ IIб [5]. На рабочем месте газоэлектросварщика наблюдается нагревающий микроклимат. Это микроклимат, при котором имеет место изменение теплообмена человека с окружающей средой, проявляющееся в накоплении тепла в организме (> 2 Вт) и/или в увеличении доли потерь тепла испарением влаги (>30%). Профилактика перегрева организма работника в нагревающем микроклимате включает следующие мероприятия: нормирование верхней границы внешней термической нагрузки на допустимом уровне применительно к восьмичасовой рабочей смене; регламентация продолжительности воздействия нагревающей

среды для поддержания среднесменного теплового состояния на оптимальном или допустимом уровне; использование специальных средств коллективной и индивидуальной защиты, уменьшающих поступление тепла извне к поверхности тела человека и обеспечивающих допустимый тепловой режим.

Таким образом, проведённая работа способствует более глубокому изучению вопроса повышения комфорта и безопасности труда работников этой профессии.

Библиографический список

1. Закон Российской Федерации "О специальной оценке условий труда" от 01.01.2014 № 426.
2. Суханов, Е.В. Организация и методика разработки систем нормирования труда на предприятиях в современных условиях / Е.В. Суханов. - Москва: ИЛ, 2016. – 326 с.
3. Закон Российской Федерации "О санитарно-эпидемиологическом благополучии населения" от 30.03.1999 № 52.
4. СанПиН 2.2.4.548-96 Гигиенические требования к микроклимату производственных помещении. Санитарные правила и нормы.
5. Кукин, П.П., Лапин, В.Л. Безопасность жизнедеятельности. Безопасность технологических процессов и производств. Охрана труда / П.П. Кукин, В.Л. Лапин. – М.: Высшая школа, 2017 – 318 с.

ЭКОЛОГО-ГЕОГРАФИЧЕСКАЯ ХАРАКТЕРИСТИКА ФИТОПЛАНКТОНА ВОЛГОГРАДСКОГО ВОДОХРАНИЛИЩА В 2017 ГОДУ

Гинзерюк К.М., студент
Научный руководитель: Зеленевская Н.А., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

В экосистемах водоемов существует большое количество различных экологических группировок. Здесь особое место занимают микроскопические водоросли, образующие альгоценозы. Подобные сообщества носят общее название «фитопланктон». Преобразуя и накапливая солнечную энергию в виде энергии химических связей органических соединений в результате фотосинтеза, водоросли выделяют необходимый для дыхания водных организмов кислород. На видовой состав и динамику развития фитопланктона водоемов значительно влияет большой комплекс внешних факторов – световой режим, температура воды, содержание различных химических элементов и веществ, как органического, так и неорганического происхождения. Но в свою очередь большинство данных факторов зависят от климатических условий и географического положения водоема.

В данной работе приводится анализ видового состава водорослей Волгоградского водохранилища в 2017 году.

Цель работы – дать эколого-географическую характеристику водорослей фитопланктона Волгоградского водохранилища.

Задачи:

1. Выявить таксономическую структуру фитопланктона Волгоградского водохранилища.
2. Определить эколого-географическую принадлежность видов фитопланктона Волгоградского водохранилища.

Материалы по фитопланктону Волгоградского водохранилища за 2017 год для выполнения дипломной работы предоставлены лабораторией гидробиологии Тольяттинской СГМО ФБГУ «Приволжское УГМС». Пробы фитопланктона отбирались, фиксировались, подвергались фильтрации и затем обрабатывались в лаборатории гидробиологии. Характеристика водорослей водохранилища определялась автором по литературным данным

[1-5].

Пробы по фитопланктону для исследования отбирались весной, летом и осенью на русловой части водохранилища от г. Балаково до с. Ровное.

Всего за период исследования в фитопланктоне обнаружено 90 таксонов водорослей. Наибольшим числом таксонов характеризовались отделы Bacillariophyta - (38 видов). Два отдела Cyanophyta (Cyanoprocariota) и Chlorophyta насчитывают поровну по 8 видов. Остальные отделы представлены меньшим числом видов: Dinophyta – 4, а точнее *Glenodinium pulvisculus* (Ehrb.) Stein, *Glenodinium sp., Peridinium sp., Gymnodinium sp.* Отдел Cryptophyta – 3, это *Cryptomonas caudata* Geitl., *Chroomonas acuta* Schiller, *Cryptomonas marssonii* Skuja. Отдел Chrysophyta представлен только одним видом *Dinobryon divergens* Imhof (рис. 1).

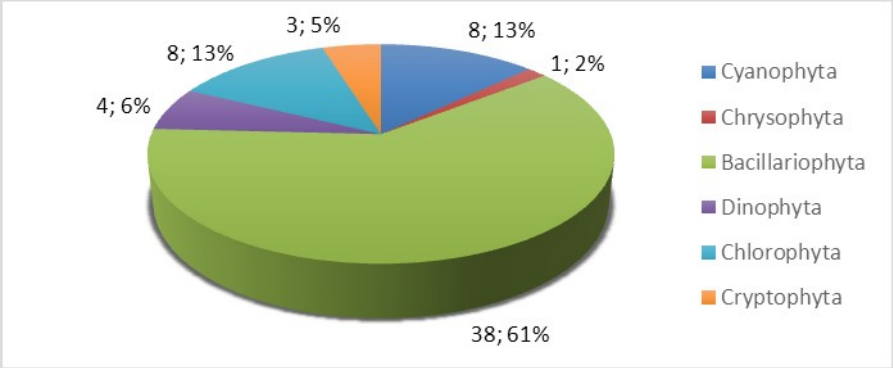

Рисунок 1 - Соотношение числа таксонов водорослей фитопланктона

Более подробная структура таксонов фитопланктона приведена в Таблице 1.

Таблица 1 - Таксономическая структура водорослей Волгоградского водохранилища

Отдел	Число				Число таксонов		
	Классов	Порядков	Семейств	Родов	Видовых	Внутривидовых	Всего, рангом ниже рода
Cyanophyta	1	2	2	5	8		8
Chrysophyta	1	1	1	1	1		1
Bacillariophyta	2	4	12	16	38	25	63
Dinophyta	1	1	3	3	4		4
Chlorophyta	2	3	5	7	8	3	11
Cryptophyta	1	1	1	2	3		3
Всего	8	12	24	34	62	28	90

Отдел Bacillariophyta представлен 2 классами - Centrophyceae и Pennatophyceae, 4 порядками. Класс Centrophyceae включал порядок Thalassiosirales с семейством Thalassiosiraceae, представленным родом *Skeletonema,* а также семейством Stephanodiscaceae с родом Scephanodiscus. Порядок Melosirales представлен семейством Aulacosiraceae и Melosiraceae. Семейство Aulacosiraceae представленно родом Aulacoseira, а Melosiraceae – родом Melosira. Класс Pennatophyceae более широко представлен и включал порядки Raphales и Araphales. Порядок Araphales содержит семейство Diatomaceae и Fragilariaceae. Порядок Raphales содержал большее число видов и включает семейства Nitzschiaceae, Naviculaceae, Gomphonemataceae, Achnanthaceae, Cymbellaceae, Surirellaceae, Rhoicospheniaceae. Наиболее богато видами семейство Nizschiaceae (15 видов). Также широко представлено семейство Naviculaceae, включающее 2 рода Gyrosigma и Navicula.

Отдел Chlorophyta представлен 2 классами – Chlorophyceae. Chlamydophyceae. Из них большую часть составляли представители из порядка Chlorococcales, включающего в себя 3 семейства – Chlorellaceae, Coelastraceae, Scenedesmaceae.

Отдел Cyanophyta представлен 8 видами из 1 класса Hormogoniophyceae и 2 порядков:

Oscillatoriales, Nostocales. Порядок Oscillatiriales включает семейство Oscillatoriaceae, которое представлено родами Lingbya, Phormidium, Oscillatoria. Порядок Nostocales представлен семейством Anabaenaceae и родами Anabaena и Aphanizomenon.

Отдел Dinophyta, который представлен 4 видами из класса Dinophyceae, порядка Peridiniales. Порядок включает в себя 3 семейства – Gymnodiniaceae, Peridiniaceae, Glenodiniopsidaceae.

Предпоследнее место по числу видов занимает отдел Cryptophyta, представленный единственным классом Cryptomonadophyceae, семейством Cryptomonadaceae, которое включает представителей родов Cryptomonas и Chroomonas.

Последнее место по числу видов занимает отдел Chrysophyta. Отдел представлен 1 видом *Dinobryon divergens Imhof* из класса Chrysophyceae порядка Ochromonadales семейства Dinobryonaceae.

Таким образом, за весь период исследования в фитопланктоне Волгоградского водохранилища обнаружено 90 таксонов водорослей, рангом ниже рода, из 6 отделов, 8 классов, 12 порядков, 24 семейств, 34 родов. Наибольшим числом таксонов фитопланктона Волгоградского водохранилища характеризовался отдел Bacillariophyta (38).

Для каждого обнаруженного таксона в фитопланктоне водохранилища по литературным данным была определена эколого-географическая принадлежность. Полученные данные сведены в таблицу 1, которая представлена в Приложении В.

Из 86 таксонов, для которых определено местообитание, преобладали планктонные организмы (35%). Среди них большинство - представители из отдела Bacillariaphyta. Такие, например, как *Stephanodiscus hantzschii* Grun., *Asterionella formosa* Hass, *Aulacoseira granulata* (Ehr.) Sim., *Scenedesmus opoliensis* P. Richt. На долю бентосных видов приходилось 32%, среди которых больше всего представителей рода Navicula, таких как *Navicula placentula f.rostrata* (Ehr.) Grun., *Navicula radiosa* Kütz., *Navicula tripunctata* (O.Müll) Bory, и другие. Так же бентосными видами представлено семейство *Gomphonemataceae (Gomphonema olivaceum* (Horn.) Breb, *Gomphonema olivaceum* var. calcareum Cl.) и семейство Cymbellaphyceae. Среди представителей последнего *Amphora ovalis* (Kütz.), *Cymbella affinis* Kütz., *Cymbella cymbiformis* (Ag., Kutz) V.H.. и другие. Также большая часть, а именно 21%, представлена планктонно-бентосными видами, большинство из которых представлены родом Nitzschia. Это *Nitzschia acicularis* (Kütz.) W. Sm., *Nitzschia apiculata* (Greg) Grun., *Nitzschia hungarica* Grun., *Nitzschia sublinearis* Hust., и другие. Также к планктонно-бентосным относятся предсавители из семейств *Rhoicospheniaceae* и *Melosiraceae,* которые представленны единичными видами *Rhoicosphaenia curvata* (Kütz) Grun.ex Rab. и *Melosira varians* Ag. соответственно. Литоральные виды составили 7% к ним относятся: *Surirella linearis var. constricta* (Her.) Grun., *Nitzschia recta* Hantzsch, *Nitzschia palea* (Kütz.) W. Sm. v*ar. palea, Navicula viridula (*Kütz) Ehr, *Diatoma vulgare* Bory*, Phormidium foveolarum* (Mont.) Gom. Обитателей обрастаний было всего 2%, и представлены они одним видом из диатомовых *Synedra tabulata* (Kütz.) Ag. Эпибионтные виды составили 3%, представлены 2 видами: *Gyrosigma acuminatum* (Kütz.), Rabenh. и *Cocconeis placentula var. euglypta* (Ehr.) Grun (рис. 2).

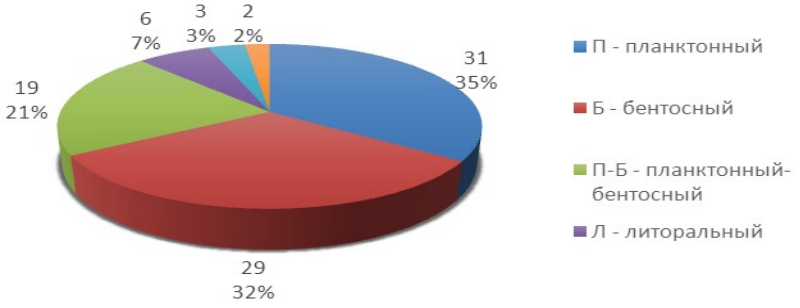

Рисунок 2 – Соотношение числа видов фитопланктона по местообитанию

Большинство видов с установленным географическим распространением, 85 из 90 обнаруженных, относилось к космополитам (90%). Незначительная часть видов относилась к обитателям бореальной зоны (4,5%), представлена 4 видами а, а именно *Surirella linearis var.*

constricta (Her.) Grun, *Gyrosigma acuminatum* (Kütz.) Rabenh, *Navicula menisculus* Schum., *Stephanodiscus dubius* (Fricke) Hust. Имеются голарктические представители 3%, такие как *Scenedesmus opoliensis var. mononensis* Chod. и *Aphanizomenon elenkinii* Kissel., а также 1 арктико-альпийскийй вид - *Aulacoseira distans var. alpigena* Grun и 1 северный - *Aulacoseira islandica* O.Mull. На их долю приходится 2 % в общем количестве (рис. 3).

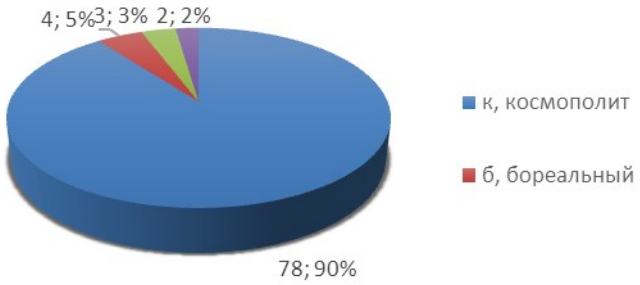

Рисунок 3 - Соотношение числа видов фитопланктона по географическому распространению

Отношение к солености воды, установленное для 81 таксонов, 67% от общего числа индифферентны к этому показателю. Например, все представители семейства Aulacosiraceae и подавляющее большинство из семейства Pennatophyceae (*Asterionella formosa* Hass., *Synedra acus* Kütz., *Diatoma vulgare* Bory, и другие*)*. Всего 14% составляли галофилы, большинство из которых принадлежат порядкам Oscillatoriales (3 вида: *Lyngbya limnetica* Lemm, *Oscillatoria limosa* Gom. и *Aphanizomenon flos-aquae* (Lyngb.) Breb.) и Raphales (6 видов), такие как *Rhoicosphaenia curvata* (Kütz) Grun. ex Rab., *Nitzschia closterium* (Ehr.) W.Sm., *Gyrosigma acuminatum var. gallica* Grun., *Navicula menisculus* Schum., и другие. Мезогалобы занимают третье место по количеству (11%), отмечены только среди представителей отдела Bacillariophyta в количестве 9 видов, например, такие как *Skeletonema potamos* (Weber) Hasle, *Synedra tabulata* (Kütz.) Ag., *Navicula hungarica* Grun. К олигагалобам принадлежат 8 % видов, в основном из таких семейств, как Nitzschiaceae (*Nitzschia recta* Hantzsch, *Nitzschia aquaea* Wisl. et Poretzky) и Scenedesmaceae (*Scenedesmus magnus* Meyen, *Scenedesmus opoliensis* P. Richt*)*, по 2 вида в каждом. А также видом *Glenodinium pulvisculus* (Ehrb.) Stein из семейства Glenodiniopsidaceae, видом *Cocconeis placentula var. euglypta* (Ehr.) Grun. из семейства Achnanthaceae, *Navicula hungarica var. capitata* Cl. из семейства Naviculaceae (рис. 4).

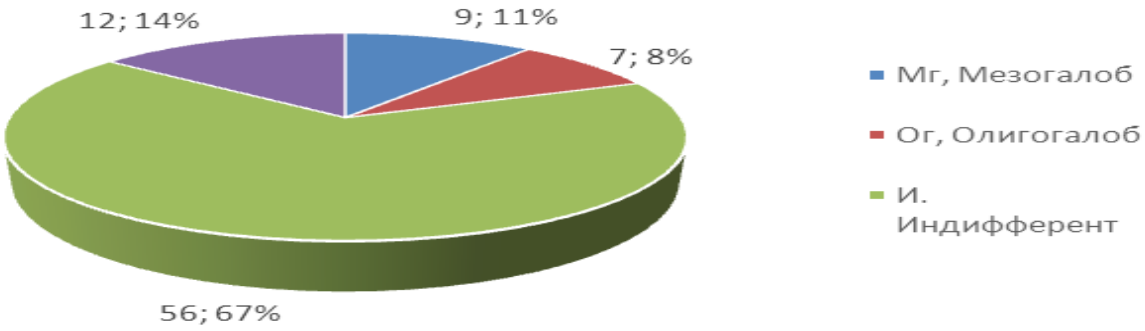

Рисунок 4 – Соотношение числа видов по отношению к солености

Отношение к pH среды, определено для 62 видов, 32% из них – индифференты (*Lingbya limnetica* Lemm., *Dinobryon divergens* Imhof, *Navicula viridula (*Kütz) Ehr), 40 видов из отдела Bacillariaphyta и 1 (*Oscillatoria limosa* Gom.) из Cyanoprocariota - алкалифилы, составившие большую часть, а именно 63%, такие как, например, *Navicula hungarica Grun*, *Synedra acus* Kütz, *Stephanodiscus hantzschii* Grun. Всего 5% составили алкалибионты, все они представители отдела Bacillariophyta, это *Synedra acus* Kütz., *Stephanodiscus rotula* (Kütz.) Hendey, *Aulacoseira italica ssp.subarctica* (O. Müll.) Simons (рис. 5).

Из общего числа таксонов обнаружено всего 55 вида-индикатора сапробности, большинство из которых относились к двум отделам водорослей Bacillariophyta и Cyanoprocariota, подробнее эти данные представлены в таблице 2.

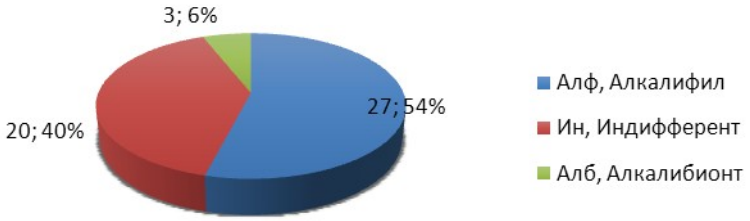

Рисунок 5 - Соотношение числа видов по отношению к pH среды

Таблица 2 - Число видов по зонам сапробности в разных отделах

Отдел	**o**	**ob**	**bo**	**b**	**ba**	**ab**	**a**
Cyanoprocariota	-	-	-	3	1	1	2
Bacillariophyta	1	6	1	17	3	-	11
Chlorophyta	-	-	-	6	-	-	-
Chrysophyta	-	-	-	1	-	-	-
Dinophyta	-	-	-	-	-	-	-
Cryptophyta	-	1	-	1	-	-	-
Всего	1	7	1	28	4	1	13

Преобладающее число видов, для которых известен коэффициент сапробности, относились к β-мезосапробным (51%) организмам. На долю индикаторов высокой степени органического загрязнения (βα-, αβ-, α-сапробных организмов) приходилось 32% среди них βα-сапробы *Aphanizomenon flos-aquae* (Lyngb.) Breb. из семейства Anabaenaphyceae, *Aulacoseira granulata var. Angustissima* (O.Mull.) Hust. *из* семейства Aulacosiraceae, *Navicula menisculus* Schum. *из* семейства Naviculaphyceae, *Nitzschia recta* Hantzsch *из* семейства Nitzschiaceae. αβ-сапробный организм представлен единственным из определенных видов *Oscillatoria limosa* Gom. α-сапробные виды: *Nitzschia sigma* (Kutz) W. Sm., *Navicula hungarica* Grun, *Synedra tabulata* (Kütz.) Ag., и другие. Низкосапробные виды (o-, oβ-, βo-сапробы) составляли 17%. Среди них o-сапробный вид только один *Navicula reinhardtii* (Grun) Cl., oβ-сапробы: *Amphora ovalis* (Kütz.), *Cryptomonas marssonii* Skuja, *Navicula radiosa* Kütz., *Asterionella formosa* Hass., и другие. К βo-сапробным организмам относится только один вид из определенных *Navicula tripunctata* (O.Müll) Bory (рис.6).

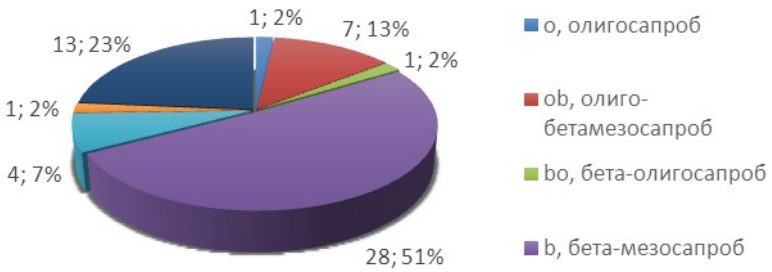

Рисунок 6 - Соотношение числа видов с разной степенью сапробности

Из показателей высокой степени органического загрязнения наиболее часто встречались рода Nitzhiaceae *(*α). Виды, обитающие в относительно чистых водах, встречались нечасто, среди них – *Cryptomonas marssonii* Skuja (oβ), *Amphora ovalis (*Kütz.) (oβ), *Cymbella affinis* (Kütz.) (oβ), *Stephanodiscus rotula* (Kütz.) Hendey (oβ) и др.

Таким образом, по местообитанию отмечено преобладание планктонных форм (57%),

по географическому распространению – космополитов (90%), по отношению к солености – индифферентов (72%), по отношению к pH преобладали индифференты (66%) и алкалифилы (63%), среди видов-индикаторов сапробности большая часть – β-мезосапробы (51%).

На основании данных, полученных при анализе материала по фитопланктону Волгоградского водохранилища, можно сделать следующие выводы.

1. По данным 2017 года в фитопланктоне русловой части Волгоградского водохранилища обнаружено 90 таксонов водорослей, рангом ниже рода, из 6 отделов, 8 классов, 12 порядков, 24 семейств, 34 родов. Наибольшим числом таксонов фитопланктона Волгоградского водохранилища характеризовался отдел Bacillariophyta (38).

2. В составе фитопланктона Волгоградского водохранилища за период исследования преобладали космополиты - по геграфическому распространению, планктонные виды – по местообитанию, индифференты и алкалифилы – по отношению к pH, индифференты – по отношению к солености воды.

3. Из 90 таксонов водорослей Волгоградского водохранилища 55 – индикаторы органического загрязнения вод, среди которых преобладали бета-мезосапробионты, составляющие 51% видов-индикаторов, при этом значительный процент (32%) составляли также высокосапробные виды.

Библиографический список

1. Баринова, С.С, Медведева, Л.А., Анисимова, О.В. Биоразнообразие водорослей-индикаторов окружающей среды. - Тель-Авив, 2006. - 356 с.

2. Каталог растений и животных водоемов бассейна Волги / отв. редактор д-р биол. наук В.Н. Яковлев; ИБВВ им. И.Д. Папанина. - Ярославль: Изд-во ЯГТУ, 2000. С. 5-112.

3. Попченко, И.И. Видовой состав и динамика фитопланктона Саратовского водохранилища / под ред. В.Н. Паутовой и Г.С. Розенберга.- Тольятти, 2001. – 148 с.

4. Унифицированные методы исследования качества вод. ч. III. Методы биологического анализа. Приложение 1: Индексы сапробности. - М., изд-во СЭВ, 1977. - 92 с.

5. Унифицированные методы исследования качества вод, ч. III. Методы биологического анализа. Приложение 2: Атлас сапробных организмов. - М., изд-во СЭВ, 1977. - 228 с.

АНАЛИЗ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ПРОИЗВОДСТВЕННОГО ПОМЕЩЕНИЯ МАСТЕРСКОЙ ПО ИЗГОТОВЛЕНИЮ КОСТЮМОВ

Кистанова А.А., студент
Научный руководитель: Петрякова О.Д., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

В связи с развитием развлекательной индустрии и увеличением её влияния на жизнь общества, появляются новые направления производственных предприятий. Благодаря все большей популяризации художественных фантастических фильмов и компьютерных игр, работа десятков тысяч работников, в число которых входят профессиональные гримеры и изготовители декораций, становится очень востребованной.

Актуальность выбранной темы заключается в том, что профессии связанные с индустрией развлечений набирают популярность. Появляются новые методики изготовления продукта, все больше людей вовлечено в процесс разработки контента. важно обеспечить безопасность на рабочем месте для каждого вида этих творческих специальностей.

Цель работы: провести анализ экологической безопасности внутренней среды помещения в мастерской по производству костюмов «Kirin Props».

Задачи исследования:

1. Изучить уровень воздействия производственных факторов на здоровье сотрудников предприятия.

1. Изучить возможные последствия опасных факторов на здоровье человека при длительном воздействии.

3. Выявить возможные варианты снижения негативных последствий и технологии предотвращения получения ущерба здоровью на рабочем месте.

Мастерская «Kirin-Props» занимается изготовлением костюмов и декораций для реализации на отечественных и зарубежных развлекательных мероприятиях.

Предприятие существует с 2014 года и до настоящего времени. В конце 2014 года, после победы на местном фестивале анимации, началось изготовление костюмов с целью реализации за границу и на территории России. На предприятии в текущее время работают 8 сотрудников. Рабочее помещение включает в себя три цеха:

- Покрасочный цех — в нем осуществляются работы по грунтовке, покраске и лакировке готовой продукции, оснащен двумя стеллажами для хранения красок и растворителей, покрасочной камерой, в которой ведутся работы при помощи воздушного компрессора и аэрографа. Покрасочный цех присоединен к вытяжке мощностью всасывания 6 куб. м /сек. Таким образом, процесс покраски становится максимально безопасным при условии ношения рабочего защитного костюма, одноразовых виниловых перчаток и использовании респиратора.

- Гравировочный цех — в котором проводятся гравировочные работы и крупная косметическая шлифовка изделия.

- Швейный цех — в нем находятся стеллажи для хранения ткани и материалов, две рабочие и одна резервная швейные машины марки Janome модели DC 4030, находящихся в индивидуальных защитных камерах звукоизоляции. Кроме того, в этом цеху находится второстепенное технологическое оборудование (резак, клеевые пистолеты, строительный фен и прочее), а так же силиконовые формы для отливки твердых деталей и изделий. В данном помещении проводятся швейные работы. Реже проходит мелкая косметическая шлифовка изделий, дополнительная термическая обработка или склейка. В исключительных случаях в швейном цехе происходит отливка изделий.

В результате проведенной исследовательской работы, были проведены замеры параметров вредных и опасных факторов на швейном предприятии «Kirin Props».

Проводились замеры следующих показателей:

- Измерение температуры при помощи термометра;
- Измерение влажности воздуха при помощи психрометра;
- Замеры освещенности при помощи люксметра;
- Измерение постоянного и колеблющегося уровня звукового давления при помощи шумомера;
- Измерение запыленности при помощи аспиратора и индикаторных трубок;
- Измерение вибрации при помощи интегрирующего шумомера-виброметра.

Соответствие полученных результатов нормативным значениям для различных помещений мастерской по производству костюмов «Kirin Props» приведено в таблице 1.

Таблица 1 - Соответствие нормативам результатов замеров

Фактор вредного воздействия	**Результат замера**	**Требования норматива**	**Соответствие**
Температура	13-15°С 32°С	20-22°С	Не соответствует не соответствует
Влажность	60%	60%	Соответствует
Давление	765мм рт.ст	765 мм рт.ст	Соответствует
Освещенность	80 лк 80 лк 140 лк	90 лк 90 лк 120 лк	Соответствует соответствует не соответствует

Фактор вредного воздействия	Результат замера	Требования норматива	Соответствие
Шумовая нагрузка	46 37 96 дБА	50 дБА	Соответствует соответствует не соответствует
Запыленность	Не превышает 1 ПДК	1 ПДК	Соотвествует
Вибрация	Непостоянная – 0,5 Гц	<0,7 Гц	Соответствует

Как видно из таблицы, не все параметры соответствуют нормативным значениям, например шум, температурный режим помещения, освещенность. Таким образом, условия труда можно отнести к вредным. Необходимо ликвидировать данные нарушения и обеспечить безопасность труда на всех рабочих местах.

В работе были предложены варианты снижения негативных последствий и предотвращения получения ущерба здоровью на рабочем месте. Данные мероприятия вполне осуществимы, не относятся к высокозатратным, помогут пройти спецоценку условий труда с получением 2 класса 9допустимые условия труда) для всех рабочих мест.

ОЦЕНКА ЭКОЛОГИЧЕСКИХ ПРОБЛЕМ ГРАДОСТРОИТЕЛЬСТВА НА ТЕРРИТОРИИ Г.О. ТОЛЬЯТТИ

Лукьянов И.А., студент
Научный руководитель: Петрякова О.Д., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Актуальность данной работы заключается в анализе экологических проблем городской среды градостроительства на территории г.о. Тольятти, так как это является ключевым вопросом фундаментального и прикладного значения. В современном городе в результате бурного развития градостроительства, промышленности и транспорта, возникает неблагоприятная экологическая ситуация. Те же природные экосистемы, что остались не могут в полной мере компенсировать отрицательное воздействие человека, а фактические административные меры направленны лишь на снижение роста воздействия отходов на городскую среду.

Современный город является центром концентрации населения, промышленности, строительства ими вызваны ухудшения ландшафта и загрязнения окружающей среды. Таким образом, в результате развития промышленности и быстрого роста градостроительства усиливаются неблагоприятные экологические условия, развиваются экологические проблемы.

Поддержание хорошего качества окружающей среды является одной из наиболее актуальных экономических, научных, технологических и социальных проблем, которая прямо или косвенно затрагивает все интересы человека.

В последние годы окружающая среда крупных городов с промышленным комплексом практически снизила качество жизни населения, ограничив его экономический и социальный потенциал развития. В этих сложных условиях является необходимым использование современных процедур для обеспечения экологического устойчивого и сбалансированного развития города, следовательно, это и послужило выбором темы квалификационной работы. Таким образом, тема исследования актуальна, как в теоретическом, так и практическом плане.

Целью работы является анализ основных экологических проблем городской среды градостроительства на территории городского округа Тольятти, сложившихся в результате интенсивного антропогенного воздействия.

Для достижения этой цели необходимо решить следующие задачи:

- Ознакомиться с особенностями региона градостроительства Тольятти;
- Проанализировать состояния экологических проблем градостроительства в городском округе Тольятти;
- Предложить комплекс мер по улучшению текущих экологических условий.

Объектом исследования является территория городского округа Тольятти.

Предмет исследования: экологические проблемы городской среды градостроительства на территории г. о. Тольятти.

Методологической основой исследования стал годовой отчет Департамента экологии и природопользования, статистические материалы Росстата, нормативные справочные материалы.

Теоретическая и практическая значимость заключается в том, что материалы данной работы могут использоваться не только для комплексного изучения экологических проблем, возникающих при градостроительстве в г.о. Тольятти, но и для улучшения экологии городской среды. Анализ фактического материала позволил обеспечить объективность полученных выводов и результатов.

Экологические проблемы - это комплексная проблема современности, требующая неотложных мер по восстановлению экологического баланса. С точки зрения экологии г.о. Тольятти считается одним из самых неблагополучных городов региона.

Экологические последствия градостроительной деятельности человека на окружающую среду в городе наблюдается повсеместно. Они весьма разнообразны, но наиболее ярко проявляются на урбанизированных территориях.

Городской округ Тольятти - крупный промышленный центр Самарской области, центр машиностроения и химической отрасли. Основными источниками загрязнения на территории города являются градообразующего предприятия автомобильной промышленности, производство нефтепродуктов, химических удобрений и строительных материалов, так же ТЭЦ и котельные, автомобильные, железнодорожные и речные вокзалы. Все эти постройки расположены по всему городу и у многих нет санитарно-защитных зон.

Следует отметить, что в городском округе Тольятти наблюдается тенденция к снижению или стабилизации ряда показателей, характеризующих состояние окружающей среды. В то же время уровень загрязнения окружающей среды в городе в целом остается высоким. В городе Тольятти, а также, в Самарской области в целом активизируется деятельность, связанная с экологической информированием, просвещением и совершенствованием экологической культуры населения.

Уровень загрязнения атмосферного воздуха определяется выбросами около 30 промышленных предприятий. Общие выбросы загрязняющих веществ от основных промышленных предприятий ежегодно достигают 40-50 тыс. тонн. Значение основных показателей загрязнения воздуха к уровню ПДК в Тольятти в 2018 году показано на рисунке 1.

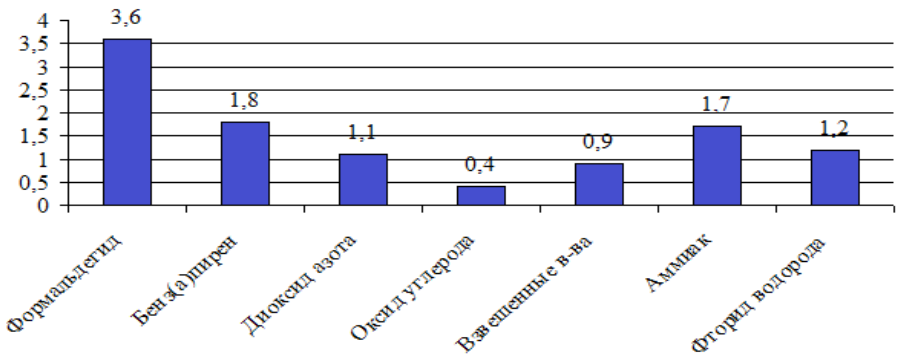

Рисунок 1 - Уровни загрязнения воздуха в Тольятти 2018

В процессе выполнения работы ознакомились с особенностями региона

градостроительства Тольятти, проанализировали состояния экологических проблем градостроительства в городском округе Тольятти, предложили комплекс мер по улучшению текущих экологических условий.

Проведенный анализ позволяет сделать следующие выводы:

1. Город - является основной формой сосредоточения людей, с постоянным увеличением в нем населения. Городская система характеризуется огромной потребностью в энергии и ресурсах. Города потребляют и перерабатывают различные ресурсы в виде продовольствия, топлива и так далее. Чем выше уровень жизни населения, тем больше они потребляют и производят отходов. С развитием урбанизации, по мере того как все больше людей концентрируется в небольших районах, возрастает антропогенное экологическое давление, экологические проблемы городов становятся все более разнообразными и трудноразрешимыми.

2. Проанализировав территорию городского округа Тольятти, можно сделать вывод о сильном загрязнении практически всех районов города. Промышленные выбросы происходят в основном в Автозаводском и Центральном районе, наиболее благоприятная экологическая ситуация наблюдается в Комсомольском районе.

3. Мегаполис типа городского округа Тольятти характеризуется целым рядом экологических проблем, но самая серьезная из них являются проблемы загрязнение атмосферного воздуха, загрязнения водных объектов, ликвидации и утилизации отходов производства и потребления.

4. Для решения экологических проблем градостроительства предложены мероприятия для улучшения экологического состояния города. При строительстве, реконструкции и эксплуатации объектов необходимо соблюдение соответствия санитарным нормам на всех этапах, включая разработку градостроительной документации.

СОВЕРШЕНСТВОВАНИЯ КАЧЕСТВА ВОДЫ ИЗ ПОДЗЕМНЫХ ВОДОЗАБОРОВ СТАВРОПОЛЬСКОГО РАЙОНА Г.О. ТОЛЬЯТТИ

Собин Д.С., студент
Научный руководитель: Петрякова О.Д., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Вода подземных водозаборов очень часто не соответствует предъявляемым критериям качества и нуждается в дальнейшей водоподготовке для использования в питьевых целях. Однако, у населения сформировалось положительное отношение к качеству воды из подземных водозаборов, по сравнению с водой из поверхностных источников, подвергающихся интенсивному антропогенному загрязнению. Из шести крупных подземных водозаборов г. о. Тольятти только два имеют удовлетворительное качество воды, остальные могут использоваться только для технических целей. Что касается небольших водозаборов, скважин, обслуживающих индивидуальные домостроения, то ситуация выглядит еще более удручающе.

Целью работы был анализ качества воды скважин Ставропольского района и разработка мероприятий по улучшению качества воды на объектах исследования.

Объектами исследования являлись скважины Ставропольского района, обсуживающие коттеджи и частные дома сел Подстепки, Ягодное, Хрящевка.

По залеганию подземных вод используемые скважины относятся к грунтовым и так называемой верховодке. Для бурения артезианских скважин требуется специальное разрешение от администрации Самарской области для использования недр, принадлежащих государству (глубина более 100 м), что представляет определенные сложности для населения. Основными источниками подземных вод Ставропольского района являются: Жигулёвское водохранилище и осадки.

Данные скважины отличаются резкой сменой качества воды в паводковые периоды весной и осенью. В процессе работы при выполнении анализов качества воды было выявлено постоянно меняющееся содержание в воде железа, марганца, сероводорода и солей калия и магния, нормы ПДК по многим показателям оказались существенно превышены. Для очистки подземных вод рекомендовано использование водоочистного оборудования: обезжелезователей, умягчителей, многоцелевых установок, ультрафиолетовых ламп, дозаторов хлора, патронных фильтров и т.д. В каждом индивидуальном случае схема очистки воды и используемое оборудование, а также объем используемых реагентов и фильтрующих агентов необходимо подбирать индивидуально. Необходимо постоянное грамотное обслуживание подобных водозаборов.

В работе представлены представлены усредненные результаты по трем наиболее проблемным скважинам Ставропольского района на основе данных анализов за двухлетний период.

Скважина №1 расположена в селе Подстепки. Глубина скважины - 70 м. При отборе проб содержание в воде железа видно невооруженным взглядом по ржавой окраске пробы. Результаты анализа воды, выполнененные в лаборатории «Тевис», показаны в таблице 1. При этом показаны только те параметры, по которым наблюдалось превышение норм качества.

Таблица 1 - Анализ воды в скважине №1 до установки водоочистного оборудования

Наименование	СанПиН 2.1.4.1074-01 и ГН 2.1.5.689-98 с доп. №1, 2, 3	Максимальный результат анализа по содержанию элементов
Жесткость общая, моль/л	7,0	10
Сероводород	0.003	0.009
Железо (Fe, суммарно), мг/л	0,30	6,0
Марганец (Mn, суммарно), мг/л	0,1	0,45

Как видно из таблицы 1, по данной скважине содержание железа в 20 раз превышает допустимые нормы СанПиН, марганца – в 4,5 раза, жесткость – в 1.4 раза, сероводород – в 3 раза.

После проведения четырех заборов проб было выяснено, что самые худшие результаты анализов оказались не в паводковые времена года (зимой и летом), как видно из рисунка 1 на примере содержания железа.

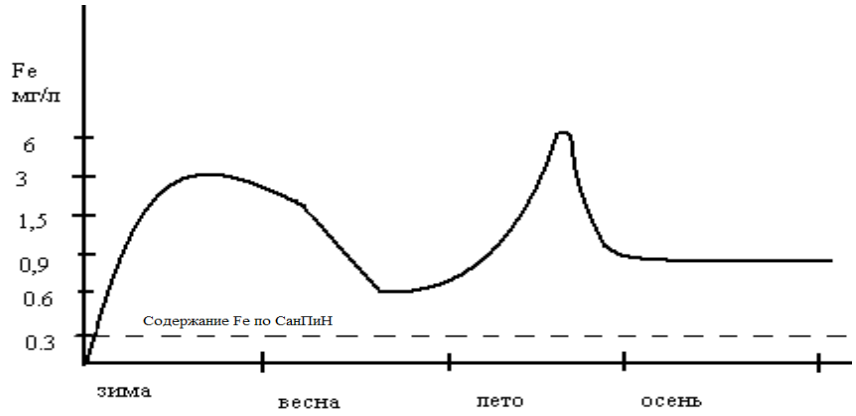

Рисунок 1 - Содержание в скважине №1 железа до установки водоочистного оборудования

После установки водоочистного оборудования была взята повторная проба воды, которая показала следующие параметры, представленные в таблице 2.

Таблица 2 - Анализ воды в скважине №1 после установки водоочистного оборудования

Наименование	СанПиН 2.1.4.1074-01 и ГН 2.1.5.689-98 с доп. №1, 2, 3	Максимальный результат анализа по содержанию элементов

Жесткость общая, моль/л	7,0	3,0
Сероводород	0.003	Отсутствует
Железо (Fe, суммарно), мг/л	0,30	Отсутствует
Марганец (Mn, суммарно), мг/л	0,1	Отсутствует

Скважина №2 расположена в селе Ягодное. Её глубина составляет 63 м. Анализ проб представлен в таблице 3.

Таблица 3 - Анализ воды в скважине №2 до установки водоочистного оборудования

Наименование	СанПиН 2.1.4.1074-01 и ГН 2.1.5.689-98 с доп. №1, 2, 3	Максимальный результат анализа по содержанию элементов
Жесткость общая, моль/л	7,0	8,0
Железо (Fe, суммарно), мг/л	0,3	0,9
Марганец (Mn, суммарно), мг/л	0,1	0,3

Как видим, также наблюдается некоторое превышение нормативов, например по железу и марганцу в три раза.

Таблица 4 - Анализ воды в скважине №2 после установки водоочистного оборудования

Наименование	СанПиН 2.1.4.1074-01 и ГН 2.1.5.689-98 с доп. №1, 2, 3	Максимальный результат анализа по содержанию элементов
Жесткость общая, моль/л	7,0	3,0
Железобактерии	Отсутствует	Отсутствует
Железо (Fe, суммарно), мг/л	0,30	Отсутствует
Марганец (Mn, суммарно), мг/л	0,1	Отсутствует

Скважина №3 расположена в селе Хрящовка. Пробурена на глубину 45 м. Анализ проб представлен в таблице 5.

Таблица 5 - Анализ воды в скважине №3 до установки водоочистного оборудования

Наименование	СанПиН 2.1.4.1074-01 и ГН 2.1.5.689-98 с доп. №1, 2, 3	Максимальный результат анализа по содержанию элементов
Жесткость общая, моль/л	7,0	12
Железобактерии	-	-
Железо (Fe, суммарно), мг/л	0,3	1,2

В данной скважине также наблюдается превышение по железу (в 4 раза), несколько превышена общая жесткость. В таблице 6 представлен результат анализа воды скважины №3 после установки водоочистного оборудования.

Таблица 6 - Анализ воды скважины №3 после установки водоочистного оборудования

Наименование	СанПиН 2.1.4.1074-01 и ГН 2.1.5.689-98 с доп. №1, 2, 3	Максимальный результат анализа по содержанию элементов
Жесткость общая, моль/л	7,0	3,0
Железобактерии	-	Отсутствует
Железо (Fe, суммарно), мг/л	0,30	Отсутствует
Марганец (Mn, суммарно), мг/л	0,1	Отсутствует

Таким образом, подбирая индивидуально технологическую схему и оборудование для

очистки, в каждом конкретном случае удалось нормализовать ситуацию и добиться получения воды питьевого качества.

В работе предлагается использовать следующие виды водоочистного оборудования: водоочистное оборудование фирм «EcoWater» и «Flack», обезжелезователи с засыпками «BIRM» и «MGS», умягчители с ионообменной смолой, патронные фильтры фирмы «Pin-teck», которые более эффективно по сравнению с другими видами оборудования справились с поставленными задачами. Для умягчения воды в качестве фильтрующего материала применялась сильнокислотная катионообменная смола гелевого типа в Na-форме на основе сульфонированного полистирола. Для обеззараживания воды - кварцевая лампа с ультрафиолетовым спектром облучения в корпусе из нержавеющей стали.

Таким образом, в работе было проанализировано состояние верховодковых и грунтовых вод в скважинах Ставропольского района, выявлены проблемы с качеством воды и найдены решения по их устранению.

В результате проделанной работы можно сделать следующие выводы:

1) результаты анализов на скважинах Ставропольского района выявили превышение железа на скважине №1 в 20 раз, на скважине №2 в 3 раза, на скважине №3 в 4 раза;

2) результаты анализов по содержанию в воде марганца выявили превышение на скважине №1 в 4,5 раза, на скважине №2 в 3 раза;

3) результаты анализов на скважинах Ставропольского района выявили превышение солей жесткости на скважине №1 в 1,4 раза, на скважине №2 в 1,1 раза, на скважине №3 в 1,7 раза;

4) результаты анализов на скважинах Ставропольского района выявили превышение сероводорода на скважине №1 в 3 раза;

5) выявлен сезонный характер загрязнения высокой концентрации по таким показателям как Fe, Mn, H_2S, солям жесткости в зимний и летний период, что объясняется снижением загрязнения в паводковый период и сезон дождей, за счет разбавления;

6) предложено эффективное водоочистное оборудование, при применении которого удалось достичь нормативных показателей качества воды.

Библиографический список

1. СанПиН 2.1.4.1074-01 «Питьевая вода. Гигиенические требования к качеству воды централизованных систем питьевого водоснабжения. Контроль качества. Гигиенические требования к обеспечению безопасности систем горячего водоснабжения» (с изменениями на 2 апреля 2018 года).

2. СанПиН 2.1.4.1175-02 «Гигиенические требования к качеству воды нецентрализованного водоснабжения. Санитарная охрана источников» от 25 ноября 2002 года N 40 (с изменениями на 2019).

3. Методическое пособие по водоподготовке. ГК «Импульс». 2011. 71 с.

ОЦЕНКА ВЛИЯНИЯ ВЫБРОСОВ АВТОТРАНСПОРТА НА ОКРУЖАЮЩУЮ СРЕДУ И ЧЕЛОВЕКА

Сумбаева А.А, студент
Научный руководитель: Петрякова О.Д., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

На данный момент выхлопные газы это основная причина загрязнения воздуха в городах, так же они оказывают постоянное влияние на здоровье человека. Выхлопные газы от работающих автомобилей составляют порядка 90% от объема общего загрязнения. Статистика гласит, что в среднем один легковой автомобиль в атмосферу за год выбрасывает около килограмма разных токсических и канцерогенных веществ. Выхлопные газы

оказывают большое негативное влияние на человеческий организм в больших городах, в особенности при нахождении человека в многочасовой пробке в районах крупных дорожных развязок и магистралей. Когда химические и физические характеристики выбросов в воздух превышают допустимые концентрации, такие выхлопные газы оказывают негативное воздействие на самочувствие человек. При постоянном воздействии на организм выхлопных газов может развиваться бронхиты, иммунодефицит, нервная система, страдают сосуды головного мозга и другие органы. В тело растения попадает мельчайшие частицы вредных соединений, и отравляют его. Поэтому газоны и деревья, расположенные у парковок или больший дорог выглядят вяло, быстро желтеют или вовсе погибают. Таким образом, тема работы является актуальной.

Целью является оценка влияния выбросов автотранспорта на окружающую среду и человека. В связи с поставленной целью в работе решаются следующие задачи:

1. Изучить влияние загрязняющих веществ выбросов автотранспорта на здоровье человека и окружающую среду в целом.

2. Изучить методики для оценки интенсивности автотранспорта, для оценки выбросов угарного газа и программу «Эколог+» для оценки объема выбросов на участке автомагистрали.

3. Оценить концентрацию угарного газа по методике Бегма – Шаповалова.

4. Выполнить расчет выбросов автотранспорта на заданном участке автомагистрали с использованием программных методов.

5. Оценить влияние выбросов автотранспорта на здоровье человека и биоразнообразие.

Объектом исследования являлись ул. Комзина и Лесопарковое шоссе, проходящие по рекреационной зоне и соединяющие два района города: Автозаводский и Центральный.

Предметом исследования являются выбросы автотранспорта и их влияние на здоровье человека и биоразнообразие.

Для выполнения работы использовались экологическое законодательство и современная нормативно-правовая база, специальные экологические программы расчетов выбросов, методика Бегма-Шаповалова для расчета концентрации угарного газа, методика подсчета интенсивности автотранспортных средств.

Изучена правовая база и теоретические аспекты по рассмотренной экологической проблеме загрязнения окружающей среды выбросами автотранспорта. В работе дана классификация видов автотранспорта, видов двигателей, так же содержится информация о каталитических решетках для нейтрализации токсичных выбросов автотранспорта. Изучены вредные вещества, которые содержатся в выхлопных газах и их влияние на здоровье человека, биоту и биоразнообразие.

В процессе выполнения работы были изучены методики для расчетов (методика Бегма-Шаповалова для расчета концентрации угарного газа, методика подсчета интенсивности автотранспортных средств).

Данные, необходимые для подсчета количества выбросов с помощью программы «Магистраль — Город» приведены в таблице 1.

Таблица 1 - Данные, необходимые для подсчета количества выбросов с помощью программы «Магистраль - Город»

Данные об объекте	Данные об интенсивности движения	Данные об условиях движения
- Название города; - Название магистрали; - Участок магистрали.	- Количество автомашин, бензиновые; - Количество автомашин, дизельные; - Количество автобусов и газелей.	- Средняя скорость автомобиля; - Средняя длина очереди автомобилей перед светофором; - Количество циклов действия стоп-сигнала за 20 минут; - Длительность действия стоп-сигнала, минут.

Для исследования был взят участок автомагистрали в рекреационной зоне, а так же участок в жилой зоне г. Тольятти. Данные магистрали (Лесопарковое шоссе и улица Комзина) связывают два самых крупных района г. о. Тольятти и проходят через территорию лесопарка Западный, где расположены лагеря и базы отдыха, санатории и расположена коттеджная застройка.

Для расчетов было выбрано три точки на трех участках:

Первая точка - лагерь отдыха «Звездный» на участке от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий «Русский бор».

Вторая точка – санаторий «Русский бор» на участке от санатория «Русский бор» до поворота с Лесопаркового шоссе на Комсомольское шоссе.

Третья точка находится на остановке ул. Комзина на третьем участке от Комсомольского шоссе до улицы Баныкина.

На данных участках были произведены расчеты по изученным методикам, В проделанной работе выполнены расчеты интенсивности движения автотранспортных средств. Для примера приведем данные по интенсивности движения автотранспорта в точке 1 (таблица 2).

Полученные результаты по интенсивности автотранспортных средств используются в расчетах и для методики Бегма-Шаповалава, и для расчетов в программах «Эколог+».

Выполнены расчеты концентрации угарного газа по методике Бегма - Шаповалова от выбросов автотранспорта для оценки воздействия на окружающую среду и биоту. Так же произведены расчеты выбросов загрязняющих веществ на трех рассмотренных участках программными методами с использованием специальных экологических программ серии «Эколог+».

Таблица 2 - Интенсивность движения автотранспорта в точке 1 - лагерь отдыха «Звездный», на участке от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий «Русский бор»

Виды транспорта	Интенсивность движения (количество автомобилей/час) за период времени		
	8:00-9:00	14:00-15:00	17:00-18:00
Легковой грузовой	80	68	124
Средний грузовой	16	60	20
Тяжелый грузовой	4	4	4
Автобусы	20	12	8
Легковой	2536	1800	3672
Всего	2656	1944	3828

По результатам проделанной работы можно сделать следующие выводы:

1. Изучено влияние загрязняющих веществ выбросов автотранспорта на здоровье человека и окружающую среду в целом.

Выбросы автотранспорта значительно более токсичны, чем выбросы, производимые стационарными источниками. Работающий автомобиль выделяет в окружающую среду более 200 веществ и соединений, обладающих токсическим действием. Среди них следует выделить оксид азота, углеводороды, оксиды тяжелых металлов, диоксид серы.

2. Изучены методики для оценки интенсивности автотранспорта, для оценки выбросов угарного газа и программа «Эколог+» для оценки объема выбросов на участке автомагистрали.

3. Выполнена оценка концентрации угарного газа по методике Бегма – Шаповалова. Максимальное превышение $ПДК_{м.р}$ в 10,64 раз было зафиксировано вечером в промежутке 17:00-18:00 ч в точке - лагерь отдыха «Звездный» на участке автомагистрали от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий «Русский бор». Максимальное превышение $ПДК_{с.с}$ в 18,62 раз было зафиксировано вечером в промежутке 17:00-18:00 ч в точке лагерь отдыха «Звездный» на участке автомагистрали от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий

«Русский бор». Вещество очень токсично. Попадая в организм, вещество вступает во взаимосвязь с гемоглобином и образует прочный комплекс – карбоксигемоглобин. Такое соединение нарушает физиологические функции крови, блокирует транспортировку кислорода в ткани. В результате кислородного голодания нарушаются биохимические процессы.

4. Выполнен расчет выбросов автотранспорта на заданных участках.

Большее количество выбросов оксида углерода, оксида азота, монооксид азота, диаксида азота, углеводородов (бензин, керосин, газ), соединений свинца выделяется утром в точке - лагерь отдыха «Звездный» на участке автомагистрали от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий «Русский бор». Большее количество формальдегида выделяется вечером в точке - лагерь отдыха «Звездный» на участке автомагистрали от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий «Русский бор». Большее количество бенз(а)пирена выделяется днем в точке - лагерь отдыха «Звездный» на участке автомагистрали от въезда на Лесопарковое шоссе со стороны Автозаводского района до остановки санаторий «Русский бор». Наибольшее количество сажи и диоксида серы выделяется вечером в точке, которая находится на остановке ул. Комзина на третьем участке от Комсомольского шоссе до улицы Баныкина.

5. Влияние выбросов автотранспорта на биоту и биоразнообразие выражается прежде всего во влиянии SO_2 , приводящего к дигрессии, гибели зеленых насаждений, особенно хвойных пород, и в конечном счете снижению биоразнообразия .

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

ОБЩАЯ ХАРАКТЕРИСТИКА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Голиков Г.О., учащийся
Научный руководитель: Антонова И.Б., учитель
МБУ СОШ № 61
г. Тольятти

Анализ научной литературы, посвящённой вопросам национальной безопасности в общем и экономической безопасности в частности, показывает постоянно растущую заинтересованность как российского, так и зарубежного научного мира к вопросам углублённого научного анализа национальной безопасности и поиска путей её совершенствования и укрепления.

Обзор публикаций на тему безопасности показал достаточно широкий спектр концептуальных и научных подходов к определению понятие «безопасность». Тем не менее, их можно условно объединить на несколько групп, объединённых общими сущностными концепциями. Наиболее часто авторы используют дефиниции понятия «безопасность» через такие подходы к определению безопасности как:

- субъект-объектное отношение;
- защита интересов личности, общества и государства;
- защищённость личности, общества и страны от внешних и внутренних угроз их безопасности.

Безопасность как субъект-объектное отношение. При таком подходе к формированию понятия «безопасность», прежде всего, определяются субъекты безопасности и её объекты.

Субъектами (от лат. subjectus – лежащий в основе) безопасности, т.е. теми, кто создаёт, обеспечивает безопасность могут быть личность (индивид), общество и государство, обладающие полномочиями, правом и обязательством по обеспечению определённых видов безопасности в т. ч. экономической на основании с действующего национального законодательства. Объектом (от лат. objectum – предмет) безопасности являются: личность, общество и государство. Личность, общество и государство, как видно из вышеизложенного, в силу жёсткой взаимосвязи между собой, обусловленной их природой, исполняют одновременно две роли - субъекта и объекта безопасности. Причём в отдельных случаях каждый субъект безопасности может выступить сразу в нескольких ролях: личность – в качестве отдельного индивида и в качестве члена какой-либо социальной группы или гражданского общества; государство – в качестве отдельного, суверенного национального страны и в качестве одной из составляющей межгосударственных блоков, союзов или иных сообществ государств.

В зависимости от субъекта или объекта безопасности определяются и такие уровни безопасности как личная (субъект или объект безопасности – личность, человек, индивид), безопасность общества (социум, общественность региона, определённого административно-территориального образования), безопасность страны (национальная безопасность) и международная (коллективная, региональная) безопасность.

Стратегия национальной безопасности определила, что обеспечение безопасности осуществляют органы государственной власти и органы местного самоуправления. В этом случае появляются субъекты, определяемые как субъекты именно обеспечения безопасности, отличающиеся от субъектов безопасности. Иными словами, субъектом обеспечения безопасности являются органы государственной власти (федеральные и региональные) и местного самоуправления, а объектом обеспечения безопасности – сама безопасность. Таким образом, понятие «безопасность» становится самостоятельным объектом научного изучения и анализа.

Стратегия национальной безопасности определила и основные государственные

интересы, которыми являются:

- укрепление Российской Федерации как страны в целом через усиление обороноспособности страны, сохранение его суверенитета и независимости, обеспечение государственной и территориальной целостности;

- укрепление межнационального согласия, улучшение политической и социальной стабильности через развитие демократических институтов во взаимодействии страны и гражданского общества;

- дальнейшее развитие социальной политики через улучшение уровня и качества жизни населения страны в целом и каждого региона в частности, укрепление здоровья населения, стабильное демографическое развитие;

- дальнейшее развитие гуманитарной политики через сохранение и развитие искусства и культуры, традиционных российских моральных и духовно-нравственных ценностей;

- усиление конкурентоспособности продукции промышленности и сельского хозяйства, подъём национальной экономики;

- поддержание статуса Российской Федерации как одной из лидеров мировых держав, фундамента стратегической геополитической стабильности и взаимовыгодных международных партнёрских отношений в условиях полицентричного мира.

Таким образом, государственные интересы могут быть соблюдены через стратегическое планирование, разработку и воплощение в действительность государственных программ обеспечения национальной безопасности Российской Федерации по каждому из видов национальной безопасности, как того и требует федеральное законодательство.

Стратегия национальной безопасности определила, что обеспечение безопасности осуществляют органы государственной власти и органы местного самоуправления во взаимодействии с институтами гражданского общества через принятие всевозможных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение государственных интересов.

Всего в Стратегии национальной безопасности определено восемь видов национальной безопасности, при этом обеспечение национальной безопасности на региональном уровне рассматривается только при обеспечении экономической безопасности. Из вышеуказанных направлений национальной безопасности более детализирована экономическая безопасность, которая принята в отдельной Стратегии экономической безопасности, и в которой в частности вводятся четыре уровня экономической безопасности: федеральный, региональный, муниципальный и отраслевой.

Стратегия экономической безопасности Российской Федерации также дополнила Стратегию национальной безопасности введением понятия «экономической безопасности» как «состояния защищённости национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство её экономического пространства, условия для реализации стратегических государственных приоритетов Российской Федерации».

Экономическая безопасность является частью национальной безопасности и гарантией независимости Российской Федерации. Экономическая безопасность обеспечивает самостоятельную экономическую политику и создает условия стабильности и экономического развития в условиях глобализации мирового хозяйства.

Национальная безопасность — это защищённость страны от внешних и внутренних угроз, устойчивость к неблагоприятным воздействиям извне, обеспечение внутренних и внешних условий существования страны, которые гарантируют возможность стабильного прогресса страны и его граждан. Она включает в себя составляющие: военную, экологическую, информационную, социальную, энергетическую и другие виды безопасности. Все они взаимодополняют друг друга.

Экономическая безопасность – совокупность внутренних и внешних условий, которые благоприятствуют эффективному динамическому росту национальной экономики, её

способности удовлетворять потребности общества, государства, индивида, обеспечивать конкурентоспособность на внешних рынках, гарантирующую от различного рода угроз и потерь.

Отличительной чертой экономической безопасности является то, что она предопределяет все необходимые для существования интересы личности, общества и государства. Недостаточность проработки экономических отношений или неспособность властей защитить экономические интересы личности, общества и страны могут свидетельствовать о слабости власти, а в дальнейшем и низкой внутренней экономической безопасности и иных проблем. Экономическая безопасность существует в совокупности с безопасностью правовой, политической, технологической, экологической и других.

Угроза экономической безопасности – совокупность условий и факторов, создающих прямую или косвенную возможность нанесения вреда национальным интересам Российской Федерации в экономической сфере.

Главная деятельность органов государственной власти заключается в недопущении угроз или сведение их минимальному влиянию на экономику государства. Минимизация угроз укрепляет экономическую безопасность, а недооценка угроз или непринятие должных мер содействует возникновению угрозы экономической безопасности страны и способна нанести вред его экономике.

Невзирая на множество научных трудов по теме экономической безопасности, среди учёных нет единой трактовки понятия «экономическая безопасность» (таблица 1).

Упрощённая схема экономической безопасности Российской Федерации представлена на рисунке 1.

Рисунок 1 - Упрощённая схема экономической безопасности Российской Федерации

Таблица 1 – Трактовка понятия «экономическая безопасность»

Автор	Трактовка понятия «экономическая безопасность»
В.А. Савин	Система защиты жизненных интересов России. При этом субъектами этих интересов могут выступать как экономика страны в целом, так и определенные субъекты федерации, юридические и физические лица различных сфер экономической деятельности.
С.Ю. Глазьева	Состояние экономики с точки зрения ее возможностей самостоятельного обеспечения устойчивого социально-экономического развития страны или поддерживания должного уровня конкурентоспособности национальной экономики в условиях международной глобальной конкуренции.
С.Ф. Федораев	Состояние национальной экономики, гарантированно обеспечивающее ее устойчивое позитивное развитие в условиях появления деструктивных внутренних и внешних факторов.
Е.Л. Олейников	Защищенность экономических отношений, определяющих позитивное развитие его экономического потенциала, и которое обеспечивает стабильн7ое повышение уровня благосостояния граждан, государства его отдельных социально-демографических групп и формирующих основы защиты страны от опасностей и угроз.
В. Сенчагов	Не только защищенность национальных экономических интересов, но и готовность институтов власти к защите национальных интересов развития отечественной экономике, поддержание социально-политической устойчивости общества и государства.
Л.И Абалкин	Совокупность условий и факторов, обеспечивающих независимость национальной экономики, ее стабильность и устойчивость, способность к постоянному обновлению и совершенствованию.

Таким образом, экономическая безопасность - состояние защищённости национальной экономики от внешних и внутренних угроз, при которой обеспечиваются экономический суверенитет страны, единство её экономического пространства, условия для реализации стратегических государственных приоритетов Российской Федерации, ставящих конечной целью всемерное развитие человеческого потенциала совместно с улучшением уровня и качества жизни населения.

Библиографический список

1. Российская Федерация. Федеральные законы. О безопасности. [Текст] Федеральный закон № 390-ФЗ принят Государственной Думой 28.12.2010 г. // Собрание законодательства РФ. - N 1. - ст. 2.

2. Абалкин, Л. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. 1994. № 12.

3. Гладких, В.И. Экономическая безопасность Российской Федерации: к вопросу о понятии, структуре, угрозах, противодействии / В.И. Гладких // Вестник Вятского государственного гуманитарного университета. 2006. N 14. С. 76 – 84.

4. Глазьев, С.Ю. Основы обеспечения экономической безопасности страны - альтернативный реформационный курс // Российский экономический журнал. 1997. №1-2 URL: http://www.re-j.ru/archive/1997

5. Олейников, Е.А. Экономическая и национальная безопасность: Учебник / Под ред. Е.А. Олейникова. - М.: Издательство «Экзамен», 2004. — 768 с.

6. Савин, В.А. Некоторые аспекты экономической безопасности России //

Международный бизнес России. - 1995. - №9.

7. Сенчагов, В.К. Экономическая безопасность России: общий курс: учебник / под ред. В.К. Сенчагова. 2-е изд. М.: Дело, 2005. 896 с.

8. Федораев, С.В. Теоретико-методологические подходы к определению содержания и классификации инноваций как фактора обеспечения экономической безопасности. // «Вестник Санкт-Петербургского университета ГПС МЧС России» URL: http:// vest-nik.igp-s.ru/wp-content/uploads/V21/7.pdf

ИНФОРМАЦИОННО-УПРАВЛЕНЧЕСКИЙ КОНТУР ПРЕДПРИЯТИЯ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Губанова С.Е., аспирант, Михайликов Н. студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Особую проблему в сфере экономической безопасности в стране добавляет быстрая изменчивость методик, основанная на изменчивости нормативно-правовой базы, информационной инфраструктуры и развитии технологий. Специалисты всех уровней должны осознавать необходимость постоянного переобучения и освоения новых компетенций [1]. В связи с чем, информационно-управленческий контур становится основным ключом к эффективности и конкурентоспособности компании. Базовые требования – качество и защищённость потоков данных, управляющих сигналов, информационного обмена в целом [2]. Этим обоснована актуальность темы исследования и ее выбор для детального изучения.

Сегодня на предприятиях можно выявить конкретные угрозы, которые касаются целостности, конфиденциальности, авторства и некоторых других существенных моментов. Особенно важен контроль и регламентация доступа к информационным ресурсам. Есть современные технологии, которые решают выявленные проблемы надёжно и безопасно [3]. Но применение данных технологий вызывает определённые трудности, порог их освоения достаточно высок для обычного пользователя. А ситуация сегодня такова, что именно широкое использование защищённых информационно-коммуникационных технологий способно поддерживать информационную и экономическую безопасность предприятия на должном уровне. Не только высококлассные специалисты, не только руководство, но и рядовые сотрудники должны умело оперировать этими средствами.

Отметим основные тезисы: передовые информационные методы чрезвычайно важны, при этом они реально сложны, изменчивы, не имеют интуитивно-понятного интерфейса и требуют постоянного обучения и освоения широким кругом пользователей, не имеющих специальной подготовки [4].

Посмотрим на ситуацию, например, с криптографической защитой как одним из важнейших элементов информационной защиты. Используется для надёжной аутентификации, подтверждения авторства, конфиденциальности, целостности и других крайне востребованных задач. Технология является широко распространённой и в ряде случаев обязательной для электронных торгов, тендеров, госзакупок, отправки отчётности госорганам, электронного документооборота, доступа к информационным системам, удалённых сервисов, любого обмена защищённой информацией. Использование данной технологии можно условно классифицировать в разрезе практического использования на три уровня: создатели стандартов и методик, обязательных к применению бизнесом; специалисты подразделений, администрирующие и встраивающие данные методики в специфические бизнес-процессы предприятия; рядовые пользователи, в силу должностных обязанностей вынужденные применять эти техники в постоянном режиме. Понятно, что

степень понимания в этой вертикали совершенно различна, как и различны решаемые задачи при общей цели – защита информации. Особая нагрузка падает на среднее звено – администраторов бизнес-подразделений, которые наряду с профессиональными компетенциями, знанием предметной области своей организации, умением интегрировать чужие техники в свои процессы должны также продуктивно коммуницировать как с рядовыми исполнителями, так и с менеджментом, а также обеспечивать обратную связь создателям стандартов и методик.

В первую очередь эти создатели работают в интересах госорганов, которые по законодательству должны получать определённую информацию от компаний, работающих на территории данного государства. Проблема в том, что государственных ведомств много, и единых методик на сегодняшний день нет, каждое ведомство использует свои алгоритмы, специальное ПО, заявляет свои требования.

Минус – отсутствие единой системы, разнобой, конгломерат отдельных алгоритмов, знаний, которые легко перепутать и которые никак не помогают администраторам.

Плюс – используя данные методики можно считать, что требования по ЗИ выполнены полностью и информация, полученная и переданная таким образом, является абсолютно доверенной. Кроме того, их можно использовать для построения собственных схем, и уровень доверия к ним будет также довольно высок.

Не обязательно только государственные ведомства могут диктовать стандарты. Информационная безопасность, как и экономическая безопасность, наиболее актуальна сегодня для бизнеса. Крупные распределённые корпорации, имеющие филиалы, дочерние подразделения, сбытовые сети и сети поставщиков, также вырабатывают свои техники и требования по защищённому обмену информацией, обязательные для подконтрольных организаций. Так же как и, например, некоторые банки, работающие в системе «банк – клиент».

В результате методик, которые требуют администрирования, интеграции в существующие бизнес-процессы, ежедневного использования, становится реально много. Цель – защита информации – одна и та же, базовая технология – в основном PKI, то есть Public key infrastructure, или инфраструктура открытых ключей - также одна и та же, а способов применения – множество.

И это ещё хорошо, если конкретный пользователь работает с одной конкретной методикой. Один взаимодействует с банком, другой с Налоговой службой, третий с Пенсионным фондом, четвёртый с Агентством по экологии и т.д.

Но есть подразделения, которые вынуждены работать сразу по нескольким стандартам с разными организациями, государственными и негосударствеными. Например, дилерские центры, которые, с одной стороны, отдельные компании, а с другой имеют дилерские соглашения с компаниями-производителями и должны также выполнять их требования. Штат, как правило, невелик, разделить функции не получается. И здесь надо создавать определённую схему, понятную, прозрачную и надёжную.

Возможно, со временем методики будут унифицированы, ключи ЭП и шифрования также можно будет сделать универсальными, но это дело будущего, а сегодня надо решать сегодняшние проблемы.

Кроме того, задача интеграции и гармонизации различных практик по защите информации, да ещё в применении к огромному разнообразию конкретных бизнесов – задача крайне сложная и не факт, что вообще решаемая. Либо решаемая частично [5].

Например, общение с государственными органами требует применения отечественных криптоалгоритмов, а взаимодействие с мировыми компаниями возможно только по западным криптостандартам. Они не сводимы в принципе по этому параметру.

Отметим, что степень ответственности за решение практических задач бизнеса, связанных с защитой информационных потоков, всё-таки разная. Специалисты верхнего звена создают эталонные схемы решений, реализуют их рядовые пользователи, а среднее звено – администраторы – должны обеспечить функционирование схем для конкретной

предметной области и наличествующего персонала. Для этого они создают свои методики, инструкции, руководства, обучают пользователей, мониторят изменения и результаты, дают фидбэк вышестоящим организациям. Имеет смысл составить некоторое описание, которое поможет в использовании криптографических средств, связанных с ключами и сертификатами, когда их достаточно много.

Для этого надо расписать параметры, в которых возможна вариативность, и по этим параметрам идентифицировать то средство, которое требуется для каждого случая. По итогу каждому средству надо придумать алиас, неформальное название, которое всем сотрудникам понятно и известно.

Параметров может быть много, во всяком случае, не меньше, чем нужно для однозначного определения одного элемента среди ряда других имеющихся. Заметим, что некоторые из них интересны только администратору, а не рядовому пользователю.

Таблица 1 – Примерный набор параметров

№	Параметр	Для пользователя	Для администратора
1	Функция: аутентификация доступа, ЭП, шифрование	+	+
2	Используется ли внешний ключевой носитель	+	+
3	Срок действия ключа (сертификата)	-	+
4	Криптоалгоритм	-	+
5	Целевая ИС, или сайт, или приложение	+	+
6	Алиас	+	+
7	Где и кем создаётся ключ	-	+
8	Длина ключа	-	+
9	Указание на пароль или PIN-код	+	+

Набор параметров может существенно отличаться, в зависимости от конкретной ситуации. Зачастую имеются специфические маркеры, которые могут быть у сертификата (например, кириллица или латиница)

Максимальная информация должна быть отражена в инструкциях. Но инструкции, как правило, это довольно объёмные и сложные для понимания тексты. И они всегда создаются для каждого средства отдельно.

А для оперативной работы должна быть короткая сводка, объединяющая все ключевые параметры по всем инструментам таким образом, чтобы можно было однозначно выбрать нужный.

Если мы пока не можем унифицировать систему использования криптографических средств на предприятии, мы должны создать максимально прозрачный и чёткий, согласованный, документально описанный способ работы по всем средствам и всем задачам. Причём необходимы документы разной степени детализации – от максимальной, с объяснением сути, нюансами, логикой, до простого перечисления порядка действий, а также сравнительной таблицы по аналогичным средствам. Как раз такой таблицы, как правило, нигде и нет. Чтобы сотрудник безошибочно выполнял свои обязанности, у него должны быть условия и у него должна быть вся необходимая информация.

Таким образом, можно сделать следующие выводы:

1. Создание информационно-управленческого контура на предприятии позволит стабилизировать возмущения внутренней среды, возникающие в результате появления внешних угроз.

2. Необходимо четко разграничить предназначение циркулирующей внутренней выходной информации: инструкция, сводка, положение, методика.

3. Необходимо унифицировать применяемую на производстве систему криптографических средств и представить ее в читаемом табличном виде, введя зоны ответственности и ответственных лиц из числа топ-менеджмента с целью повышения

экономической безопасности.

Библиографический список

1. Программа «Цифровая экономика РФ». [Электронный ресурс]. - Режим доступа: **http://static. government.ru/media/files/9gfm4fhj4psb 79i5v7ylvupgu4bvr7m0.pdf**.
2. Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 05.12.2016 № 646). [Электронный ресурс]. Источник: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.
3. Губанова, С.Е. Особенности работы корпоративного Удостоверяющего центра крупного промышленного предприятия // Информационные системы и технологии: управление и безопасность. Сборник статей II Международной заочной научно-практической конференции // Поволжский гос. ун-т сервиса – Тольятти - Русе: Изд-во: ПВГУС. 2013 № 2, С. 185-191.
4. Глухова, Л.В. Концептуальные основы управления интеллектуальным потенциалом предприятия // Вестник Волжского университета имени В.Н. Татищева. 2016. №1(35), том 2. С. 117-125.
5. Глухова, Л.В., Губанова, С.Е. Некоторые аспекты менеджмента информационной безопасности промышленных комплексов // Вестник Волжского университета имени В.Н. Татищева, 2015. № 3 (34), С. 135-144.

ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

Маслов А.А., студент
Научный руководитель: Голикова О.В., к. э. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

С недавних пор в России получила большую популярность у экономических субъектов полутеневая экономика – процессы, при которой экономические блага уводятся от налогообложения в тень частично.

Уклонение от уплаты налогов считается прибыльной деятельностью организованной преступности, с этой целью, организовываются различные коммерческие структуры основное предназначение которых заключается в оказании помощи в уклонении от уплаты налогов, сборов. Средства, укрытые от налогов, автоматически переходят в разряд источника финансовой поддержки организованной преступности, в том числе и терроризма. При прочих равных условиях, бизнесмены, в деятельности которых возникла «необходимость» в уклонении от уплаты налогов и сборов, возникает обязанность по осуществлению различных видов платежей структурам, противоположным государственным, то есть криминальным структурам.

Сокрытые денежные средства опасны тем, что они создают благоприятные условия для прочих видов преступлений различной направленности.

Одним из наиболее сильнейших отрицательных факторов, влияющим на степень защищённости, является экономическая преступность. Как правило, она представляет собой массовое явление, которое формируется под воздействием всей совокупности произошедших преступлений.

Само по себе экономическое преступление - наказуемое действие, корыстного и систематического характера.

В уголовном праве РФ есть определение преступлений в области экономики. Это такой вид правонарушений, при котором существует определенный объект посягательства: имущественные и производственные отношения, экономические права физических и юридических лиц, региональных и федеральных, а также муниципальных и государственных образований.

Одним из самых распространенных видов экономических преступлений в России является незаконное присвоение имущества, на втором месте - коррупция и взяточничество, а также - искажение финансовой отчётности и целенаправленное нарушение бухгалтерского учета.

Преступления в сфере экономики возникают из-за активного государственного вмешательства в дела отдельных экономических субъектов, а также систематического изменения налогового законодательства.

Кроме этого, существуют также отдельные факторы возникновения преступлений в сфере экономики:

1. Экономический фактор, к нему относятся:
- деструктивное финансовое состояние бизнеса и домохозяйств;
- падение объёмов промышленного производства (обрабатывающей отрасли);
- постоянно увеличивающиеся издержки, связанные с предпринимательской деятельностью;
- отток капитала;
- снижение налогового потенциала отдельных слоев экономических субъектов;
- отсутствие финансирования инвестиций в научно-исследовательские и опытно-конструкторские разработки;
- большая налоговая нагрузка.
2. Законодательные факторы, к ним относятся:
- слабо проработанное законодательство;
- нестабильность нормативно-правовых норм;
- несовершенство налоговых «рычагов»;
- несправедливые методы оценки имущества в качестве объектов обложения;
3. Организационные факторы, к ним относятся:
- увеличивающиеся тенденции криминализации экономики;
- отсутствие всякой самостоятельности в регулировании налоговой политики субъектов Российской Федерации;
- несовершенство видов и методов налогового администрирования;
- слабые взаимодействия и согласованности различных мероприятий между структурными подразделениями и главками, а также между ведомствами в целом.

Формы проявления преступлений при криминализации экономики: представлены в таблице 1.

Таблица 1 - Формы проявления преступлений при криминализации экономики

Факторы возникновения	Формы проявления преступлений
Подлог фактов и искажение итогов всей финансово – хозяйственной деятельности организации в учётной документации и регистрах бухгалтерского и налогового учётов	- осуществление и оформление хозяйственных ситуаций и сделок без должного документального фиксирования; - отсутствие фиксирования поступления в организацию товарно-материальных ценностей; - отсутствие фиксации денежной выручки от продажи товаров (работ, услуг) в соответствующих первичных документах
Операции с денежной наличностью в нарушение законодательству РФ	- нарушение использования денежных средств (рублёвой и валютной наличности); - нарушение кассовой дисциплины
Искажение объекта налогообложения	- фиктивное занижение объёмов реализации; - завышение стоимости выполненных работ, оказанных услуг; - сокрытие объектов налогообложения и их стоимости
Умышленное искажение результатов экономической деятельности	- искажение размеров налоговой базы; - фиктивные расходы
Фальсификация объектов налогообложения	- фиктивный бартер; - лжеэкспорт; - подмена объекта налогообложения либо его стоимости

Искажение результатов финансово-хозяйственной деятельности ведёт к возникновению внутренних угроз экономической безопасности, возникающих в налоговой сфере и снижающие экономическую безопасность государственной экономики:

- угроза низкой доходной части бюджета;
- рост социальной напряжённости;
- повышения уровня теневой экономики;
- снижение инвестиционной привлекательности России и регионов;
- криминализации экономики.

Самый негативный и губительный эффект на экономику оказывает коррупция. Как ни странно, но сильному коррупционному давлению подвергаются малый и средний бизнес, в основном от них зависят экономические настроения и рост национального хозяйства. Такие организации имеют ряд преимуществ перед крупным бизнесом: они предоставляют больше возможностей для проявления инициативы и творчества, также такой тип бизнеса в состоянии достаточно быстро перестроить производство в соответствии с меняющимся состоянием рынка.

Негативный эффект теневого сектора экономики может проявляться в следующем виде:

- отток материальных, финансовых, трудовых и интеллектуальных ресурсов из сфер легальной экономики;
- разрушение экономической структуры легальной экономики;
- проникновение коррумпированных элементов в экономическую структуру легальной экономики;
- непосредственное развитие теневого сектора;
- угроза утечки финансовых потоков в развитие криминальных структур.

Таким образом, основными внутренними угрозами экономической безопасности, в первую очередь являются стабильно высокий уровень уклонений от уплаты налогов и сборов в бюджетную систему, а также ежегодный прирост в неуплате налогов и сборов, тем самым повышается угрозы экономической безопасности. Также следует отметить высокий уровень коррупции в различных государственных учреждениях и оффшоризация Российской экономики в целом.

Библиографический список

1. Анищенко, В.Н. Расследование экономических преступлений. Теоретико-методологические основы экономико-правового анализа финансовой деятельности [Текст]: учебное пособие для бакалавриата, специалитета и магистратуры / В.Н. Анищенко, А.Г. Хабибулин, Е.В. Анищенко. - 2-е изд., испр. и доп. - М.: Издательство Юрайт, 2018. - 250 с.
2. Безопасность. [Электронный ресурс] // Энциклопедия права URL: http://encyclope-diya_ prava.academic.ru/491/Безопасность.
3. Борин, Б.В. Понятие оперативно-розыскной профилактики преступлений / Б.В. Борин, Я.Г. Ищук // Пробелы в российском законодательстве. 2017. N 3. С. 381 – 386.
4. Чистотина, О.Н. Взаимодействие органов внутренних дел с общественностью по противодействию коррупции / О.Н. Чистотина // Социально-экономические и правовые меры борьбы с преступлениями и иными правонарушениями: Материалы межрегиональной научно-практической конференции (г. Рязань, 28 марта 2018 г.). Рязань, 2018. С. 318 – 328.

МЕЙНСТРИМ КАК НОВЕЙШЕЕ НАПРАВЛЕНИЕ ЭКОНОМИЧЕСКОЙ МЫСЛИ

Михайликов Н.А., студент
Научный руководитель: Щукина А.Я., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Любая страна является высокоразвитой, если имеет современную экономику, эффективность функционирования которой напрямую связано с развитием экономической мысли, что в итоге позитивно влияет на укрепление национальной безопасности.

Мейнстрим экономической науки - это все те концепции, в которых экономическое поведение людей трактуется с точки зрения оптимизации. К мейнстриму относятся все ветви неоклассической теории (в том числе и самая модная из них - школа новых классиков), а также неокейнсианство и новый институционализм. Представители всех этих ветвей и школ экономической мысли трактуют поведение людей как оптимизирующее, а во всех моделях мейнстрима экономические функции, начиная от функций полезности или прибыли индивидуальных агентов и заканчивая функциями потребления или спроса на деньги на макроуровне, выводятся из оптимизирующего выбора отдельных субъектов [1]. Говоря о современном мейнстриме, мы имеем в виду те особенности, которые преобладают в экономической теории с 70-х годов XX в. Поэтому нельзя согласиться с теми, кто считает, что "мейнстрима" в обычном значении сейчас нет, что сегодня якобы господствует состояние так называемого "постмодерна", и "признание постмодерна логически отрицает "мейнстрим" - существование главного направления, а признание "мейнстрима" отрицает постмодерн - отсутствие чего-то общего, главного. Поскольку большинство ныне здравствующих экономистов признают наличие трудно классифицируемого многообразия теорий, то вольно или невольно они признают отсутствие мейнстрима...

Оптимизация как основной способ описания экономического поведения и равновесный анализ как основной метод исследования экономической динамики - вот ведущие принципы современного мейнстрима. Если некий современный экономист мечтает, чтобы его работы упоминались или, еще лучше, анализировались в учебниках по экономической теории, а сам он имел бы шансы оказаться в числе претендентов на получение Нобелевской премии, то ему приходится строить модели на основе этих принципов.

В «мэйнстриме» центральным аппаратом анализа выступает анализ рынков. Кривые предложения и спроса пересекаются в точке, отражающей равновесную цену и равновесное количество продаваемых товаров. Это равновесие может быть нарушено в результате изменения факторов, вкусов потребителей, изменение издержек производства, изменение технологий, психологическими сдвигами и т.д. В этом случае реальная цена будет

отличаться от равновесной. Равновесие называется устойчивым, если отклонение от него сопровождается возвращением к первоначальному состоянию. В противном случае оно называется неустойчивым. Стабильность этого равновесия зависит от продавцов и покупателей. Относительно проблемы равновесия и отклонения имеются два подхода. Во-первых, Л. Вальраса Дж. Хикса. Когда преобладает спрос, покупатели стремятся увеличить закупки, цена возрастает. В этих условиях рынок стабилизируется, и наоборот, если спрос меньше предложения, то продавцы стремятся снизить свои цены и избыток предложения исчезает. Ситуация полностью определяется наклонами (эластичностью) кривых спроса и предложения. Во-вторых, А.Маршала. В том случае, когда цена, по которой покупатели готовы заплатить за данное количество товаров выше цены, приемлемой для продавца, следовательно, производство расширяется [5]. Равновесие будет устойчивым, если увеличение объема выпуска продукции сокращает разрыв между теми и другими ценами. При неравновесной ситуации, а экономика обычно находится именно в неравновесной ситуации, смещения спроса и предложения происходят перманентно под действием указанных выше факторов. Подлинная теория экономики – это теория, обобщающая факторы, определяющие направление и скорость такого движения.

Самый популярный метод в «мэйнстриме» – сравнительный статический анализ, суть которого заключается в изучении влияния сдвига значений экономических параметров на функцию экономической системы. Цель этого анализа заключается в том, чтобы определить, как изменяется равновесие в результате экзогенных воздействий. Но «мэйнстрим» абсолютно не лишён динамической постановки задачи. Большая часть моделей экономического роста, исходным пунктом которых приняты предложения Р. Солоу, являются динамическими моделями. Большая часть параметров этих моделей признаются функциями времени. Кроме того, сдвиг кривой спроса и предложения также создают динамическую версию изменения точки равновесия.

Итак, заслуга «мэйнстрима» может быть измерена следующими положениями:

- созданием каркаса экономического знания, базовых исходных предпосылок и моделей, развитие и изменение которых составило содержание иных исследовательских программ и научных школ, в том числе и тех, которые противопоставили себя «мэйнстриму»;

разработкой общих исходных предпосылок моделирования, с возникновением потребностей в эконометрике;

- применение научного метода познания социально-экономических явлений и разработка вполне действенных для своего исторического периода времени объяснительных и описательных схем и моделей, влияющих на подготовку правительственных решений;

- расширение проблематики экономического анализа от рассмотрения проблем накопления и использования богатства, до проблем бедности, безработицы, цен, капитала, производства, обмена, распределения, торговых, валютных кризисов, экономического развития (роста), организации рынков, монополизма, эксплуатации, равновесия и устойчивости экономической системы и др.

Теперь нужно детально разобраться, в чём же видится пересмотр природы общественных наук и, в частности, экономики, насколько он возможен. Насколько правомерны и логически верны приводимые тезисы зарекомендовавшим и ставшим очень популярным старым институционалистом. С первых слов задаётся установка о пользе эволюционных и институциональных идей. Действительно, ещё А.Смит отмечал, что в экономике принимаются решения, которые не являются следствием замысла и целевого назначения, то есть возникают спонтанно, случайно. Однако, наличие таких решений совсем не означает, что их доля в общем объёме решений преобладает. Ничего неизвестно, как такие решения взаимосвязаны и взаимодействуют с другими типами решений, а именно с теми, которые являются следствием и замысла и целенаправленных действий, порождающих затраты.

Кстати, аспект затрат очень важен, насколько различные типы решений приводят к

большим или меньшим затратам? В связи с этой неясностью, остаётся проблема по поводу утверждения о том, что социальный порядок может быть организован без централизованного управления. Да, какая-то регуляция возможна и без централизованного управления, но такие виды общественной организации остались давно в прошлом и на протяжении обозримого периода, особенно в последние столетия бурного и, как принято считать, успешного развития капитализма, приведшего к научно-техническому прогрессу и развитию наук и искусств, хотя существовало сильное обратное влияние, централизация управления присутствует в разных странах [5]. Более того, компьютерная революция, широкая информатизация многих процессов – производства, обмена, распределения, потребления, управления, порождает эффект локальной централизации, ибо сервер есть не что иное как некий центр, собирающий информацию, обрабатывающий и распределяющий её.

Экономическая наука в направлении мейнстрима попадает в странную ситуацию: следуя базовым установкам о рыночной системе, о рынках, она как будто не видит эффектов централизации и новых форм управления и организации общества, а если и видит, то пытается приложить все интеллектуальные усилия для доказательства того, что рынки эффективнее, чем централизованное управление какие бы формы оно не принимало. Это не совсем корректное утверждение, ни на чём не основанное и нечем на практике не подтверждаемое, потому что сравниваются несравнимые объекты, процессы, изначально неверно устанавливается соотношение между ними. Рынок порождает конкуренцию там, где она по существу не нужна и приводит к перерасходу ресурса за счёт искусственного роста разнообразия, который экономическая наука не оценивает, не считает, не принимает во внимание ни в одной модели, ни в рамках «мэйнстрима», ни в рамках эволюционной экономики.

Считается, что мэйнстрим исходит из представлений об абсолютной рациональности, что не отвечает наблюдаемым фактам, когда человек ведёт себя ограниченно рационально (Г. Саймон) [4]. Кроме того, с появлением концепции эндогенных предпочтений эволюционисты связывают широкие перспективы в противостоянии с «мэйнстримом» [4]. Проблема в том, что со времени написания статьи Г.Беккером «О вкусах не спорят». Мэйнстримовская точка зрения не изменилась, что предпочтения индивидов заданы и стабильны в экономической системе. Активным противником этой идеи был Дж. Гэлбрейт, на которого, почему-то, стали мало ссылаться, в отличие от других экономистов, повторяющих уже этот протест и говорящих, что вкусы изменчивы и формируются самой экономической системой, изменяются при измене социально-экономических условий, например, рекламы и иных психологических факторов [3]. Тем самым, сдвиги в предпочтениях и выборе вводятся в процесс эволюции экономической системы, что повышает сложность анализа, но и приближает его к правдоподобной интерпретации. Вместе с тем, если это делает мэйнстрим, зачем упрекать его в таком совершенствовании [3]. Это всё равно, что упрекать человека, который отказался от курения или алкоголя, что он поменял принципы, но он же приблизил их к лучшему состоянию, а не к худшему. Та же аналогия относится и к «мэйнстриму». Разрыв экономического знания и разведение его по принципам и условным допущениям порождает ненужное противоборство между теоретическими школами и является отражением организации самой экономической науки, то есть сферы, работающей и воспроизводящей знания, причём не всегда эффективно это делается отдельными ее школами.

Справедливым остаётся утверждение Дж Ходжсона [4]. Относительно весомого изменения «мэйнстирма». С этой трактовкой следует определенно согласиться и, более того, подчеркнуть те моменты, которые не учтены в проводимом анализе. Важно то, что такое серьезное изменение происходит за счёт повышения роли «экономического империализма», то есть вовлечения в экономический анализ других дисциплин, расширение предметной области исследований, модификации принципов, например, рассмотрение динамических изменений, ограниченной рациональности и неполноты информации. Данное изменение сопровождается ростом плюрализма и снижением строгости анализа, ещё большей

релятивизацией экономической науки и фрагментарностью. Важные проблемы, на которые обращали поверхностное внимание в экономической науке, теперь вышли на первый план. Речь идёт о принципе суверенитета потребителя. Если выбор может быть навязан чем или кем-либо, то нужны иные модели, описывающие процедуру выбора. Более того, тогда экономисты и не имеют независимой кривой спроса, какой бы наклон она не имела. В таком случае модели и схемы, предполагающие введение кривых предложения и спроса обязаны установить зависимость между кривыми спроса и предложения как графическую, так и аналитическую. Иначе мы располагаем просто ложными представлениями. Когда анализируем факторы сдвига кривых, например, шоки спроса или предложения.

Исходя из выше изложенного, следует сделать вывод, что новейшие экономические теории, позволяют усовершенствовать работу современной экономической системы, а, следовательно, укрепить экономическую безопасность.

Библиографический список

1. Справочник по теории Мейнстрима / Под ред. А.А. Красовского. - М.: Наука, 2007. - 712 с.
2. Министерство экономического развития [Электронный ресурс] - Режим доступа: URL: http://economy.gov.ru/minec/main
3. Собрание сочинений Гэлбрейта [Электронный ресурс] - Режим доступа: URL: http:// economy.samregion.ru/
4. Википедиа [Электронный ресурс] — Режим доступа: URL:https://ru.wikipedia.org/wiki
5. Кольберт, Ж. Б. Теории по концепции мейнстрима. - М.: Академия, 2016. - 447 с.
6. Антонова, М. Экономическая мысль в ретроспективе. М. Антонова. - М.: CAF-Россия, 2019 г. - 50 с.
7. Волкова, Е.Д. Эволюционизм в экономике: монография / Е.Д. Волкова. - М.: Готика, 2018. - 165 с.

ПОВЫШЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ОСНОВЕ СОВЕРШЕНСТВОВАНИЯ УПРАВЛЕНИЯ ФИНАНСОВЫМИ РЕЗУЛЬТАТАМИ ЕГО ДЕЯТЕЛЬНОСТИ

Муравьева А.А., студент
Научный руководитель: Журова Л.И., к. э. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Финансовые результаты являются важнейшей характеристикой экономической деятельности хозяйствующих субъектов. Величина и динамика финансовых результатов определяют уровень финансовой конкурентоспособности и экономической безопасности предприятия, оценивают, в какой степени гарантированы экономические интересы предприятия и его контрагентов по финансовым отношениям. Данное обстоятельство обусловливает актуальность темы работы, посвященной воспросам повышения экономической безопасности предприятия на основе совершенствования управления финансовыми результатами его деятельности.

Финансовый результат предприятия может выражаться либо в форме прибыли (превышения доходов над расходами), либо в форме убытка (превышения расходов над доходами) [3]. Показатели финансовых результатов являются наиболее важными в процессе диагностики экономической безопасности предприятия. На практике при анализе финансовых результатов чаще используются следующие методы, основанные на

использовании финансовой отчетности предприятия: методы горизонтального, вертикального, сравнительного, факторного анализа, а также анализ коэффициентов [2, 3].

Проведем анализ финансовых результатов предприятия на примере ПАО «АВТОВАЗ». Финансовые результаты ПАО «АВТОВАЗ» определяются состоянием и тенденциями развития автомобильного рынка. На рис. 1 представлена динамика продаж легковых автомобилей в России.

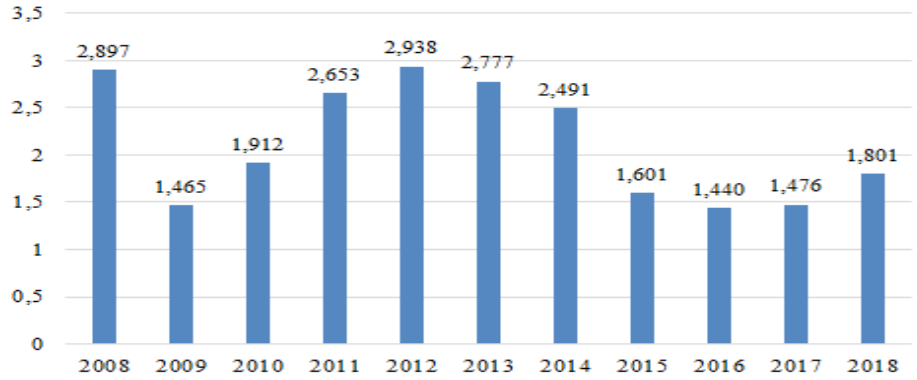

Рисунок 1 – Динамика продаж новых легковых автомобилей в России, млн шт. [4]

По итогам 2018 года продажи увеличились на 22%. Среди факторов, оказавших позитивное влияние на рынок, можно выделить следующие: государственную поддержку, относительную стабилизацию экономической ситуации, отложенный спрос в период с 2016 по 2017 годы. Продажи автомобилей ПАО «АВТОВАЗ» на внутренний рынок увеличились за три года на 35%, вследствие этого выручка от продаж также увеличилась (таблица 1).

Таблица 1 – Динамика объемов продаж автомобилей и выручки ПАО «АВТОВАЗ»

Показатели	2016	2017	2018	Динамика (2018 к 2016)
Продажи автомобилей LADA на внутреннем рынке, шт.	266281	311588	360204	+35,3%
Выручка, млн. руб.	189974	233826	291773	+53,6%

Источник: данные годовых отчетов ПАО «АВТОВАЗ» [5].

В связи с тем, что расходы предприятия превысили доходы, в 2016 и 2017 году предприятие получало чистый убыток. В 2018 году финансовый результат предприятия был нулевым (рис. 2).

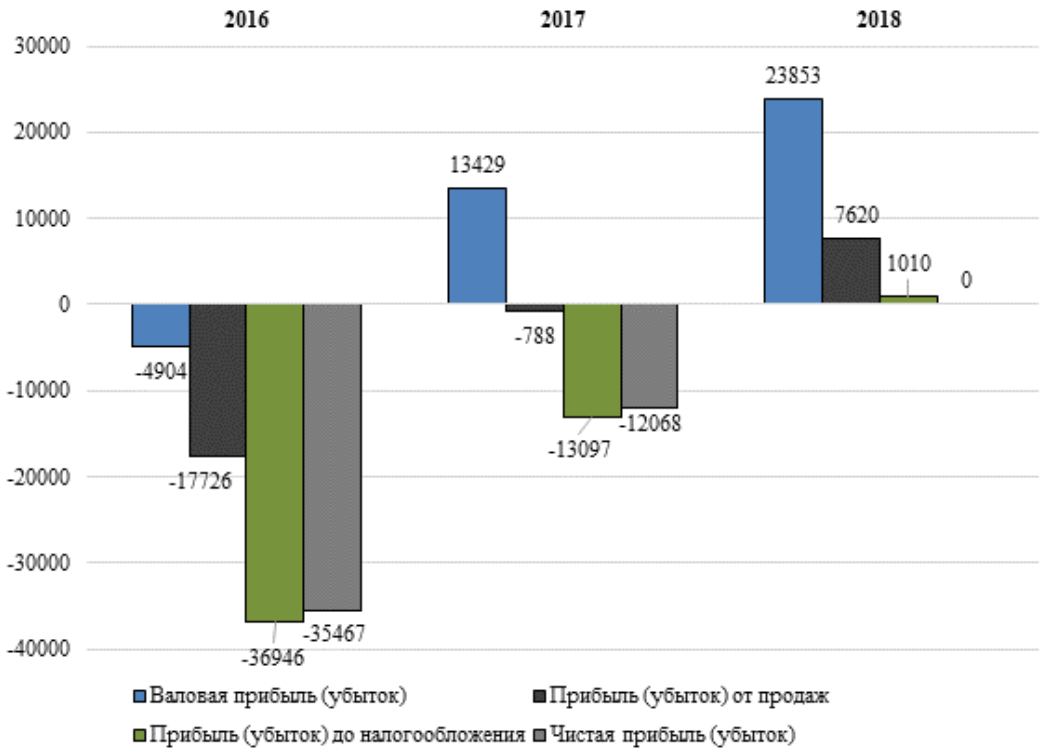

Рисунок 2 – Динамика показателей прибыли ПАО «АВТОВАЗ», млн руб.

Для оценки эффективности финансово-хозяйственной деятельности предприятия используются показатели рентабельности. В табл. 2 представлена динамика показателей рентабельности ПАО «АВТОВАЗ».

Таблица 2 – Динамика показателей рентабельности ПАО «АВТОВАЗ», %

Показатели	2016	2017	2018	Отклонение	
				2017 к 2016	2018 к 2017
Рентабельность продукции	-9,3	-0,3	2,6	9,0	2,9
Рентабельность продаж	-7,9	-0,3	2,4	7,6	2,7
Фондорентабельность	-21,3	-1,0	10,4	20,3	11,4
Рентабельность активов по чистой прибыли	-21,9	-7,9	0,0	14,1	7,9
Рентабельность собственного капитала по чистой прибыли	74,2	20,7	0,0	-53,5	-20,7

Наличие убытков от продаж предопределило отрицательные показатели рентабельности продукции, продаж и фондорентабельности в 2016 и 2017 годы. В 2018 году за счет получения положительного финансового результата по операционной деятельности данные показатели имеют положительные значения.

Получение чистого убытка в 2016 и 2017 годы обусловило отрицательные значения показателей рентабельности активов по чистой прибыли. Положительные значения рентабельности собственного капитала в 2016 и 2017 годы обусловлены отрицательными значениями собственного капитала и чистыми убытками, и не могут положительно характеризовать деятельность предприятия. В 2018 году нулевые значения показателей рентабельности активов и собственного капитала по чистой прибыли обусловлены нулевым финансовым результатом.

Таким образом, результаты анализа свидетельствуют о низкой эффективности деятельности предприятия и обусловливают необходимость разработки мероприятий, направленных на улучшение финансовых результатов предприятия, позволяющих повысить эффективность финансово-хозяйственной деятельности и уровень экономической

безопасности предприятия.

Величина и динамика финансовых результатов ПАО «АВТОВАЗ» обусловлена, в первую очередь, уровнем спроса на российском автомобильном рынке, уровнем активности конкурентов на рынке. Поэтому одно из ключевых направлений в области повышения экономической безопасности данного предприятия – совершенствование инструментов управления прибылью, в частности – совершенствование процессов планирования (бюджетирования) прибыли.

С учетом высокого уровня нестабильности и изменчивости факторов внешней среды предприятия актуальным является реализация процессов планирования прибыли на принципе учета факторов риска.

Процесс планирования прибыли начинается с разработки планов и бюджетов продаж продукции предприятия. Бюджет продаж включает в себя планируемые объемы продаж продукции в разрезе номенклатуры, цены на продукцию, прогнозные объемы выручки. Достижение целевых показателей объемов продаж, выручки, прибыли сопряжено с множеством рисков. Для повышения эффективности процесса планирования прибыли необходимо выявление рисков, влияющих на целевые показатели предприятия, оценка их уровня, обоснование выбора адекватных методов воздействия на риск.

С нашей точки зрения, можно выделить следующие основные виды рисков, влияющих на целевые показатели бюджета продаж ПАО «АВТОВАЗ» (рис. 3).

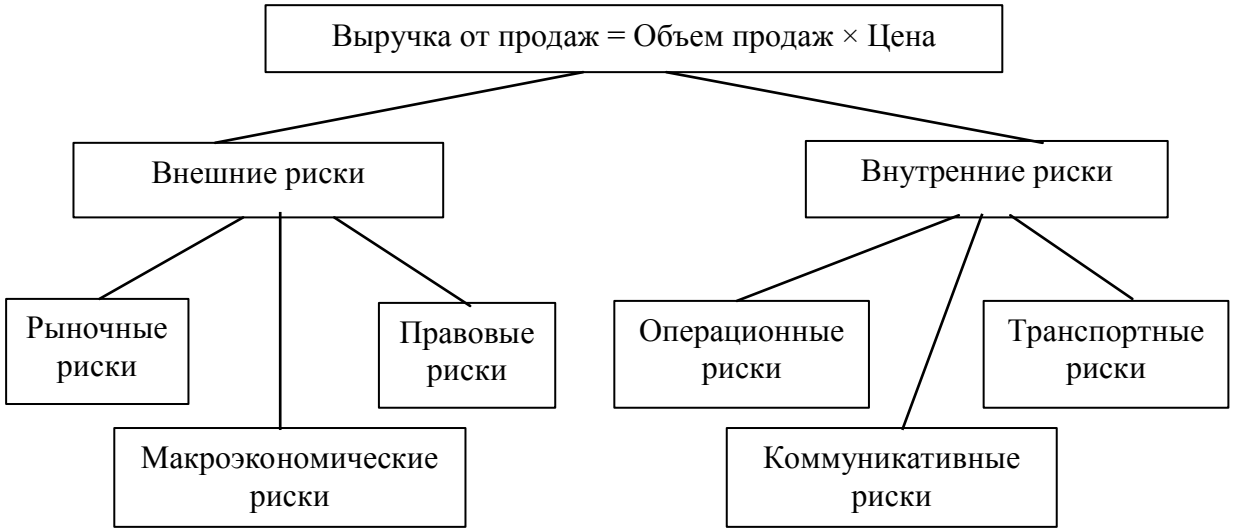

Рисунок 3 – Риски, влияющие на показатели выручки в бюджете продаж ПАО АВТОВАЗ»

Рассмотрим некоторые виды рисков.

Рыночные риски возникают как следствие изменения цен на рынке, активизации действий конкурентов, снижения уровня платежеспособности покупателей. Реализация данных рисков приводит к снижению натуральных объемов продаж, выручки от продаж;

Операционные риски возникают из-за ошибок при совершении бизнес-процессов (сбои в процессе производства, поставок автомобилей) и приводят к неудовлетворенности покупателей, снижению объемов продаж;

Коммуникативные риски возникают вследствие несвоевременности или недостоверности получаемой информации от контрагентов, что также приводит к ухудшению фактических показателей продаж.

Таким образом, реализация принципов управления рисками в процессе бюджетирования позволит адекватно оценить рыночные возможности предприятия, выработать мероприятия по снижению тех или иных видов риска, способствовать достижению целевых показателей выручки и прибыли.

В целом на предприятии должна быть внедрена целостная система риск-менеджмента,

охватывающая все функции управления и бизнес-процессы предприятия.

Другим направлением в рамках совершенствования процессов управления прибылью предприятия является совершенствование процесса формирования прибыли, касающееся вопросов увеличения доходов от продаж и снижения затрат, связанных с производством и реализацией продукции.

Выбор направлений снижения затрат объясняется отраслевой принадлежностью предприятий и, соответственно, особенностями технологических процессов и экономических показателей, характеризующих эти процессы: снижение расхода сырья и энергоресурсов на единицу готовой продукции за счет внедрения более прогрессивных и ресурсосберегающих технологий; снижение транспортных расходов за счет повышения эффективности управления поставками производственных ресурсов; сокращение непроизводительных расходов и т.д.

В настоящее время актуальным для предприятий, в т.ч. для ПАО «АВТОВАЗ», является снижение расходов на потребляемые энергоресурсы.

Многие крупные российские корпорации внедряют современные системы энергоменеджмента, представляющие собой комплекс взаимосвязанных и взаимодействующих организационных мероприятий, технических средств и программно-методического обеспечения, направленных на разработку целей энергетической политики и разработке мероприятий по их достижению.

Проекты по внедрению системы энергетического менеджмента реализуются на основе требований международного стандарта ISO 50001:2011 (ГОСТ Р ИСО 50001-2012) [1].

Так, например, в ПАО «КАМАЗ» в 2012 году была принята «Программа развития энергетического хозяйства ОАО «КАМАЗ» на 2012–2020 годы». Результатом реализации данной программы стало снижение доли затрат энергоресурсов в товарной продукции – с 6% в 2008 году до 5% в 2017 году. В целом экономический эффект от реализации программ ожидается в сумме около 1 млрд руб. ежегодно и снижение доли затрат энергоресурсов в товарной продукции до 4,5% в 2020 году [6].

Эффективность деятельности в области энергосбережения в ПАО «АВТОВАЗ» может быть обеспечена только за счет реализации системного подхода к решению проблем энергосбережения, предусматривающего:

1) формирование системы целей и задач для различных сфер деятельности предприятия в области повышения энергоэффективности;

2) обоснование политики энергосбережения и методов достижения сформированных целей и задач в области энергосбережения;

3) определение потребности в необходимых ресурсах (материальных, трудовых, финансовых) для обеспечения деятельности в области энергосбережения.

Успешная разработка и реализация мероприятий в области энергосбережения и повышения энергоэффективности предполагает наличие соответствующей системы управления, определяющую:

- распределение ответственности и полномочий по управлению деятельностью в области энергосбережения;
- технологию исполнения процессов управления деятельности в области энергосбережения;
- временные регламенты исполнения процессов управления деятельности в области энергосбережения;
- методы и критерии оценки результатов деятельности ПАО «АВТОВАЗ» в области энергосбережения.

Для повышения энергоэффективности в ПАО «АВТОВАЗ» возможны следующие направления:

- локализация производства отдельных видов энергоносителей, таких как оборотная и деминерализованная вода, редуцированный пар;
- переход на более экономичные системы освещения корпусов с использованием

индукционных источников света;

- повсеместное внедрение частотно-регулируемых приводов;

- автоматизация управления энергообеспечением и энергопотреблением, синхронизация работы энергохозяйства и основного производства;

- использование новых материалов и конструктивных элементов при проведении ремонтов зданий, сооружений и тепловых сетей, позволяющих снизить потери тепловой энергии при ее транспортировке.

Реализация мер по энергосбережению позволит сократить затраты предприятия, что положительно скажется на его финансовых результатах и уровне экономической безопасности.

Библиографический список

1. Системы энергетического менеджмента. Требования и руководство по применению [Электронный ресурс]: национальный стандарт Российской Федерации ГОСТ Р ИСО 50001-2012 от 26.10.2012 № 568 – Режим доступа: URL: // http://base.garant.ru/70571304//

2. Ковалев, В.В., Ковалев, В.В. Корпоративные финансы: учебник. – М.: Проспект, 2018. – 638 с.

3. Шеремет, А.Д. Анализ и диагностика финансово-хозяйственной деятельности предприятия: учебник. – 2-е изд., доп. – М.: ИНФРА-М, 2017. – 372 с.

4. Статистика российского авторынка: итоги 2018 года [Электронный ресурс]. – Режим доступа: URL: https://autoreview.ru/news/statistika-rossiyskogo-avtorynka-itogi-2018-goda

5. Официальный сайт ПАО «АВТОВАЗ» [Электронный ресурс] – Режим доступа: URL: // https://lada.ru

6. Официальный сайт ПАО «КАМАЗ» [Электронный ресурс] – Режим доступа: URL: //https://kamaz.ru/

СТАНДАРТИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ФАРМАЦЕВТИЧЕСКОЙ ОРГАНИЗАЦИИ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Назарова А.Р., студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Экономическая безопасность фармацевтической системы это состояние организационных, финансовых, производственных и информационных связей, при котором осуществляется наиболее эффективное использование различных видов ресурсов для предотвращения внутренних и внешних угроз, обеспечение стабильности функционирования и развития фармацевтической системы.

Сегодня экономическая безопасность в аптечном сервисе служит гарантом качества всей жизни населения.

Стандартизация - это деятельность организации по внедрению совокупности стандартов с целью обеспечения соответствия выполняемых услуг и продаваемых товаров удовлетворенности потребителей.

Внедрение в деятельность аптек систем менеджмента качества позволило сегодня без особого труда отслеживать в процессе проводимого внутреннего и внешнего аудита несоответствие требованиям различных нормативов. Такой подход позволяет снизить количество выявленных рекламаций и повысить качество оказываемых услуг.

Любые несоответствия, выявленные в процессе аудита, влекут за собой экономические и финансовые потери, наносят ущерб, и, следовательно, увеличивают риски возникновения

ситуаций, приводящих к нарушению экономической безопасности в малом аптечном бизнесе.

Актуальность темы исследования обоснована тем, что роль систем менеджмента качества (СМК) в аптечном бизнесе постоянно возрастает, поскольку позволяет оценивать качество не только товаров или услуг, но и всей деятельности компании. Аудит позволяет своевременно выявлять различные отклонения и улучшать текущую деятельность.

Определение понятия «фармацевтическая деятельность», сформулировано в законе «Об обращении лекарственных средств» [2]. «Фармацевтическая деятельность – это деятельность, которая включает в себя оптовую и розничную торговлю лекарственными средствами, их изготовление, хранение, перевозку».

В целом, основные положения Закона «Об обращении лекарственных средств» достаточно полно раскрывают особенности взаимодействия участников фармацевтической деятельности. Основными участниками фармацевтической деятельности являются:

- Предприятия фармацевтической промышленности;
- Предприятия, занимающиеся разработкой медицинской техники и изделий медицинского назначения;
- Аптечные организации;
- Ветеринарные аптечные организации.

Аптечная организация – организация или структурное подразделение МО, которая осуществляет розничную торговлю лекарственными средствами, их хранение, перевозку, изготовление для медицинского применения в соответствии с требованиями настоящего Федерального закона.

Аптеку проверяет десяток государственных контролеров, которые за любое нарушение требований законодательства накажут штрафом. Заранее выявить недоработки, улучшить работу аптечного предприятия и подготовиться к внешним проверкам поможет внутренний аудит.

При проведении внутреннего аудита в аптеке основным направлением является производственные процессы. Эти процессы подлежат проверки на соответствие СОП.

СОП - это стандартная операционная процедура, применение которой является обязательным после ввода приказа № 647н (Приказ от 31 августа 2016 г. N 647н об утверждении Правил надлежащей аптечной практики лекарственных препаратов для медицинского применения).

Применение СОП на рабочих местах фармацевтов позволит им действовать строго по шаблону и избежать ошибок.

Целью аудитов является оценка правильности работы в аптечной организации в соответствии с установленными требованиями, а также проверка всех документов. Важно осознавать, что внутренний аудит - это проверка пригодности и результативности системы менеджмента качества (СМК).

При работе с лекарственными препаратами необходимо строго соблюдать санитарно-эпидемиологические нормы аптечной организации (АО). Нарушения этих условий в аптеках могут спровоцировать риск возникновения вредных производственных факторов, которые в конечном итоге могут привезти к профессиональным заболеваниям аптечных работников.

Аптечная организация нередко подвергается внешним проверкам со стороны надзорных органов, которые проводят контрольные закупки, проводят обследований помещений на предмет соответствия требованиям, изучают документы.

Поэтому, внутренний аудит надо готовить и проводить силами своих сотрудников, и в соответствии с разработанными стандартными правилами и процедурами.

Для проведения внутреннего аудита аптечной организации на основе СОП «Порядок проведения внутреннего аудита» рекомендована схема внутреннего аудита СМК (рисунок 1).

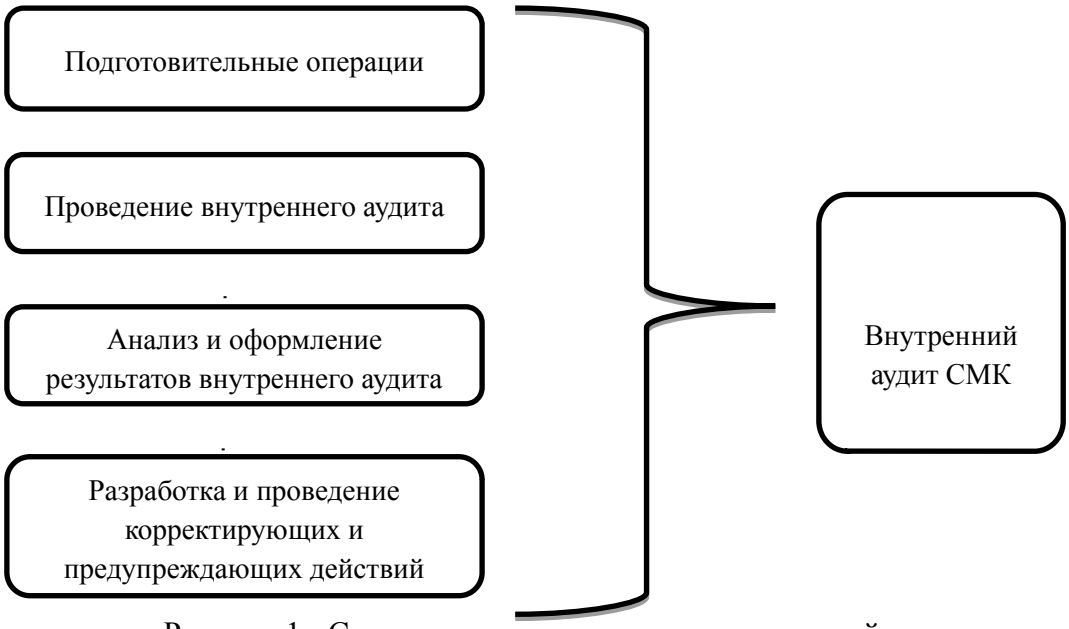

Рисунок 1 - Схема внутреннего аудита для аптечной организации

Целью СОП «Порядок проведения внутреннего аудита» является стандартизация процедуры проведения внутреннего аудита.

Область применения – все производственные помещения аптеки.

Основная часть СОП состоит из 4 частей:

1. Подготовительные операции. Внутренний аудит осуществляется комиссией в соответствии с программой внутреннего аудита, которая утверждается приказом руководителя аптечной организации.

2. Проведение внутреннего аудита. При проведении проверки комиссия заполняет проверочные листы по установленной форме. При проведении комплексной проверки используются несколько форм проверочных листов. Внеплановые проверки проводятся в соответствии с проверочными листами или по отдельным показателям (критериям оценки).

3. Анализ и оформление результатов внутреннего аудита. После проведения аудита составляется отчет с указанием результатов проверки. Информация о результатах аудита доводится до сведения руководителя организации (подразделения) и уполномоченного по качеству.

4. Разработка и проведение корректирующих и предупреждающих действий. При выявлении несоответствий должностные лица проводят работу по устранению нарушений (коррекция). Контроль за выполнением порядка проведения внутреннего аудита возлагается на уполномоченного по качеству (или руководителя).

Таким образом, можно сделать следующие выводы:

а) стандартизация как вид деятельности активизирует сотрудников аптеки на изучение стандартов, регламентирующих действия коллектива;

б) экономическая безопасность для сферы аптечной деятельности позволяет гарантированно оставаться конкурентоспособными, так как позволяет получать прибыль по факту качественного труда;

в) проведение систематических аудитов позволяет своевременно выявить возможность появления ситуации нарушения экономической безопасности;

г) постоянное изучение сотрудниками организации требований стандартов дисциплинирует их деятельность и повышает требования к качеству по всем бизнес-процессам.

Библиографический список

1. Приказ Минздрава от 31.08.2016 № 647н «Об утверждении Правил надлежащей аптечной практики ЛП для медицинского применения».

2. Федеральный закон "Об обращении лекарственных средств" от 12.04.2010 N 61-ФЗ.
3. ГОСТ Р ISO 9001-2015. Система менеджмента качества. Требования. М.: Стандарты и качество. 2016. - 34 с.
4. Кузнецов, Д.А., Коржавых, Э.А. Экономическая безопасность фармацевтических организаций. Словарь терминов и определений. Москва, 2013. 197 с.
5. СОП «Порядок проведения внутреннего аудита аптечной организации ООО «Формула здоровья».

БУХГАЛТЕРСКАЯ ЭКСПЕРТИЗА В СИСТЕМЕ ЭКСПЕРТНЫХ ИССЛЕДОВАНИЙ

Пудовкина С.А., студент
Научный руководитель: Голикова О.В., к. э. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Под экспертизой в правовой литературе принято понимать процессуальное действие, состоящее из проведения исследования с предоставлением мотивированного заключения экспертом по вопросам, для ответа на которые требуются специальные знания в области науки, техники, искусства, ремесла и которые поставлены перед экспертом, органами дознания, следователем, судом, прокуратурой.

Среди множества судебных экспертиз можно выделить группу судебно-экономических экспертиз. Без качественно проведенной бухгалтерской экспертизы невозможно применение соответствующих статей уголовного кодекса, законодательства, регулирующего экономическую деятельность хозяйствующих субъектов.

На этапе современного развития многих государств рыночные модели хозяйствования характеризуются широким спектром преступности в сфере экономики, что приводит к масштабной криминализации экономических отношений и угрозе национальной экономической безопасности. В целях эффективного противодействия экономической преступности в настоящее время целесообразно активное развитие института использования специальных экономических познаний в судопроизводстве, где основной процессуальной формой их применения является судебная экономическая экспертиза. Использование специальных экономических знаний в процессе выявления и расследования преступлений данной категории играет важную роль в установлении признаков объективной стороны экономических преступлений.

Экспертная деятельность представляет собой особенную категорию экспертных исследований в процессе реализации которых используются теоретические знания и практический опыт в области не только дисциплин экономического профиля, но и смежных с экономикой направлений, таких так финансовое право, гражданское право, уголовное право, финансовое право, налоговое право, ценообразование, денежное обращение, аудит и другие.

Использование специальных знаний экспертов позволяет чётко и точно установить и дать оценку искажений экономической информации, вывить образовавшиеся, в следствии этого, отрицательные моменты и определить их влияние на экономические результаты деятельности организации и, соответственно, обозначить степень угрозы экономической безопасности предприятия.

В процессе эволюции экспертная деятельность прошла все без исключения периоды формирования и развития. Среди них акцентируют внимание на: финансово-экономической, финансово-кредитной и бухгалтерской экспертной деятельности.

Таким образом, судебно-бухгалтерская экспертная деятельность является одной из разновидностей экономических экспертиз.

В ходе работы эксперт-бухгалтер анализирует объекты, которые представлены в таблице 1.

В процессе осуществления экспертной деятельности находят решение определённые задачи, продемонстрированные в таблице 2.

Таблица 1 - Объекты исследования экспертизы

Объекты исследований	
Общие	- первичные сводные бухгалтерские документы; - материалы инвентаризаций; - результаты бухгалтерского оформления (бухгалтерские проводки, накопительные ведомости), записи в регистрах аналитического и синтетического учётов; - документы и записи оперативного и «неофициального учётов
Специфические	- акты документальной ревизии; - заключения экспертов в других областях; - протоколы изъятия документов и постановлений о приобщении их к делу; - протоколы иных процессуальных действий (допросов, очных ставок, обысков и выемок)

Таблица 2 - Задачи экспертной деятельности

№ п/п	Задачи
1	Установление нарушений в процессе документальной фиксации сведений о финансовых операциях, в процессе организации, распределения и использования доходов, денежных средств
2	Установление искажений в налоговом и бухгалтерском учёте и анализ их воздействия на размер налогооблагаемой базы
3	Выявление фактов отклонений, нарушений в финансово-кредитной сфере
4	Определение кредитоспособности заемщика, т.е. его способность своевременно и в полном объёме осуществить возврат заёмных средств
5	Определение направлений расходования целевых средств
6	Установление налогооблагаемой базы, исчисление и уплата налогов и иных обязательных взносов и платежей в бюджеты различных уровней и внебюджетные фонды
7	Выявление соответствия между налогооблагаемой базой, суммой налоговых отчислений и между нормами отечественного законодательства
8	Расчёт доли учредителей (акционеров) в имуществе хозяйствующего субъекта, определение суммы денежных средств, которые причитаются участнику общества в случае его выходы его из состава, а также размера дивидендов акционерам по результатам финансового года
9	Иные ситуации, разрешение которых требует участие специалиста в области экономических наук

С помощью набора аналитических процедур по существу эксперт исследует информационные и документальные «следы» преступлений экономической направленности.

Экспертные процедуры и их результаты представлены в таблице 3.

Таким образом, выявленная в процессе осуществления экспертной деятельности «скрытая» информация, используется правоохранительными органами с целью установления соответствующей версии, корректировки хода расследования и осуществления следственных мероприятий.

Таблица 3 - Экспертные процедуры и их результаты

Процедура	Результат
Проверка и установление факта и размера недостачи или излишков товарно-материальных ценностей, денежных средств, а также времени и места возникновения недостачи.	Можно определить и материально-ответственное лицо за ценности на данном предприятии, что имеет большое значение для правильного разрешения условного или гражданского дела.

Процедура	Результат
Проверка и определение размера материального ущерба, причиненного должностными и иными лицами в результате совершенных нарушений и злоупотреблений.	Можно определить размер материального ущерба, его характер, организацию ил лица, которыми он причинен путем исследования определенных хозяйственных операций.
Проверка документальной особенности списания сырья, материалов, готовой продукции и товаров.	Может быть выявлено списание на производство сырья и материалов, в действительности похищенных со складов путем исследований технологии и операций производства (хранения, реализации), в случае отпуска готовой продукции не по назначению, указанному в документах поставщика, анализа документов у получателя.
Проверка случаев нарушения финансовой дисциплины, по существу которых эксперт может дать заключение.	Может быть определен перерасход фонда заработной платы и сметных ассигнований, неправильное использование банковских ссуд, неправильное исчисление налогов, нарушение кассовой дисциплины и т.п.
Проверка и определение факта совершения хозяйственной операции, не получившей должного отражения в данных бухгалтерского учета.	Может быть установлен отпуск со склада товарно-материальных ценностей в большем количестве, чем указано в накладной.
Определение и анализ недостатков в системе бухгалтерского учета и отчетности.	Можно определить действительные размеры недостач, с одной стороны, и состояния бухгалтерского учета – с другой.

Библиографический список

1. Ашмарина, Е.М. [и др.] Правовое обеспечение контроля, учета, аудита и судебно-экономической экспертизы [Текст]: учебник для академического бакалавриата; под ред. Е.М. Ашмариной; отв. ред. В.В. Ершов. - М.: Издательство Юрайт, 2018. - 289 с.

2. Петренко, А.В. Система предупреждения экономических преступлений органами внутренних дел: Дис. … канд. юрид. наук / А.В. Петренко. М., 2011. 218 с.

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ДЕЯТЕЛЬНОСТИ УЭБИПК МВД РОССИИ ПО САМАРСКОЙ ОБЛАСТИ

Труфанова Н.Ю., студент
Научный руководитель: Голиков О.И., к. э. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Стратегическими целями обеспечения национальной безопасности Российской Федерации являются экономическое развитие, обеспечение экономической безопасности и противостояние влиянию коррупционных угроз.

Стратегия государственной безопасности РФ определяет национальные приоритеты, к которым относится государственная и общественная безопасность, реализуемая методами выявления, предупреждения и пресечения экономических преступлений. Соответственно, противодействие коррупции и обеспечение государственной безопасности являются актуальным и приоритетным направлением деятельности правоохранительных органов, которые должны решать задачи по выявлению, предупреждению и устранению угроз,

связанных с экономической и коррупционной преступностью, в свете современных тенденций экономической и геополитической ситуации.

Однако формирование, осуществление, нормативно-правовое регулирование государственной политики как одно из направлений деятельности правоохранительных органов в данных сферах в нормативных правовых документах не конкретизированы и вызывают проблему выполнения не свойственных МВД России функций.

Так, базой для развития и осуществления государственной политики в области обеспечение государственной безопасности на всех уровнях управления (государственном и муниципальном) является Стратегия экономической безопасности Российской Федерации на период до 2030 г., в реализации которой МВД РФ принимает участие, в том числе в лице Главного управления и территориальных подразделений экономической безопасности и противодействия коррупции территориальных органов МВД РФ.

Исходя из того что безопасность и защита национальных интересов в экономической области являются приоритетными направлениями политики государства, то приоритетное значение придается:

– разработке и формированию действенного механизма контроля за соблюдением национального законодательства и усилению государственного регулирования в экономической сфере, её нормативно-правовому регламентированию, а также принятию эффективных мер по преодолению результатов кризисов и др.;

– совершенствованию и поддержанию отлаженного механизма функционирования и сотрудничества всех ступеней государственной власти, строгой вертикали исполнительной власти и единства судебной концепции Российской Федерации и, установлению точного многофункционального распределения обязанностей между государственными органами;

– противодействию коррупционной преступности и легализации преступных доходов, в первую очередь профилактическими средствами, путём реализации уголовной политики по направлениям – создание действенной системы правоохранительного контроля, совершенствование мер административного, гражданского и уголовно-правового воздействия.

Таким образом, в Российской Федерации разработана сложная национальная концепция профилактики преступлений в сфере экономики.

На основании п. 1. ч. 1 ст. 5 Закона N 182-ФЗ «Об основах системы профилактики преступлений в Российской Федерации» МВД РФ относится к числу субъектов профилактики правонарушений. МВД РФ является главным органом, реализующим исполнительно-распорядительные полномочия, осуществляющим противодействие экономической преступности в государстве. ГУ ЭБиПК реализует концептуальные положения уголовной политики и осуществляет правовое регулирование в сфере обеспечение государственной безопасности государства, в том числе и противодействия коррупции.

Полномочия сотрудников подразделений ЭБиПК по предупреждению преступлений закреплены в Приказе МВД России от 17 января 2006 г. N 19 «О деятельности органов внутренних дел по предупреждению преступлений».

Практика проводимых правоохранительными органами мероприятий по профилактике экономических и коррупционных преступлений демонстрирует незаинтересованность работников в работе, нацеленной преимущественно на использование профилактических процедур.

Целесообразно заметить, что ведомственный подход к определению и содержанию профилактической работы подразделений ГУ ЭБиПК отсутствует. Ведомственные нормативные акты нечётко регламентируют профилактическое направление, в них не обозначены цели и проблемы, способы и ресурсы профилактической деятельности, сущность и состав «профилактического мероприятия», разновидности виды профилактических мероприятий. Указанные недостатки обусловлены следующим:

во-первых, в доктрине криминологии не сформировалось единого представления о системе профилактики, осуществляемой правоохранительными органами в рассматриваемой сфере, особенно с помощью оперативно-розыскных сил и средств;

во-вторых, представление о роли и содержании профилактики преступлений в сфере экономики в уголовной политике, ведомственных задачах длительное время упрощалось и предусматривало лишь перечень типовых превентивных методов без учета специфики отдельных отраслей хозяйствования, их субъектов, современных векторов развития общества и государства, что в целом не обеспечивало эффективность уголовно-превентивных и организационных мер воздействия на детерминанты экономической преступности.

Повышению эффективности деятельности УЭБиПК МВД России будет способствовать нормативное закрепление участия правоохранительных органов в выработке и реализации государственной политики в области обеспечения государственной безопасности и противодействия коррупции в части их профилактической работы.

Для реализации этой целесообразно выполнение мероприятий, приведённых на рисунке 1.

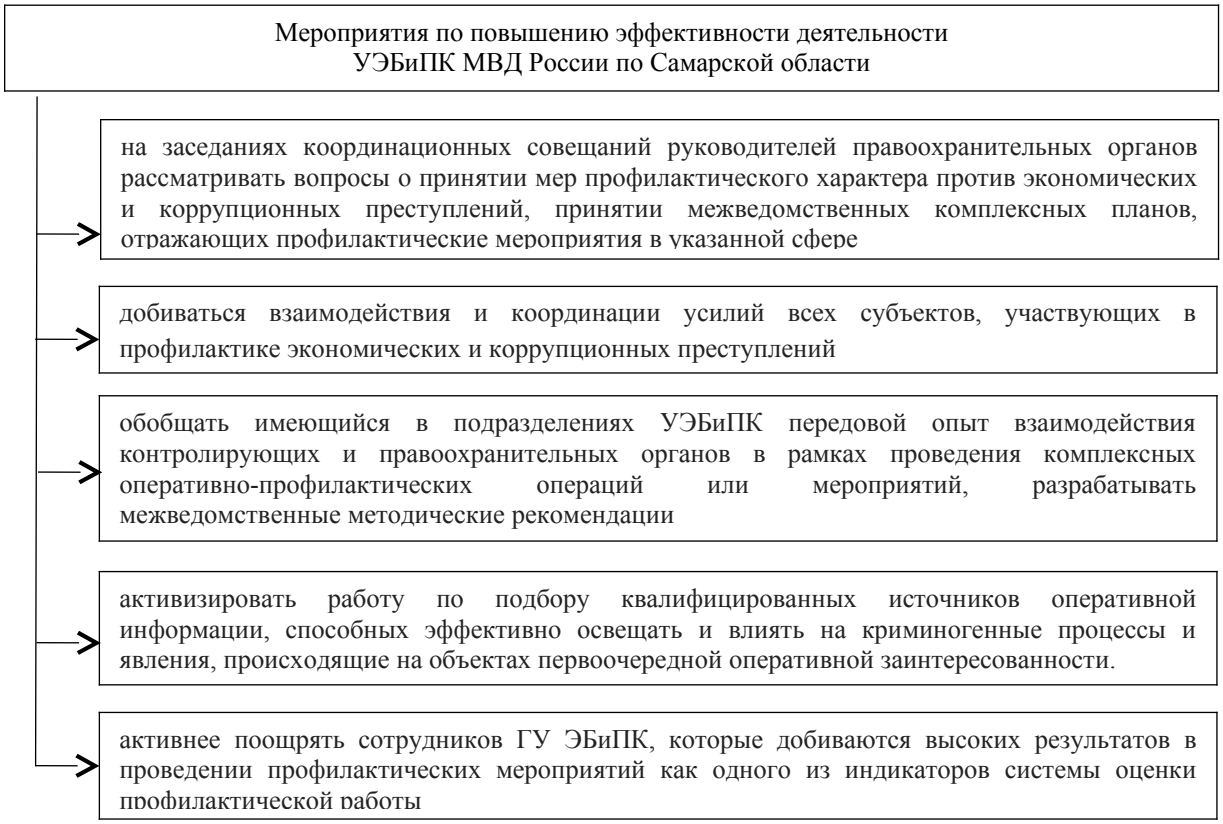

Рисунок 1 - Мероприятия по повышению эффективности деятельности УЭБиПК МВД России по Самарской области

Исходя из того, что в работе сотрудников УЭБиПК МВД России по Самарской области имеются существенные недостатки в части профилактики преступлений в экономической сфере, результативность такой деятельности не может быть оценена, поскольку отсутствуют соответствующие методики, которые позволяют установить соответствие мер по борьбе с профилактическими мерами в сфере экономики, оценить их эффективность.

В показатели оценки деятельности личного состава подразделений УЭБиПК МВД России по Самарской области необходимо включить критерии, которые представлены на рисунке 2.

Таким образом, для реализации указанного направления необходима согласованная, научно обоснованная ведомственная правовая основа, создание которой должно основываться прежде всего на базисной норме, являющейся фундаментом реализации профилактического направления по линии ГУ ЭБиПК МВД России.

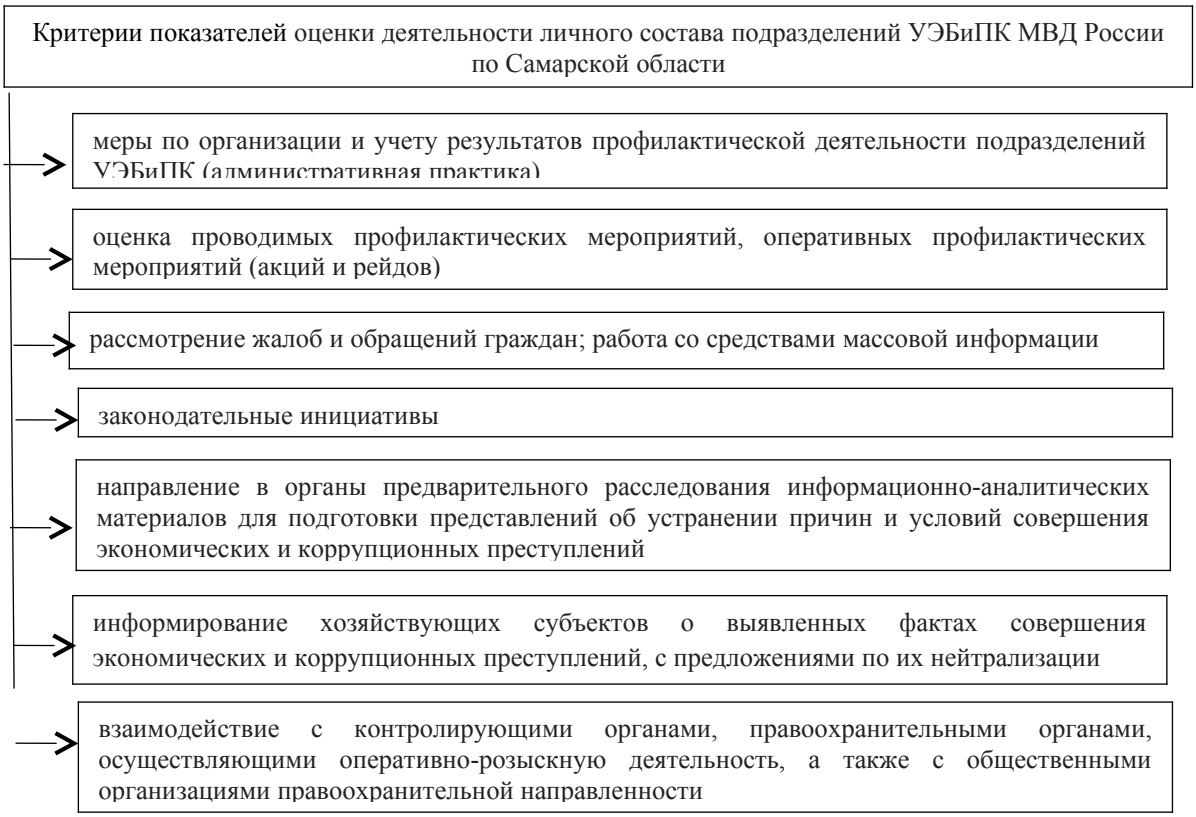

Рисунок 2 - Критерии показателей оценки деятельности личного состава подразделений УЭБиПК МВД России по Самарской области

Библиографический список

1. Российская Федерация. Приказы. О деятельности органов внутренних дел по предупреждению преступлений [Текст] Приказ МВД России N 19 от 17.01.2006 (ред. от 28.11.2017).

2. Российская Федерация. Федеральные законы. Об основах системы профилактики правонарушений в Российской Федерации [Текст] Федеральный закон N 182-ФЗ от 23.06.2016 // Собрание законодательства РФ, 27.06.2016, N 26 (Часть I), ст. 3851.

3. Борин, Б.В. Понятие оперативно-розыскной профилактики преступлений / Б.В. Борин, Я.Г. Ищук // Пробелы в российском законодательстве. 2017. N 3. С. 381 – 386.

4. Мусеибов, А.Г. Правовые и организационные основы разработки и реализации программ профилактики правонарушений / А.Г. Мусеибов, А.В. Борбат // Российский следователь. 2017. N 24. С. 52 – 56.

5. Шегабудинов, Р.Ш. Основные формы профилактики преступлений экономической и налоговой направленности / Р.Ш. Шегабудинов // Вестник Московского университета МВД России. 2010. N 8. С. 190 – 194.

6. Портал правовой статистики Генеральной прокуратуры РФ. [Электронный ресурс] – Режим доступа: www.crimestat.ru

7. Официальный сайт МВД РФ. [Электронный ресурс] – Режим доступа: www .мвд.рф

8. Федеральная служба государственной статистики. [Электронный ресурс] – Режим доступа: www.gks.ru

9. Официальный сайт Прокуратуры Самарской области. [Электронный ресурс] – Режим доступа: www.samproc.ru

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Устинова Я.А., студент
Научный руководитель: Шехтман А.Ю., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Экономическая безопасность предприятия, является важнейшей категорией деятельности любого хозяйствующего субъекта, так как многие организации в настоящее время, вынуждены функционировать в ситуации неопределенности, непредсказуемости, резкого изменения, как внутренних условий хозяйствования, так и внешних (политических, макроэкономических, экологических, правовых и др.).

Вместе с тем, предприятия принимают рисковые решения в условиях жесткой конкуренции, добиваясь предотвращения, ослабления или защиты от существующих или прогнозируемых опасностей и угроз, обеспечивая достижение целей бизнеса.

В этих условиях обеспечение экономической, в том числе финансовой, безопасности является приоритетной задачей предприятия любой организационно-правовой формы.

Цель данной научной статьи, заключается во всестороннем раскрытии сущности и структуры экономической безопасности предприятия.

Экономическая безопасность предприятия, это степень защищенности жизненно важных и законных интересов предприятия от внутренних и внешних угроз, проявляющихся в разных противоправных формах. При этом защищенность обеспечивает стабильное развитие предприятия в соответствии с его статусными целями.

Актуальность деятельности по обеспечению экономической безопасности предприятия заключается в предотвращение угроз и убытков от негативного влияния внешней среды на хозяйственную деятельность.

Принятие эффективных решений в области обеспечения экономической безопасности предприятия предполагает проведение оценки уровня его финансовой безопасности, позволяющей выявить угрозы безопасности с целью их снижения.

В экономической литературе [1-4], выделяются различные подходы к диагностике уровня финансовой безопасности предприятия. Большинство авторов для целей диагностики предлагают оценку финансовой безопасности на базе системы показателей финансового состояния предприятия.

Результаты анализа финансового состояния позволяют выявить причины финансовых затруднений предприятия, определить возможности улучшения использования финансовых ресурсов, ускорения оборачиваемости капитала, укрепления финансового положения предприятия и повышения уровня его финансовой безопасности.

Устойчивое финансовое состояние предприятия является основным индикатором эффективности деятельности предприятия, важнейшим критерием его деловой активности и надежности для контрагентов. Поэтому результаты анализа финансового состояния предприятия представляет значительный интерес не только для руководства предприятия, но и многих других лиц, заинтересованных в деятельности предприятия – собственников, инвесторов, поставщиков, покупателей, работников и т.д.

В частности, собственников (акционеров) интересует прибыльность предприятия, темпы экономического развития в будущем и связанные с ними выплаты дивидендов.

Инвесторов результаты анализа финансового состояния предприятия интересует с позиций наиболее выгодного вложения капитала и снижения риска потери инвестиций.

Поставщиков материальных ресурсов результаты анализа финансового состояния

предприятия интересует с позиций обеспечения своевременной оплаты поставок.

Обеспечение устойчивого финансового состояния предприятия предполагает принятие и реализацию рациональных управленческих решений в области формирования, распределения и использования финансовых ресурсов предприятия, содействующих обеспечению требуемого уровня экономической безопасности предприятия.

Экономическая безопасность является системной категорией, построенной на принципах устойчивости, саморегуляции, целостности и призвана защищать каждую составляющую охраняемой системы, т. к. разрушительное воздействие на любую из этих составляющих приведет к гибели системы в целом.

Поэтому в целях самозащиты предприятия от внешних и внутренних угроз, бизнес обязан уделять основное внимание экономической безопасности.

Экономическая безопасность предприятия рассматривается как широкое понятие, включающее финансовую, интеллектуальную, кадровую, правовую, техническую, экологическую компоненты безопасности [2, 3].

Главной целью экономической безопасности предприятия является обеспечение его устойчивого и максимально эффективного функционирования в настоящее время и обеспечение высокого потенциала развития роста предприятия в будущем.

Для достижения цели, поставленной в ходе проведения исследования, необходимо представить примерную структуру функциональных составляющих экономической безопасности предприятия (рис. 1).

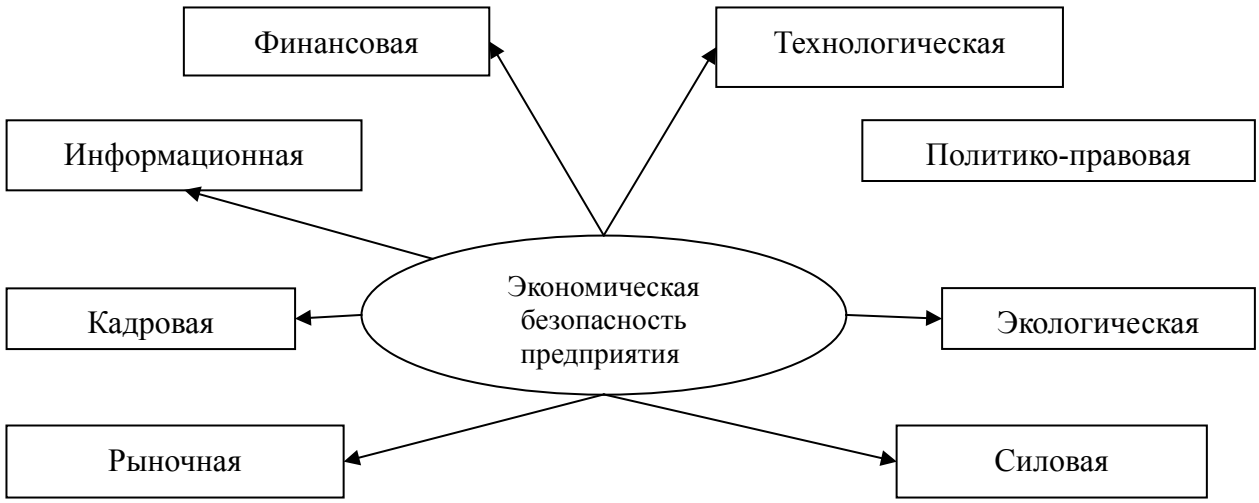

Рисунок 1 – Основные функциональные составляющие экономической безопасности предприятия

По данным рисунка 1, можно сделать вывод, что каждая из представленных функциональных составляющих экономической безопасности предприятия характеризуется собственным содержанием, набором функциональных критериев и способами обеспечения.

Важно отметить, в рамках настоящего исследования, обеспечение экономической безопасности предприятия обусловливается способностью органов управления предприятием на соответствующих уровнях:

- обеспечить устойчивое экономическое развитие предприятия, достижение основных целевых параметров деятельности при сохранении платежеспособности предприятия, необходимого уровня финансовой независимости при существующем уровне финансовых рисков;

- нейтрализовать негативное воздействие последствий кризисных явлений в экономике, действий конкурентов;

- предотвратить сделки с активами предприятия, создающие угрозу утраты контроля над предприятием;

- сформировать эффективную систему анализа и контроля состояния, структуры и движения финансовых ресурсов предприятия [1, 4].

Таким образом, экономическая безопасность представляет собой способность предприятия противостоять существующим и возникающим угрозам и рискам, ухудшающим его финансовое состояние, или приводящие предприятие к банкротству, обеспечивая достижение стратегических и текущих целей.

Для оценки экономической безопасности предприятия большинство авторов предлагают систему показателей, характеризующих финансовой состояние предприятия, в числе важнейших из которых являются показатели платежеспособности.

Регулярность проведения оценки повышает эффективность управления финансовой безопасностью, способствует сокращению финансовых потерь предприятия вследствие влияния неблагоприятных факторов внешней и внутренней среды и укреплению финансовой устойчивости предприятия.

Библиографический список

1. Бланк, И.А. Управление финансовой безопасностью предприятия. – 3-е изд., стер. – К.: Эльга, 2016. – 776 с.

2. Иванова, Л.К. Экономическая безопасность предприятия // Вестник Уфимского государственного авиационного технического университета. – 2013. – Т. 17. № 7 (60). – С. 30-33.

3. Кашин, А.В. Экономическая безопасность предприятий управленческие проблемы // Экономические науки. – 2017. – № 1. – С. 22-28.

4. Яндулова, И.Г. Управление финансовой безопасностью предприятия // Современные тенденции в экономике и управлении: новый взгляд. - 2016. - № 14 (2). - С. 161-166.

ТРАНСФОРМАЦИЯ СТРАТЕГИЧЕСКОГО ПРИОРИТЕТА В ТАКТИЧЕСКИЙ КАК ОСНОВА УКРЕПЛЕНИЯ БЕЗОПАСНОСТИ СТРАНЫ

Устинова Я.А., студент
Научный руководитель: Щукина А.Я., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Суверенитет страны, в первую очередь, зависит от уровня национальной безопасности, которая на прямую связана с экономической, а их взаимосвязь обеспечивается трансформацией стратегических приоритетов в тактические (отраслевые).

Проследим развитие этих процессов на примере реализации атомного проекта, который позволил создать новый технологический облик страны – сверхдержавы

Работа в направлении атомных исследований активно ведется в Курчатовском институте. Его история началась 12 апреля 1943 года, когда для разработки советского ядерного оружия была создана под руководством выдающегося ученого-атомщика Игоря Курчатова лаборатория №2 Академии наук СССР, которая затем стала лабораторией измерительных приборов АН СССР, институтом атомной энергии АН СССР имени Курчатова и российским научным центром "Курчатовский институт". В 2010 году институт получил статус национального исследовательского центра.

Лаборатория №2 осуществляла научное руководство разработкой первых советских атомной и водородной бомб. С 1943 по 1945 год лаборатория, ставшая научным "ядром" советского атомного проекта, с привлечением ряда научных институтов и предприятий страны провела исследования по разделению изотопов урана, разработала технологии получения металлического урана, тяжелой воды и многое другое. В 1944 году в лаборатории был построен и введен в действие циклотрон, позволивший наработать индикаторные количества плутония- "взрывчатки" для первого советского атомного заряда. В 1946 году в

институте был пущен первый в Евразии атомный реактор.

В 1950-е годы начались исследования и разработки по мирному исследованию атомной и термоядерной энергии. С участием института была построена и пущена первая в мире промышленная атомная электростанция - Обнинская АЭС. В институте были разработаны атомные реакторы для ледоколов (1957), подводных лодок (1958) и космической техники.

Важным направлением работ в Курчатовском институте с середины 1950-х годов стал управляемый термоядерный синтез - переход к новым принципам овладения энергией, процессами, происходящими на Солнце и других звездах, где термоядерные реакции протекают при температуре около 20 миллионов градусов. Там происходит слияние ядер изотопов водорода- дейтерия и трития, в результате чего выделяется огромное количество энергии. В 1985 году в институте была построена первая в мире экспериментальная термоядерная установка с «ловушкой» из магнитного поля, которая получила название «токамак».

С середины 1960-х годов осуществляет научное обеспечение эксплуатации действующих атомных реакторов, утилизации выведенных из эксплуатации установок и научное руководство разработкой реакторов и ядерных энергетических установок новых поколений.

Курчатовский институт всегда был главной научной организацией СССР и России в атомной сфере. По существу, из первого советского реактора Ф-1 вышли реакторы разных типов – промышленные, энергетические, исследовательские и транспортные, которые используются на подводных лодках и атомных ледоколах, ядерные энергетические установки для космоса. Институт является непосредственным участником проектов госкорпорации «Росатом» по строительству АЭС, будучи научным руководителем проектов энергетических реакторов типа ВВЭР.

Одно из основных направлений работы института – обеспечение безопасности атомной энергетики. Разработанные здесь новые системы безопасности – так называемые ловушки расплава – уже входят в состав оборудования АЭС, они были впервые установлены на Тяньваньской АЭС в Китае и АЭС «Куданкулум» в Индии. В случае тяжелой аварии расплавленное ядерное топливо будет удержано в таких ловушках, что не даст радиоактивным веществам выйти за пределы реакторной установки.

Институт занимается и продлением сроков эксплуатации энергоблоков АЭС.

Благодаря разработанной «курчатовцами» системе так называемого отжига корпусов реакторов удается почти полностью восстанавливать их эксплуатационные характеристики. Также с участием ученых института разработана новая марка стали, которая приобретает особые свойства, что позволит продлить срок работы корпусов реакторов до сотни лет.

Особое место в послужном списке Курчатовского института занимают разработки для освоения Арктики. Во многом благодаря им у России имеется единственный в мире атомный ледокольный флот.

Также с 1970 годов в институте работают над проектами атомных энергоблоков малой мощности, действующих по принципу прямого преобразования энергии - они помогли бы снабжать энергией небольшие поселки и российские военные базы в арктическом регионе. Такие установки не требует постоянного обслуживания на протяжении многих лет, их можно изготавливать серийно и устанавливать практически в любом месте.

Курчатовский институт занят и экологической работой по очистке Арктики. Под его научным руководством в Сайде-губе (Мурманской области) в рамках международного проекта был создан не имеющий аналогов комплекс по переработке, кондиционированию и долговременному хранению радиоактивных отходов, образовавшихся в результате утилизации атомных подводных лодок. Этот комплекс, как считают специалисты, гарантирует безопасное, экологически чистое развитие ядерных технологий в Арктике.

По мере развития Курчатовского института его технологические направления разнообразились. Так, в конце 1960-х - начале 1970 годов были получены результаты мирового значения в области микроэлектронной технологии: ионная имплантация,

сверхвысокочистые вещества, литография, плазменная химия, тонкие пленки. Такой технологический задел позволил позднее развить в институте работы в области нанотехнологий, создания гибридных систем и суперкомпьютеров.

С конца 1960-х годов Курчатовский институт стал научным руководителем проблемы использования сверхпроводимости в атомной науки и техники. С начала 1970-х годов институт участвовал в разработке новых технологий микроэлектроники. А в 1980-е годы благодаря активному развитию информационных технологий в институте были заложены основы отечественного интернета (Рунета).

В 1999 году в институте был введен в эксплуатацию первый на постсоветском пространстве специализированный источник синхротронного излучения - уникальный комплекс, необходимый для изучения материи на атомарном уровне. С середины 2000-х годов в Курчатовском институте началось активное развитие нанотехнологий.

В 2009 году был создан первый в мире центр конвергентных наук и технологий - Курчатовский комплекс на био - информационных, когнитивных и социогуманитарных технологий (НБИКС-технологий), ориентированный на междисциплинарные исследования и разработки. НБИКС- технологии стали вторым важнейшим магистральным направлением научного развития Курчатовского института в последние годы.

Как считают специалисты, создание принципиально новых технологий и систем, воспроизводящих принципы живой природы, позволит человечеству перейти на новые, гораздо более экономичные и безопасные принципы производства и потребления энергии.

Курчатовский институт в последние годы стал флагманом научного сотрудничества российских ученых с иностранными коллегами. Центр представляет Россию во всех международных исследовательских крупных научных проектах. Например, проект строительства международного термоядерного экспериментального реактора (ITER), Европейский рентгеновский лазер на свободных электронах (XFEL), Большой адронный коллайдер, Европейский центр синхронного излучения (ESRF), Европейский центр по исследованию ионов и антипротонов (FAIR).

Проект европейских рентгеновских лазеров на свободных электронах по созданию самого мощного в мире рентгеновского лазера стал наиболее ярким примером крупного проекта, в создании которого большой вклад внесла Россия (Курчатовский институт курирует ее научное участие в проекте).

Эксплуатация лазера началась в сентябре 2017 года. На этом проекте будут получены исключительно яркие и сверхкороткие импульсы рентгеновского излучения, что даст ученым новое понимание строения атома, а также процессов, происходящих в наномире. С помощью него ученые в реальном времени смогут изучать структуру биологических молекул и различных веществ, следить за сверхбыстрыми химическими процессами. Это даст возможность лучше понять природу вещества и научиться конструировать принципиально новые материалы с заданными свойствами.

Одним из направлений деятельности Госкорпорации "Росатом" является развитие ядерной медицины (медицинской диагностики и лучевой терапии, применяемые при лечении онкологических заболеваний). В сотрудничестве с Федеральным медико-биологическим агентством России и ведущими производителями в отечественной отрасли началось воссоздание всего производственного медицинского комплекса, от изотопов для оказания медицинской помощи на отечественном оборудовании.

Рассмотрим далее трансформацию стратегических приоритетов в тактические на примере космических проектов.

Создание новых технологий и устройств для изучения космоса - одно из направлений работ, ведущихся в российской атомной отрасли. Предприятия госкорпорации «Росатом» здесь работают в разных областях – от создания новой техники для наземной ракетно-космической инфраструктуры до изготовления устройств, помогающих изучать свойства планет.

Сейчас при участии Росатома в России создается транспортно-энергетический модуль

на основе ядерной энергодвигательной установки мегаваттного класса. Этот проект выполняется совместно предприятиями Росатома и Роскосмоса в соответствии с решением, принятым в 2009 году президентской комиссией по модернизации.

Не имеющий аналогов транспортный модуль позволит создать качественно новую технику высокой энерговооруженности для изучения и освоения дальнего космоса. Новый проект предполагает использование ионных электрореактивных двигателей, в которых реактивная тяга создается за счет ускоренного электрическим полем потока ионов.

Такие установки позволят в будущем приступить к реализации многих амбициозных задач.

В их числе – полет на Марс, детальные исследования планет и их спутников, промышленное производство в космосе. Также можно будет заниматься очисткой околоземного космического пространства от космического мусора, бороться с астероидной опасностью, создавать на планетах автоматизированные базы.

Ключевой вопрос создание реакторной установки для работы в космосе – обеспечение требований ядерной и радиационной безопасности. Они учтены при разработке конструкции нынешней реакторной установки.

Созданные в ходе реализации космического проекта новые технологии пригодятся и в разных отраслях народного хозяйства – могут быть созданы ядерные энергоустановки малой мощности, например, для тепло- и электроснабжения удаленных районов Арктики.

Разработка Специализированного научно-исследовательского института приборостроения (СНИИП, входит в машиностроительный дивизион Росатома холдинг «Атомэнергомаш») помогла ученым оценить риск воздействия космической радиации на космонавтов в условиях длительных полетов.

Для того, чтобы узнать, какую дозу радиации получает космонавт в космосе и получить наиболее точные данные для оценки радиационной нагрузки в условиях длительных полетов, был проведен эксперимент под названием «Матрешка-Р».

Фантом в виде шара был создан специалистами СНИИП. Состав его материала напоминал химический состав тела человека. На разной глубине фантома были вмонтированы детекторы. Которые расположены в тех точках, где находятся критические органы человека, именно поэтому фантом назвали «Матрешкой». Через определенное время детекторы вынимали и отправляли на Землю. Вместо них ставили новые детекторы, привезенные с Земли. Эксперимент продолжался в течение 10 лет. Его результаты показали, что реальное воздействие радиации на внутренние органы значительно ниже, чем показывали «обычные» дозиметры. Внутри МКС доза облучения, которому подвергаются космонавты, на 15% меньше, а при выходе в открытый космос – более чем в два раза меньше той, что считалась ранее.

Благодаря этим измерениям для космонавтов выработаны рекомендации, например, в каких отсеках МКС лучше находиться в период повышения солнечной активности, чтобы избежать лишней радиационной «нагрузки»

Российские автономные машиностроители давно помогают испытывать оборудование, которое будет использоваться на орбите. Тестирование проводится в условиях, имитирующих открытый космос.

Речь идет о работах еще одного предприятия «Атомэнергомаша» центрального научно-исследовательского института технологии машиностроения (ЦНИИТМАШ) по созданию вакуумного испытательного и технологического оборудования для космической отрасли.

Первым и успешным опытом ЦНИИТМАШа в этой области были разработка и изготовление жидкостной системы обеспечения теплового режима для тестирования бортовых электротехнических систем в условиях производства и предстартовых испытаний.

Пилотные системы были использованы при подготовке запуска модуля международной космической станции «Заря». Машины были поставлены в НПО «Энергия», и одна из них в последствии была направлена на стартовый комплекс космодрома «Байконур».

Аналогичные системы, но с другими характеристиками, были поставлены в ЦСКБ

«Прогресс» и в дальнейшем на стартовые комплексы космодрома «Плесецк» и «Байконур». В дальнейшем ЦНИИТМАШ создавались установки для проведения термовакуумных испытаний, имитирующих условия космического вакуума и температурные режимы эксплуатации космических аппаратов при орбитальном полете. Установки были оборудованы специально разработанными термостолами и холодильно-нагревательными машинами, позволяющими испытывать изделия в глубоком вакууме в широком диапазоне температур.

Сейчас в ЦНИИТМАШ создается исследовательский комплекс, в котором будут смоделированы условия космического пространства, и который будет предназначен для испытаний научной аппаратуры международной орбитальной обсерватории «Спектр-УФ». Эта обсерватория по своим возможностям близка к американскому космическому телескопу «Хаббл». С обсерватории ученые будут изучать физические процессы в ранней Вселенной, образование звезд, эволюцию галактик, процессы падения вещества в черные дыры, атмосферы планет и комет.

В создании элементов «Спектра-УФ» участвует еще одно предприятие Росатома, Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики (Саров).

Другое машиностроительное предприятие Росатома «ОКБМ Африкантов» (тоже входит в «Автомэнергомаш») создало опытный образец нового герметичного электронасоса для заправочного комплекса российской ракеты-носителя «Протон-М».

При успешном завершении всего комплекса испытаний, предприятием будет изготовлена партия таких насосов для «Байконура».

Без разработок Росатома не обходится и изучение свойств космических тел. Радиоактивный источник на основе изотопа кюрия-244, изготовленный Димитровградским Научно-исследовательским институтом атомных реакторов (НИИАР), «помог» научному модулю «Фила», севшему на поверхность ядра кометы Чурюмова-Герасименко, собрать данные о составе ее грунта. В результате облучения грунта альфа-частицами от источника возникает вторичное гамма-излучение, по которому с помощью спектрометра на борту модуля можно судить об особенностях поверхности кометы.

Именно НИИАР, где расположено уникальное производство кюрия-244 в свое время зарубежными партнерами было доверено выполнить работы для «кометной» миссии.

Изделия лаборатории отделения радиохимических источников и препаратов НИИАР используются в изучении Марса аппаратами НАСА.

Открытие, сделанное одним из таких марсоходов с помощью спектрального анализа грунта, позволило с большой вероятностью предположить, что когда-то на этой планете действительно была вода в виде снега, наледи или инея.

Кроме того, сейчас на борту марсохода Curosity работает российский прибор ДАН (Динамическое альбедо нейронов) для изучения состава марсианского грунта. В состав этого прибора входит нейтронный генератор, созданный другим предприятием Росатома – Всероссийским научно-исследовательским институтом автоматики имени Духова.

Благодаря прибору ДАН выяснилось, что в отдельных местах поверхности Марса содержания воды достигает 6% - столько же, сколько в земных пустынях.

Всё вышеизложенное свидетельствует о том, что сегодняшние технологии – это лишь далеко не совершенные копии отдельных элементов природных процессов. Решение проблем современного мира заключается в реализации стратегической цели – включить создаваемые технологии в естественный природный ресурсооборот на базе развития НБИКС – технологий. В этом состоит главное направление обеспечения национальной безопасности а, следовательно, укрепление суверенитета страны.

Библиографический список

1. Инновационное развитие – основа модернизации экономики России: национальный доклад. – М.: ИМЭМО РАН: ГУ «ВШЭ», 2008.

2. Официальный сайт Министерства образования и науки РФ. [Электронный ресурс]. – Режим доступа: www.fasi.gov.ru

3. Научно-популярные новости и статьи. [Электронный ресурс]. – Режим доступа: www.globalscience/ru

4. Сетевое издание "Вести.Ру". 2019. Главный редактор: Ениколопов Н.С. [Электронный ресурс]. – Режим доступа: https://nauka.vesti.ru/

5. Официальный сайт частного инвестиционного фонда «Онэксим» [Электронный ресурс]. – Режим доступа: www.onexim.ru

6. Информационно-аналитический центр. 2018. [Электронный ресурс]. – Режим доступа: https://inance.ru/2018/04/kosmonavtika-2/

7. Российский космос. [Электронный ресурс]. – Режим доступа: https://ruxpert.ru/

8. «Культура.РФ» - гуманитарный просветительский проект. 2013-2019. [Электронный ресурс]. – Режим доступа: https://www.culture.ru/materials/ 50445/kosmich-eskaya-gonka

9. Доклад о мировой атомной энергетике президента Всемирной ядерной ассоциации Агнеты Ризинг. [Электронный ресурс]. – Режим доступа: http://www.atomic-energy.ru/articles/ 2019/09/25/97637

10. Российская газета RG.RU [Электронный ресурс]. – Режим доступа: https://www.-google.ru/amp/s/rg.ru/amp/2017/06/02/kosmos-10-samyh-realistichnyh-proektov-osvoeniia-vselen-noj.html

СОДЕРЖАНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ И РОЛЬ ПРИБЫЛИ В ЕЁ ОБЕСПЕЧЕНИИ

Цыкунов Д.В., студент
Научный руководитель: Елисеева И.В., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Экономическая безопасность служит составной частью национальной безопасности и выступает залогом независимости Российской Федерации.

Национальная безопасность представляет собой гарантию защищённости государства от внутренних и внешних опасностей, устойчивость к нежелательным влияниям снаружи, обеспечение страны и её граждан стабильностью развития, противостоянием к негативным ситуациям. Она включает в себя составляющие: военную, экологическую, информационную, социальную, энергетическую и другие виды безопасности. Все они взаимодополняют друг друга.

Термин «экономическая безопасность» включает в себя комплекс действенных и результативных мероприятий, которые оказывают поддержку эффективному и масштабному росту национальной экономики, её способности удовлетворять потребности общества, нейтрализовать угрозы, обеспечивать конкурентоспособность на международных рынках. Причинно-следственная связь обеспечения экономической безопасности представлена на рисунке 1.

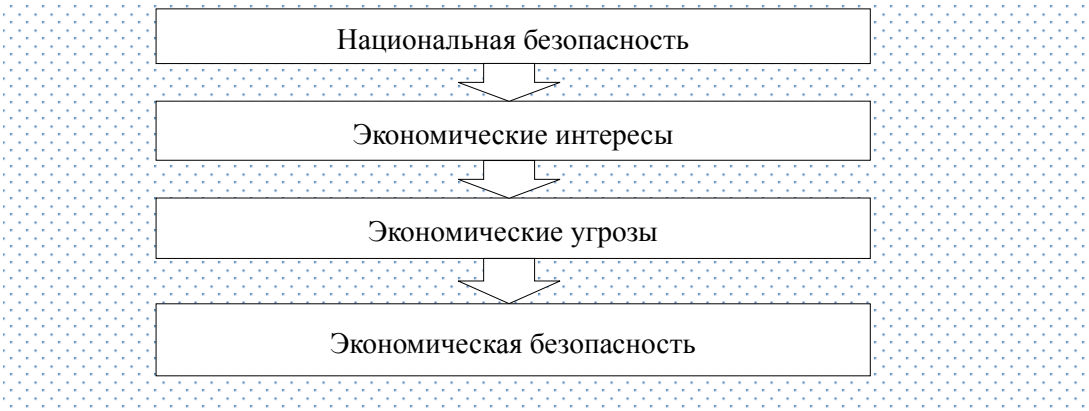

Рисунок 1 – Причинно-следственная связь обеспечения экономической безопасности

Экономические интересы основываются на стремлении государства и общества создавать необходимую материальную базу для обеспечения экономической безопасности во всех отраслях экономики, независимости на финансовом рынке, стабильности развития и устойчивого финансового положения в мире в целом. Характерной особенностью экономической безопасности выступает создание условий для потенциального удовлетворения интересов экономического характера как человека и общества, так и государства в целом.

Между тем, полное отсутствие экономической безопасности делает, бесспорно, невозможным реализацию иных сторон безопасности, таких как политического, военного, медицинского, правового и т.д. Недостаточность проработки экономических отношений или неспособность властей защитить экономические интересы общества и государства могут свидетельствовать о слабости власти, а в дальнейшем и низкой внутренней экономической безопасности и иных проблем. Экономическая безопасность существует в совокупности с безопасностью правовой, политической, технологической, экологической и других.

Экономическая категория «угроза экономической безопасности» представляет собой комплекс мероприятий, создающих потенциальную возможность нанесения экономического ущерба национальным интересам Российской Федерации в экономической сфере [1]. Классификация угроз экономической безопасности предприятия по месту возникновения представлена на рисунке 2.

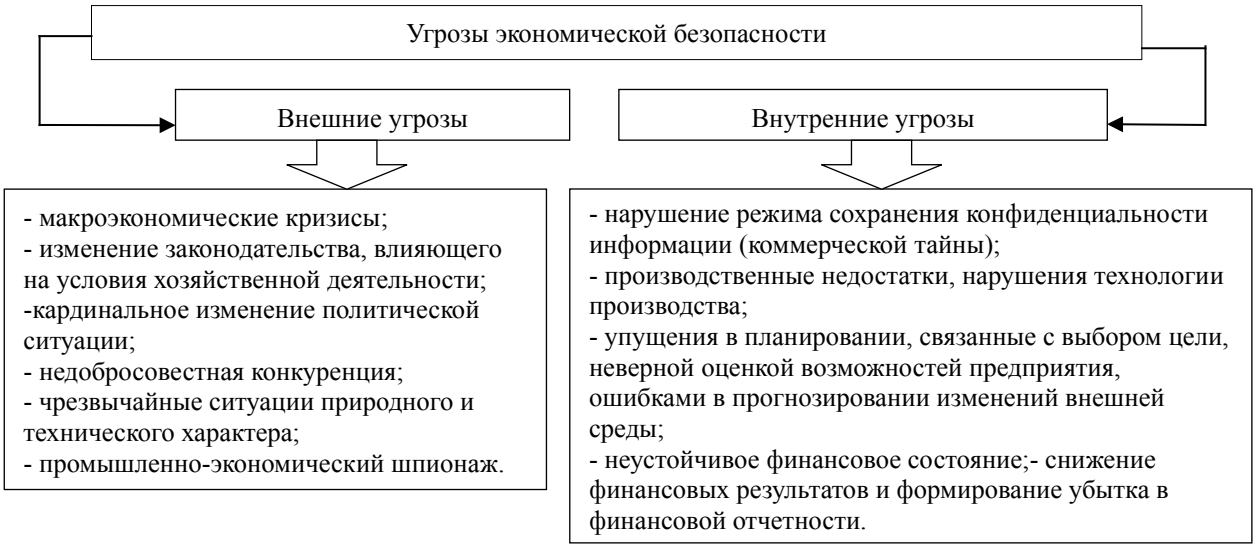

Рисунок 2 - Классификация угроз экономической безопасности предприятия по месту возникновения

Угрозы экономической безопасности можно рассмотреть с двух сторон. Первое

направление характеризуется влиянием угроз на экономические интересы, как следствие, вынуждая формирование современных целей и задач [2].

Второе направление включает совокупность откорректированных экономических интересов, которые активно воздействуют на государство, экономику страны в целом, в части принятия ими объективных и справедливых решений по сохранению экономических интересов общества и личности. Выполнение вышеприведённых направлений приведёт к укреплению экономической безопасности страны.

Понятие «экономическая безопасность» – это важнейший элемент устойчивости предприятия, его защищённости от потенциальных опасностей и угроз, противостояния кризисам, способности беспрепятственно функционировать и объективно определять пути экономического развития на перспективу.

Важнейшей составляющей при оценке уровня экономической безопасности предприятия является определение её критерия, их структура представлена на рисунке 3 [3].

Организационные критерии экономической безопасности дают представление о защите организации, её организационной целостности, как предприятия, так и его структурных подразделений.

Информационные критерии квалифицируют безопасность в аспекте сохранения защищённости и конфиденциальности внутренней информации от разглашения или утечки в различных формах.

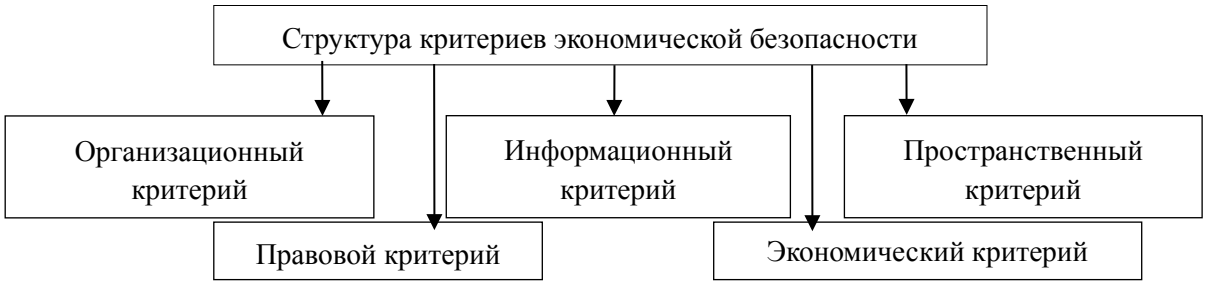

Рисунок 3 - Структура критериев экономической безопасности

Пространственный критерий включает в себя четыре уровня масштабного воздействия, которые представлены на рисунок 4 [4].

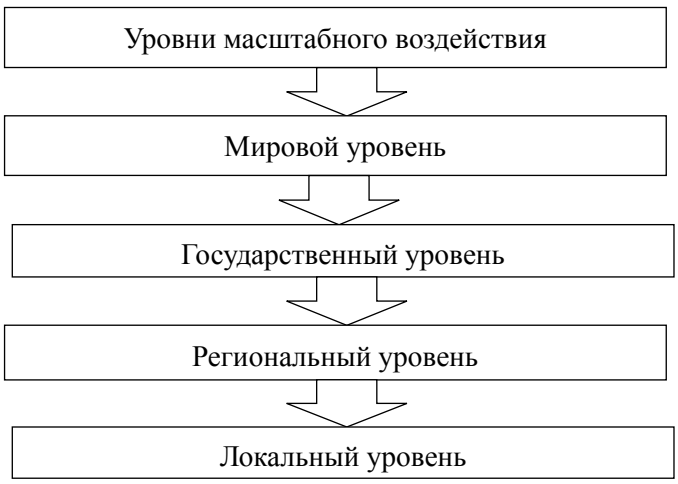

Рисунок 4 - Уровни масштабного воздействия

В работе обратим внимание на локальный уровень, именно он характеризует экономическую безопасность предприятия с позиции устойчивости, прибыльности и финансового риска. Что касается решения задач собственной экономической безопасности, то в данную стратегию входит поддержание ритмичного производства, предупреждение и устранение нанесённого ущерба, создание препятствия для доступа к инсайдерской информации и вскрытия компьютерных баз данных, противодействие злостной конкуренции

и преступным побуждениям.

Что касается правовых критериев, то они дают представление о соблюдении предприятием требований законодательства в отношении ведения финансово-хозяйственной деятельности.

Методологической основой экономического критерия является сохранение и преумножение определяющих показателей деятельности организации, таких как обеспеченность собственным капиталом, прибыль и рентабельность.

Прибыль как первостепенный показатель эффективности деятельности хозяйствующего субъекта является важнейшей составляющей экономической безопасности. Используя критериальный подход к определению перечня индикаторов экономической безопасности и влияния прибыли на её обеспечение предлагается воспользоваться мнениями различных авторов (рисунок 5).

Главной целью экономической безопасности организации является минимизация внешних и внутренних угроз, обеспечение устойчивого и максимально эффективного функционирования, а также создание высокого потенциала развития и роста предприятия в будущем[1].

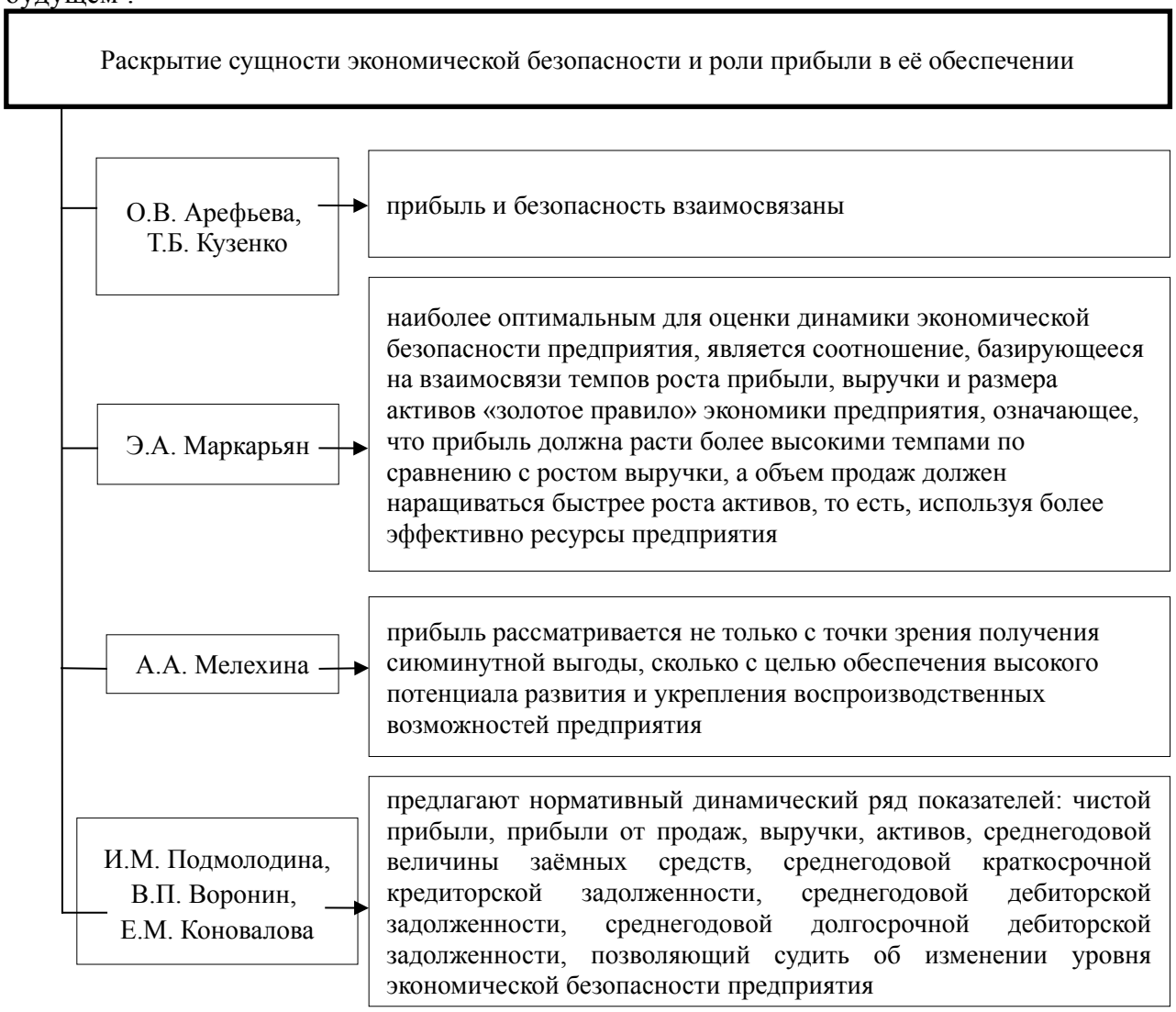

Рисунок 5 – Подходы авторов к раскрытию сущности экономической безопасности и роли прибыли в её обеспечении

[1] Ильяшенко, С.Н. Составляющие экономической безопасности предприятия и подходы к их оценке [Текст] // Актуальные проблемы экономики. 2017. №3. – С. 12-19.

Основные задачи обеспечения экономической безопасности предприятия: эффективное использование ресурсов предприятия; повышение инновационной активности предприятия; формирование оптимальной структуры источников формирования имущества: собственного и заёмного капитала; обеспечение устойчивого финансового состояния и роста финансовых результатов; обеспечение эффективной организационной структуры управления, создание новых центров финансовой ответственности; разработка и реализация основных методов и приёмов снижения риска и предотвращения угроз кризисного экономического состояния предприятия; обеспечение эффективной информационной защиты ресурсов предприятия; разработка методологического инструментария оценки и анализа экономической безопасности предприятия; процесс формирования и реализации системы стратегических планов экономического развития и безопасности предприятия.

Таким образом, термин «экономическая безопасность» включает в себя комплекс действенных и результативных мероприятий, которые оказывают поддержку эффективному и масштабному росту национальной экономики, её способности удовлетворять потребности общества, нейтрализовать угрозы, обеспечивать конкурентоспособность на международных рынках. В свою очередь обеспечение экономической безопасности находится в прямой зависимости от полученной прибыли предприятия.

Библиографический список

1. Боримская, Е.П. Роль прибыли в обеспечении экономической безопасности предприятия: направления усовершенствования бухгалтерского учета для целей управления [Текст] / Е.П. Боримская, И.А. Панченко // Международный бухгалтерский учет. 2017. № 35. – С. 58 - 68.

2. Бескрайная, Т.С. Экономическая безопасность предприятия: индикаторы и оценка [Текст] // Российский предприниматель. 2018. №8. – С. 62-68

3. Гапоненко, В.Ф. Экономическая безопасность предприятия. Подходы и принципы [Текст] / В.Ф. Гапоненко, А.Л. Беспалько, А.С. Власов. – М.: Ось-89. 2017. – 208 с.

4. Евсеева, А.Ю. Экономическая безопасность и ее значение для предпринимательской деятельности [Текст] / А.Ю. Евсеева, С.В. Котик // Налоговое планирование. 2018. № 3. – С. 46 - 48.

СУЩНОСТЬ И НЕОБХОДИМОСТЬ ЭКОНОМИЧЕСКОЙ ЭКСПЕРТИЗЫ НАЛИЧИЯ ПРИЗНАКОВ БАНКРОТСТВА

Цыкунов Д.В., студент
Научный руководитель: Елисеева А.И., преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Одной из разновидностей экономической экспертизы выступает экспертиза преднамеренного банкротства и фиктивного банкротства, на базе которой выясняются вопросы наличия признаков банкротства юридического лица, экономических правонарушений, непосредственно связанных с фиктивным банкротством и несостоятельностью юридических лиц с помощью применения специальных знаний в сфере процедуры банкротства.

Обзор экономической и научной литературы указывает на малую освещённость вопроса выявления наличия признаков преднамеренного и фиктивного банкротства путём проведения экономической экспертизы, поскольку проблема его обнаружения стоит на стыке двух сфер деятельности, как экономической, так и правовой.

Необходимо подчеркнуть отсутствие единого мнения учёных и экономистов в отношении преднамеренного и фиктивного банкротства, поскольку оно относится

специфическому виду экономических преступлений.

Юридическое понятие преднамеренного банкротства изложено в ст. 10 Федерального закона «О несостоятельности (банкротстве)» [1], где указывается, что в случае банкротства должника по вине его учредителей или участников или иных лиц, в том числе по вине руководителя должника, которые имели право давать обязательные для должника указания либо имеют возможность иным образом определять его действия, на учредителей (участников) должника - юридического лица или иных лиц в случае недостаточности имущества должника может быть возложена субсидиарная ответственность по его обязательствам.

Экономическое понятие «преднамеренное банкротство» выражается в умышленном создании, либо увеличении неплатёжеспособности предприятия, совершенном его руководителем или собственником в личных интересах или интересах иных лиц, причинившее крупный ущерб либо иные тяжкие последствия путём заключения заведомо невыгодных сделок, некомпетентного ведения дел, принятия на себя чужих долгов в качестве поручителя и иных действий, ведущих к невозможности удовлетворить требования кредиторов [2].

Существует объективная необходимость разграничивать преднамеренное банкротство в интересах собственника бизнеса с целью избежание материальной и юридической ответственности перед кредиторами, и преднамеренное банкротство в интересах третьих лиц с целью раздела имущества. Следует отметить, что сформировать доказательную базу применительно к действиям руководителя достаточно проблематично, поэтому на практике такие преступления чаще классифицируются как мошенничество и причинение имущественного вреда в особо крупном размере.

Фиктивное банкротство – введение в заблуждение кредиторов путём ложного объявления компании о своей неплатёжеспособности. Целью такого банкротства является получение от кредиторов льгот по оплате финансовых обязательств, утаивание активов для расчётов с кредиторами, либо понуждение приёма неконкурентоспособной продукции в счёт погашения задолженности предприятия. По представлению арбитражных управляющих, лица, виновные в ложном объявлении организации неплатёжеспособной, преследуются в уголовном порядке [3].

Основная цель эксперта, выполняющего экономическую экспертизу наличия признаков преднамеренного и фиктивного банкротства, состоит в выявлении действий заинтересованных лиц, управляющих предприятием-банкротом до и после процедуры банкротства, а также предоставление суду необходимых подтверждений раскрытых нарушений в процедуре банкротства.

Задачи экономической экспертизы банкротства представлены на рисунке 1.

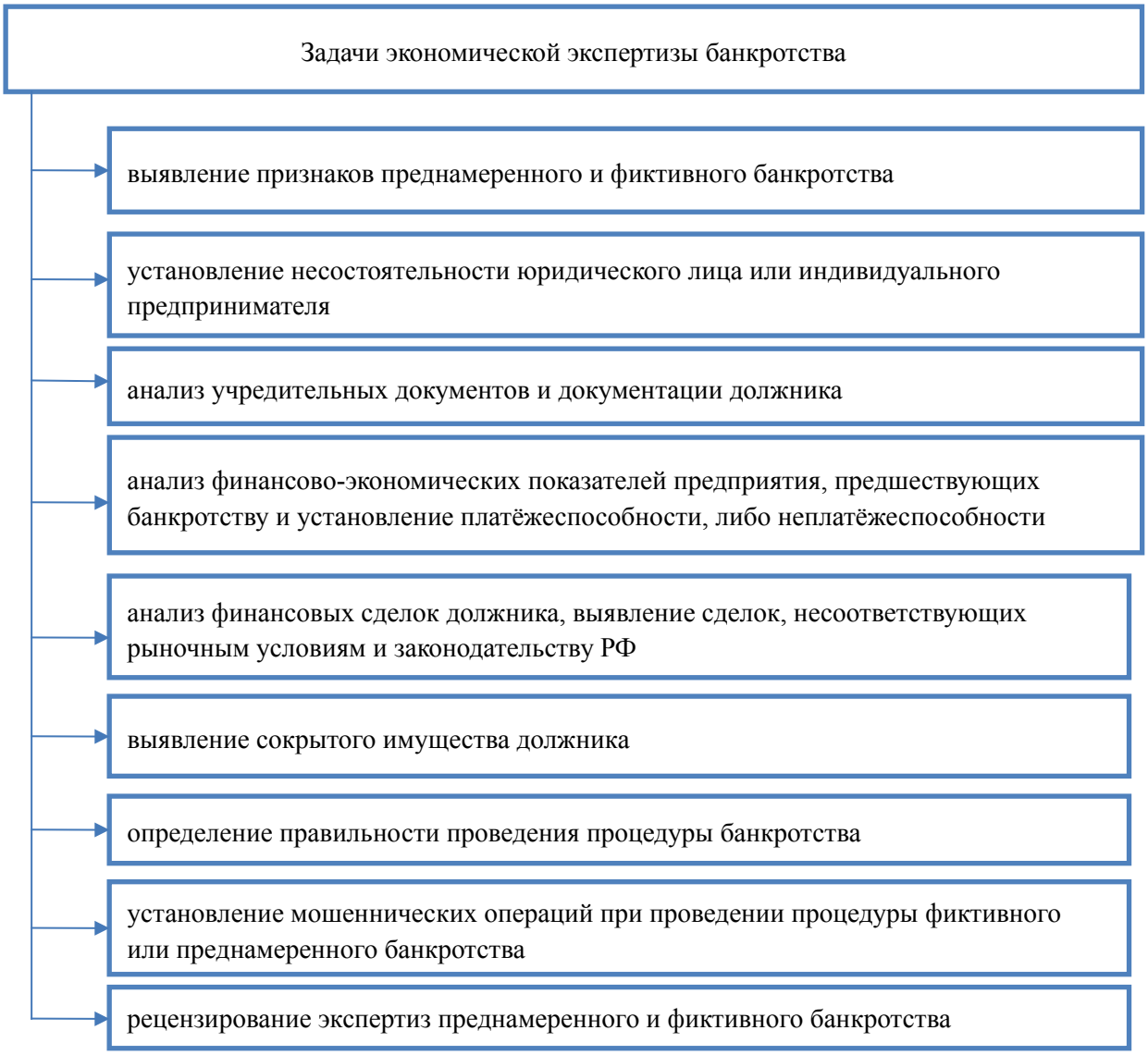

Рисунок 1 - Задачи экономической экспертизы наличия признаков банкротства

В целях подготовки логичного и экономически верного экспертного заключения необходимо обозначить основные вопросы, требующие решения:

1. Зафиксировать формулировку экспертного задания.
2. Обозначить кандидатуры на место эксперта.
3. Отразить сроки и стоимость проведения экономической экспертизы.

При верном подходе к решению указанных важных вопросов вероятность формирования достоверного и объективного экспертного заключения возрастает.

Одним из методов диагностирования преднамеренного и фиктивного банкротства, связанного с неправомерными действиями руководителя или третьих лиц является необходимость обнаружения следующих форм несоответствий:

- между заявлением руководителя или владельца бизнеса о несостоятельности и действительным положением платёжного баланса фирмы;
- между фактами действующего договора о получении отсрочек, скидок и неуплаченными долгами или оплатами в адрес аффилированных лиц, в том числе с использованием взаимозачётной системы;
- факт отсутствия эффективного управления хозяйствующим субъектом от лица руководителя или арбитражного управляющего (назначенного предприятием или судом);
- между заявленными и подтверждёнными документально финансовыми улучшениями, и текущими действиями заинтересованных лиц, которые манипулируют

неплатёжеспособностью предприятия-банкрота;

- между официальной заработной платой и отражёнными зачислениями выручки, и нелегальными действиями по выводу средств, причиняющие существенные убытки для бизнеса;

- между имуществом должника и мероприятиями по сокрытию информации об указанной собственности, её размерах и положению;

- между объективной необходимостью введения конкурсного производства, а также вопреки установленной очерёдности удовлетворения требований кредиторов, действий по выводу имущества, фальсификации бухгалтерских и юридических документов, отражающих действительную экономическую ситуацию и оплаты в адрес третьих лиц в убыток реальных кредиторов.

На основе изучения трудов учёных-экономистов выявлены основные факты, на которые необходимо обратить внимание при проведении экономической экспертизы бухгалтерской отчётности предприятия-банкрота:

- наличие ликвидных активов;

- наличие денежных средств;

- убеждённость заимодавцев в неплатёжеспособности должника;

- факт невыполнения финансовых обязательств перед кредиторами при условии наличия денежных средств, материалов или готовой продукции;

- отсутствие оплат по долгам при условии положительного платёжного баланса;

- факты необоснованного роста себестоимости;

- наличие значительной величины кредиторской задолженности при условии получения положительного аудиторского заключения в части платёжеспособности;

- факт отгрузок продукции без выставления счетов на оплату;

- факт авансовых оплат, в том числе без оформления договоров;

- заключение договоров на заведомо невыгодных условиях (например, по завышенным или заниженным рыночным ценам или с принятием чрезмерных рисков);

- факт нецелесообразного увеличения количества штатных работников или существенный рост заработной платы отдельных категорий управленческого персонала;

- факт выдачи руководящему персоналу беспроцентных займов или долгосрочных фактически невозвратных ссуд;

- необоснованный рост затрат предприятия в виду проведения ремонта или покупки дорогостоящих транспортных средства для личного пользования управленческого персонала, оплата путёвок или неправоверных командировок указанных лиц;

- факт инвестирования отдельных компаний при условии, что предприятие находится в предкризисном состоянии;

- факт сдачи имущества в аренду по заниженной цене;

- факт продажи или безвозмездной передачи имущества при условии предкризисного состояния предприятия;

- факт невозврата хищений или растраты материально ответственными лицами денежных средств или имущества предприятия;

- признаки причастности управленческого состава к мошенническим схемам, применяемым к предприятию-банкроту;

- факт наличия невыгодных сделок с признака коррумпирования руководящего состава;

- дробление бизнеса;

- факт подачи заведомо ложных ответов на вопросы заимодавцев;

- факт нарушения очерёдности оплаты кредиторам в виде завуалированных оплат;

- искажение финансовых документов для занижения налоговой базы;

- намерение подкупа членов инвентаризационной комиссии для сокрытия информации об имуществе.

Таким образом, необходимость проведения экономической экспертизы преднамеренного и фиктивного банкротства состоит в обнаружении несоответствий и

прецедентов посредством применения специальных знаний эксперта. При этом особое внимание обращается на такие признаки, как сокрытие собственности должника, использование схем по выводу денежных средств, наличие значительных сумм просроченной дебиторской задолженности и другие факторы, указанные выше в настоящей работе.

В виду вышеизложенного необходимо отметить, что анализ финансового состояния и финансовых результатов является ключевым инструментом при оценке показателей деятельности с целью обнаружения преднамеренного и фиктивного банкротства. Следовательно, далее целесообразно рассмотреть методологию диагностики вероятности банкротства.

Библиографический список

1. Федеральный закон от 26.10.2002 N 127-ФЗ «О несостоятельности (банкротстве)» (ред. от 27.12.2018) (с изм. и доп. вступ. в силу с 01.01.2019).
2. Федорова, Г.В. Учёт и анализ банкротств. - М.: "Омега-Л", 2016. 360 с.
3. Хоружий, Л.И. Учёт, отчётность и анализ в условиях антикризисного управления [Текст]: Учебное пособие/Л.И. Хоружий, И.Н. Турчаева, Н.А. Кокорев - М.: НИЦ ИНФРА-М, 2015. – 320 с.

ИНФОРМАЦИОННАЯ УГРОЗА СМИ В МЕЖКУЛЬТУРНОЙ ПОЛИТИЧЕСКОЙ КОММУНИКАЦИИ

Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти
Благов А.В., к. т. н.
Самарский национальный исследовательский университет
имени академика С.П. Королева
г. Самара

Одно из наиболее полных определений межкультурной политической коммуникации сформулировал французский политолог Р.-Ж. Шварценберг, трактуя ее как «процесс передачи политической информации, благодаря которому она циркулирует от одной части политической системы к другой и между политической системой и социальной системой. Идет непрерывный процесс обмена информацией между индивидами и группами на всех уровнях» [8, С. 60].

Существует три способа межкультурной политической коммуникации:

1) коммуникация через средства массовой информации;

2) коммуникация через организации, такие как политические партии, научные центры и институты, консультационные службы;

3) коммуникация через неформальные контакты на основе личных связей, характерная как для примитивных, так и для развитых обществ. [4, С. 15].

Именно осуществление межкультурной политической коммуникации через СМИ позволяет говорить о том, что они выступают в роли активного субъекта политической жизни. СМИ создают образ страны, который влияет на внешнюю и внутреннюю политику государства и на мнение общества о данной стране.

Под образом подразумеваются «отраженные» в сознании участников коммуникации с разной степенью адекватности фрагменты реальности. При формировании образа государства СМИ используются для достижения следующих целей: утверждение позитивных характеристик объекта; создание неблагоприятного облика противоборствующей стороны.

Каждое государство пытается максимально эффективно использовать ресурс, предоставляемый средствами массовой информации, в свою пользу. Межкультурной политической коммуникации свойственна информационно-пропагандистская деятельность по производству и распространению социально-политической информации, направленной на формирование образа мыслей и действий индивидуумов.

Наиболее значимые для общественности и наиболее обсуждаемые темы в СМИ получили название медиатопиков (регулярно воспроизводимых тем). Тематические составляющие зависят от страны и культуры. Например, из постоянных тем для британских СМИ является освещение подробностей частной жизни членов королевской семьи и высокопоставленных политиков. Если обратиться к темам российского медиаландшафта, то значительную долю занимают новости о коррупции и криминальных разборках. Регулярно воспроизводимые темы, отражающие национально-культурную специфику того или иного медиаландшафта, называются buzz-topics, или темы, вызывающие повышенный интерес [2, С. 55].

В статье «Типология медиатекстов как основа формирования медиаграмотности» Н.В. Чичерина говорит о том, что любой текст СМИ обладает совокупностью устойчивых характеристик, связанных с функциональной определенностью современных средств массовой информации:

1) ориентированность медиатекстов на массовую аудиторию;

2) динамический характер медиатекстов, проявляющийся на внутритекстовом, надтекстовом и гепертекстовых уровнях;

3) многоплановость, многомерность, полифоничность, гетерогенность и интегральность медиатекстов, обусловленные развитием новых информационных технологий;

4) социально-регулятивная природа медиатекста как «уникального средства интерпретации и репрезентации реальности» [7].

Рассмотрим подробнее последнюю характеристику.

Тексты СМИ создаются с какой-либо целью и рассчитаны на определенное воздействие. Они представляют собой социально значимые сообщения, превалирующие в обществе над всеми другими видами текстов. Их взаимодействие с сознанием реципиента создают медиа-коммуникативное событие, которое является основным механизмом формирования картины мира индивида. Передавая социальную, политическую и культурную информацию, СМИ способствуют формированию конкретной картины мира в сознании адресата. Еще американский политолог Г. Ласуэлл выделил основные функции СМИ:

1) наблюдение за миром (сбор и распространение информации);

2) «редактирование» (отбор и комментирование информации);

3) формирование общественного мнения;

4) распространение культуры.

Воздействующая функция СМИ в основном проявляется на уровне публицистики. Являясь наиболее «открытым» в системе функциональных стилей, публицистический стиль «обслуживает политико-идеологические, общественно-экономические и культурные отношения» [5]. Через публицистику отображается политическая жизнь общества. Одна из особенностей межкультурной политической коммуникации сегодня состоит в том, что политик, претендующий на сколько-нибудь значительную роль в общественной жизни своей страны, должен активно использовать медийную информационную сферу, чтобы иметь реальную возможность заявить о себе и обеспечить продвижение своих идей, опираясь на поддержку общественного мнения [1, С. 9].

По мнению исследователя проблематики психологического манипулирования в средствах массовой информации психолога Р.Р. Гарифуллина, средства массовой информации представляют собой особое окно в мир. Они искажают реальный образ мира, окружающего человека. Объективно охватить весь мир невозможно. Средства массовой информации умышленно вводят в заблуждение интернет-пользователей, читателей, телезрителей, радиослушателей.

Исследователь С. Г. Кара-Мурза выделил несколько приемов, с помощью которых СМИ манипулируют сознанием общественности.

1. Фабрикация фактов (прямая ложь). Сложность при реализации данного приема заключается в том, чтобы создать у адресата иллюзию независимости, плюрализма каналов информации. Для этого создается видимость многообразия СМИ по типу организаций, политической окраске, жанрам и стилям – при условии, что реально вся эта система подчиняется единым главным установкам.

2. Отбор событий реальности для сообщений. Несмотря на изобилие изданий и передач, разнообразии «позиций» и стилей СМИ создают и используют одни и те же стереотипы и внушают один и тот же набор главных желаний. При такой хорошо построенной системе допускается возможность конструирования взглядом, но структура мышления должна быть одинаковой.

3. Прием замалчивания «ненужной» информации и создания «виртуальной» реальности вместо отражения действительности. При использовании данного приема СМИ опираются на принцип *демократии шума* – потопление сообщения, которого невозможно избежать, в хаотическом потоке бессмысленной, пустопорожней информации.

4. Серая и черная пропаганда. Во второй половине XX века СМИ стали использовать

технологии *психологической войны*. Здесь информация выступает в роли «оружия» [3, С. 29].

Термин «информационное оружие» обозначает информационное воздействие на противника.

В случае с межкультурной политической коммуникацией противник – это определенное государство, его система ценностей, политический режим и т. д. И воздействие оказывается на сознание граждан как этой страны, так и мировой общественности через создание конкретного образа данного государства.

Исследователями выделяются следующие виды информационного оружия:

1) информационные средства, методы, технологии воздействия на человеческую психику (СМИ, аудио- и видеопродукты, компьютерные игры, плакаты и листовки, слухи);

2) средства дезинформации, влияющие на систему принятия решений (навязывание, искажение, блокирование информации, отвлечение на другую информацию с помощью СМИ и средств связи);

3) средства радиоэлектронной борьбы (радиопомехи, внедрение подслушивающих устройств, перехват передач, блокировка сотовой связи и т.д.);

4) воздействие на программно-техническое оборудование (взлом компьютерных систем, кража личных паролей, уничтожение данных и т.д.).

Сообщая соответствующую социальную, политическую и культурную информацию, СМИ включаются в процесс и результаты социально-политической коммуникации, способствуя формированию конкретной картины мира в сознании адресата. Они обеспечивают расширенную форму человеческой коммуникации. Функциями СМИ в рамках межкультурной политической коммуникации являются политизация общества и политическое просвещение широких слоев населения. Наличие в СМИ различной информации и множества средств подачи материала способствует «поддержанию в информационном поле плюрализма репрезентаций реальности и, в частности, наличию некоторого множества репрезентаций одного и того же фрагмента реальности» [6].

Они репрезентируют реальность для индивидов, однако, важным остается вопрос насколько полно и точно СМИ репрезентуют данную реальность.

Библиографический список

1. Володина, М.Н. О роли СМИ в процессе политической коммуникации (на материале немецких массмедиа) [Текст] / М.Н. Володина // Политическая лингвистика / гл. ред. А.П. Чудинов. – Екатеринбург: ГОУ ВПО Урал. гос. пед. ун-т. – 2010. – № 4 (34). – С. 9 – 13.

2. Добросклонская, Т.Г. Медиалингвистика: системный подход к изучению языка СМИ [Текст] : учеб. пособие / Т.Г. Добросклонская. – М.: Наука, 2008. – 202 с.

3. Кара-Мурза, С.Г. Манипуляция сознанием [Текст] / С.Г. Кара-Мурза. – М.: Эксмо, 2000. – 864 с.

4. Кретов, Б.Е. Средства массовой коммуникации – элемент политической системы общества [Текст] / Б.Е. Кретов // Социально-гуманитарные знания. – 2000. – №1. – С. 15 – 17.

5. Кушнерук, С.Л. Расширение коммуникативного пространства: специфика текстов электронных СМИ в сравнении с печатными [Электронный ресурс] // Политическая лингвистика. – 2007. – № 23. – С. 140–143. URL: https://goo.gl/zWUEzs

6. Стриженко, А.А. Зарубежная и российская журналистика: трансформация картины мира и ее содержания [Электронный ресурс] / А.А. Стриженко. Монография. 2003. URL: https://goo.gl/fYxgfO

7. Чичерина, Н.В. Типология медиатекстов как основа формирования медиаграмотности [Электронный ресурс] / Н.В. Чичерина // Известия Российского гос. пед. ун-та им. А.И. Герцена. Серия: Общественные и гуманитарные науки (философия, языкознание, литературоведение, культурология, экономика, право, история, социология). – 2007. – № 9. URL: https://goo.gl/qNs8mD

8. Шварценберг, Р.Ж. Политическая социология [Текст] / Р.Ж. Шварценберг: в 3 ч. – Ч.1. – Москва, 2013. – 174 с.

ДЕЗИНФОРМАЦИЯ В СОЦИАЛЬНЫХ СЕТЯХ КАК ОДНА ИЗ ОПАСНОСТЕЙ В СИСТЕМЕ СМИ

Гаврилова А.А., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

Об эффекте воздействия СМИ мир начал говорить с момента появления первого печатного станка и, на самом деле, задолго до него, но никто просто не задумывался над этим и не давал данному явлению название. Когда человечество еще не пришло к созданию печатного издания и понятию «СМИ», можно говорить о том, что каждый отдельно взятый человек был средством массовой информации, являясь передатчиком информации, как передавался, к примеру, фольклор. Дезинформация, как одно из негативных явлений СМИ, раньше просто называлась намеренной ложью. Она существовала также задолго до появления первых изданий и посему всегда находилась бок обок с развитием журналистики.

Можно утверждать, что навык владения информацией определяет уровень развития человека. Чем выше в своем развитии поднимается человек, тем больше его потребность в информировании себя. Но важно понимать, что любую информацию, из абсолютно любого источника нужно уметь «фильтровать», перепроверять, нужно уметь определять цель написания того или иного материала, посыл автора, замысел или даже умысел.

В наше время большая часть людей обладает ускоренным покадровым мышлением, которое играет злую роль. Такое мышление не толкает человека задуматься над прочитанной новостью, оценить её правдивость, источник. Аудитории с преимущественно таким мышлением даже не интересно открывать материал и тем более читать его, если она видит, что он большой. Отсюда и вытекает побочный эффект «выдергивания» смысла, контекста и общего посыла текста, так как такая аудитория просто выхватывает пару предложений из всего материала. Следовательно, разбираться в правдивости материала такая часть аудитории не будет, она безоговорочно принимает то, что ей дают.

Усложняется ситуация тем, что происходит все это в основном в интернете, как правило, в социальных сетях, где контролировать поток лжеинформации почти невозможно. Некоторый контроль существует лишь у больших, известных и авторитетных интернет-изданий, а также там, где люди должно относятся к тому, что они предоставляют информацию аудитории и она должна соответствовать некоторым критериям, один из которых это правдивость.

Предотвратить распространение дезинформации в принципе своем невозможно, но можно и даже нужно научиться и учить других, как можно обезопасить себя от лжеинформации, урегулировав в лучшую сторону свою социальную жизнь в интернете.

В первую очередь, необходимо избавиться от лишних подписок на всевозможные группы, сообщества, страницы. Не нужно копить мусор, разобраться в котором на 100% вы не сможете. Но если же все источники, по-вашему мнению, вам необходимы, то не заходите в общую ленту новостей, а открывайте вкладку «Сообщества» и выборочно открывайте нужный вам источник.

Интересы и потребности людей меняются бессчетное количество раз. На досуге вы можете заняться упорядочиванием, удалением ненужных подписок, которые, скорее всего, давно потеряли для вас актуальность в силу утраты того или иного интереса.

Важно отметить, что не стоит отписываться от всех неофициальных СМИ и читать только широко известные и наоборот. Важно иметь под рукой и источники официальных средств массовой информации, и неофициальных, и по месту вашего жительства, и т.д. Это

обуславливается тем, что в разных источниках соответственно разная информация. Материалы, касающиеся вашего региона проживания, никак не будут публиковаться в сообществе СМИ, которое охватывает всю страну или даже мир. И в большей степени наоборот. А также у вас будет хорошая возможность сравнивать материалы, уточнять детали, видеть реакцию аудитории, с которой нужно обращаться предельно аккуратно и внимательно.

Не читайте комментарии под публикацией от и до, не вникайте в возникшие конфликты читателей, обобщенные оскорбляющие комментарии и т.п. Это, на самом деле, очень опасно. Фильтровать просматриваемые комментарии, где сплошь может быть недостоверная информация, нужно с предельным пониманием того, что все люди пишут в интернете то, что хотят.

Если вы не согласны с предоставленной для вас информацией того или иного СМИ, то писать гневные комментарии и ступать в спор с другими пользователями сети не стоит. Если у вас возникло сильное желание исправить ситуацию, как-то попытаться на нее повлиять, что-то опровергнуть и наоборот, то для таких случаев существует прямая связь со СМИ в виде приложенных контактов для обращения читателей. Не нужно бояться писать в редакцию, но и не забывайте о соблюдении всех форм приличия, обращения, тона и т.д.

Что касается еще одного вида дезинформации в интернете, так это мошенничество, нечестные конкурсы и розыгрыши. Именно благодаря интернету, мошенники обманывают бессчетное число населения, которое не задумалось о перепроверке информации, особенно если речь идет о внесении некоторой денежной суммы. Даже если на ваш взгляд все в порядке, не бойтесь задавать много вопросов. Если перед вами обман, недобросовестный человек обязательно совершит осечку. Осечка бывает настолько незаметна, что и здесь вам придется применить всю вашу логику и здравый смысл.

Многие легко верят в то, что им говорят или в то, что они читают, если это соответствует их ожиданиям, представлениям и идеалам. Дезинформация зачастую – это именно то, что люди хотят услышать или попросту то, над чем они не хотят размышлять, поэтому подсунуть такую информацию довольно просто. Как ни странно, намного труднее донести до людей правду, особенно если она противоречит некоему мифу или идеалу, основанному на внутренних убеждениях и внешних ориентирах.

Определить дезинформацию можно, только если сам обладаешь информацией. Важно определить источники дезинформации, чтобы потом оградиться от них. Лучший способ обезопасить себя — это одинаково осторожно относится ко всем источникам информации и не воспринимать за правду любую информацию, даже если вы получаете ее из официальных СМИ. Нынешние реалии таковы, что даже самый проверенный, официальный источник может ошибаться.

Библиографический список

1. Володина, М.Н. Язык СМИ - основное средство воздействия на массовое сознание [Текст] / М.Н. Володина // Язык СМИ как объект междисциплинарного исследования. - М.: Изд-во МГУ, 2003.

2. Добросклонская, Т.Г. Вопросы изучения медиатекстов (опыт исследования современной английской медиаречи) [Текст] / Т.Г. Добросклонская // Изд. 2-е, стереотипное. М., 2005. – 83 с.

3. Короткова, Л.Н. «Социология общественного мнения» [Текст] / Л.Н. Короткова // Конспект лекций, Санкт-Петербург, 1999.

БЕЗОПАСНОСТЬ В СМИ: ОСОБЕННОСТИ РАЗРЕШЕНИЯ КОНФЛИКТА В МЕДИАПРОСТРАНСТВЕ

Гудкова С.А., магистрант
Тольяттинский государственный университет
г. Тольятти

Сегодня средства массовой информации являются мощнейшим инструментом, оказывающим влияние на становление личности в обществе. Этому в большей мере способствовало развитие средств вычислительной техники, Интернет и коммуникационных каналов доступа к информации. Благодаря современным направлениям развития информатизации и цифровизации, средства массовой информации стали основным источником знаний о ситуации в мире и стране.

СМИ, как инструмент важного влияния на массы, должен выдавать проверенную информацию, гарантирующую социальную стабильность безопасность в стране, поэтому выбор темы исследования является актуальным и обоснованным.

Анализ различных информационных источников показал, что медиапространство сегодня является одним из факторов возникновения угроз информационной безопасности, так как непосредственно к самим угрозам информационной безопасности можно отнести манипулирование информацией (сокрытие, искажение). К сожалению, конфликты между участниками коммуникации в медиапространстве продолжают распространяться. На рисунке 1 показан рост возникновения конфликтных ситуаций в процессе коммуникации.

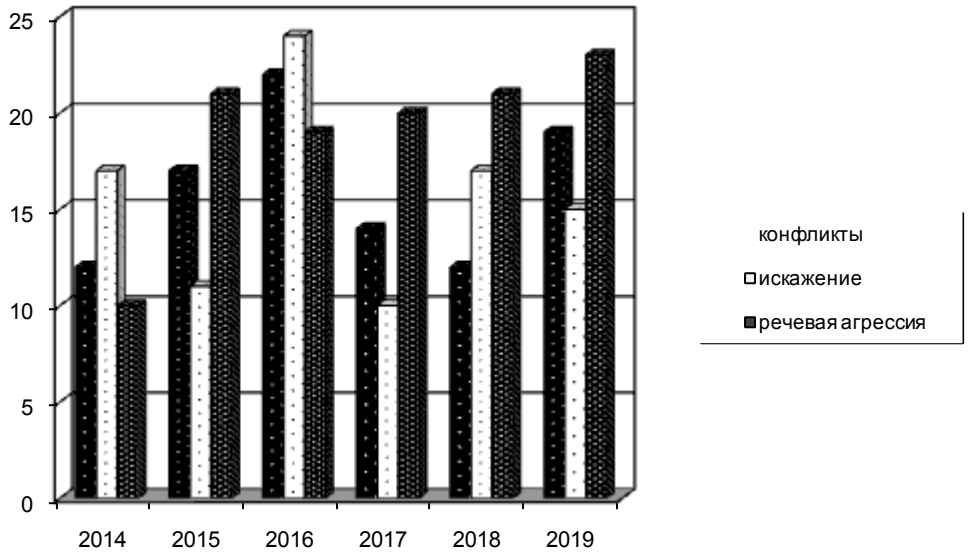

Рисунок 1 - Динамика возникновения возможностей нарушения безопасности

Данные получены автором путем анализа интернет-источников. Анализ производился за период 2014-2018 гг., на основе текстовой информации, отраженной в средствах массовой информации.

Полученные результаты позволили сделать выводы о том, что в современном медиапространстве наблюдается тенденция к снижению у коммуникантов способности ведения конструктивных диалогов.

В качестве подтверждения можно привести наличие на телеэкранах передач в жанре ток-шоу, особенно с политической тематикой («Время покажет, Право голоса», политические дебаты в преддверии выборов президента РФ и т.д.). Разнообразные ток-шоу проводятся с целью показать разные точки зрения на имеющуюся проблему, предоставить участникам передачи возможность озвучить и защитить свою точку зрения, тем самым воздействовать на сознание зрителей, способствовать формированию и распространению коммуникационных ценностей, моделей поведения в обыденной жизни.

По мнению Н.А. Кондратьевой и Л.В. Мордовиной, распространенная форма ток-шоу – это обсуждение какого-либо вопроса, в котором принимают участие приглашенные эксперты и аудитория зрителей. При этом важно как наличие актуальной проблемы, так и присутствие участников общения (ведущий, эксперты, зрители). Как отмечает В.Н. Степанов, значительной фигурой ток-шоу является ведущий (модератор коммуникации). Его задача

вовлекать в процесс общения, при этом использовать провокацию как средство активизации аудитории, возбуждать интерес, направлять аудиторию по заранее выстроенному сценарию, формировать общий настрой.

Это влечет за собой вербальную (речевую) агрессию, провоцирующую коммуникативный конфликт.

Под конфликтом будем понимать такую ситуацию, в которой участники сталкиваются по поводу расхождения взглядов, интересов, целей, и при этом один из участников сознательно действует в ущерб другому, а второй участник, осознавая, что эти действия направлены против его интересов, предпринимает ответные действия.

Таким образом, возникающий в средствах СМИ речевой конфликт можно считать результатом особенного взаимодействия субъектов, возникающего в результате речевого поведения.

Отметим, что особо ярко речевая агрессия демонстрируется в рамках политического дискурса, особенно в формате предвыборных политических дебатов (табл. 1). Здесь замечено использование участниками коммуникативных и манипулятивных стратегий, дискредитирующих оппонента; вербальная агрессия коммуникантов, проявляющаяся в использовании пейоративной (оценочно-отрицательной) лексики и построении с ее помощью инвективных высказываний. Зачастую такая лексика является катализатором дискуссии и переключает внимание слушателей с обсуждаемой тематики общественно-политического характера на личностные характеристики участников коммуникации.

В таблице показаны результаты анализа высказываний в медиапространстве кандидатов в президенты РФ в предвыборных дебатах 2012 и 2018 годах. Анализировались высказывания В. Жириновского, М. Сурайкина, К. Собчак и М. Шевченко (который представлял доверенное лицо кандидата П. Грудинина).

Таблица 1 - Анализ инвектив, относящихся к третьему конкретному лицу (фрагмент)

Инъективы	Кто о ком
Если мы будем следовать рецептам Михаила Дмитриевича Прохорова, Россия погибнет!	В. Жириновский о М. Прохорове
Если мы будем следовать рецептам Михаила Дмитриевича Прохорова, Россия погибнет!	В. Жириновский о В. Зюганове
Даже КПРФ, которую мы считаем братской партией, продалась капиталу и выдвинула олигарха Грудинина, который сбежал с эфира, струсил, не хочет уважать избирателей.	М. Сурайкин в адрес М. Шевченко

Таким образом, инвективные высказывания участников политических телевизионных шоу становятся все более разнообразными и, как показывают результаты выборов, их целенаправленное использование помогает политикам достигать запланированных результатов. Зачастую речевая агрессия становится информационным поводом, а оскорбление – катализатором политических дискуссий и демонстрацией яркого эмоционального отношения оппонентов друг к другу.

В качестве рекомендаций по профилактике и разрешению конфликтных ситуаций можно рекомендовать следующие приемы: корректное объяснение своей позиции, извинение, признание своей вины, умение вовремя промолчать, игнорирование речевой агрессии собеседника, кроме того, умение идти на компромисс, вежливый тон, соблюдение правил этикета, доброжелательное отношение к партнеру.

Библиографический список

1. Воронцова, Т.А. Речевая агрессия: коммуникативно-дискурсивный подход [Текст]: автореферат диссертации на соискание ученой степени доктора филологических наук. – Челябинск, 2006. – 43 с.

2. Щербинина, Ю.В. Речевая агрессия. Территория вражды [Текст] / Ю.В. Щербинина. – М.: Форум, 2012.

НЕПРИКОСНОВЕННОСТЬ ЖУРНАЛИСТОВ В ЗОНЕ ВООРУЖЕННЫХ КОНФЛИКТОВ

Пензова А.А., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

Журналисты в зоне вооруженного конфликта имеют особый статус и в своем роде неприкосновенность. Об этом говориться в документах права вооруженных конфликтов. В статье 81 Женевской конвенции 1929 года указывается, что «лица, следующие за вооруженными силами, но не входящие при этом в их личный состав, такие, как корреспонденты, репортеры газет, маркитанты и поставщики, оказавшиеся во власти противника, который считает необходимым их задержание, имеют право на обращение с ними как с военнопленными при условии имеющегося у них законного разрешения военных властей вооруженных сил, за которыми они следуют». А это значит, что в случае захвата журналистов стороной противника, они имеют права военнопленных и должное к ним обращение и статус, но только при условии имеющегося удостоверения, выданного властями их страны. Как только журналист берет в руки оружие он теряет привилегии и становится комбатантом.

Но все это идеально лишь в документах и самых редких случаях в жизни, так как на самом деле журналисты часто подвергаются обстрелам и используются стороной противника в своих корыстных целях.

Запрещено нападать на СМИ даже если они ведут пропаганду против противоположенной стороны. В документах гуманитарного права это выглядит идеально, но на практике как правило совсем другое. По статистике с 1990 года в мире уже было убито в общей сложности более 2500 журналистов. В любой горячей точке где бы не находились СМИ к ним нет никакой жалости. В Афганистане в 2018 году в результате нападений погибли 10 журналистов, позже в Кабуле была подорвана еще одна группа журналистов и таких случаем по всему миру огромное количество. А количество убитых представителей СМИ в Ираке, как одной, так и другой стороны, подвергает в шок. Ничего не гарантирует безопасность журналистов, все держится на честном слове и «благородности» воюющих сторон. Но во время бойни в ход идут все нечестные методы ведения войны.

Но пока в мире продолжаются войны, журналисты будут погибать. И никакие меры не смогут это предотвратить.

Библиографический список

1. Исакова, Т.Б. Международное гуманитарное право и средства массовой информации [Текст] / Т.Б. Исакова // Учебно - методическое пособие. Тольятти, 2011. - 156 с.

2. Международное гуманитарное право [Электронный ресурс]: // URL: https://w.histrf.ru/articles/article/show/miezhdunarodnoie_gumanitarnoie_pravo.

FAKE NEWS В СМИ

Сивенкова П.В., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

Мы живем в век бурного развития современных информационных технологий, где информация теперь на вес золота. Каждое крупное информационное издание борется друг с другом ради внимания аудитории: в СМИ уже недостаточно просто иметь сайт на просторах Всемирной паутины, необходимо быть в постоянном контакте с аудиторией, а значит присутствовать и в социальных сетях.

Житель цивилизованного государства не представляет жизнь без цифровых технологий, его каждый день окружает информация: интернет, радио, телевидение, книги, журналы, газеты.

В большом информационном потоке на наряду с объективной и проверенной информации, появляется очень много ложной, безграмотной и негативной.

Вследствие восприятия некорректной информации у личности могут наблюдаться следующие последствия (по Е.Е. Прониной): развитие патологических состояний нервной системы и развитие метапатологий. Часть информации носит явно агрессивный характер, и это может влиять на психику реципиента. Опосредованная СМИ-реальность может влиять на убеждения людей и таким образом определять их поведение.

Поэтому, проблема защиты информации является очень актуальной и для государств, и для организаций, и для отдельных людей. Вопрос безопасности — важная часть внедрения новых информационных технологий во все сферы жизни общества.

Информационная безопасность — такое состояние системы СМИ, когда все социальные субъекты: надежно обеспечены полной, достоверной, оперативно поступающей информацией, позволяющей ориентироваться в действительности и принимать оценочные и поведенческие решения; имеют доступ к информационным ресурсам и СМИ в соответствии с их стоимостью и режимом получения; могут знакомиться с различными позициями, точками зрения и оценками общественно значимых явлений и событий.

Информационная безопасность защищает личность, различные социальные группы и сообщества людей от воздействий, способных против их воли менять психические состояния и психологические характеристики человека, менять его поведение и ограничивать свободу выбора.

Обилие фальшивых сообщений, маскирующихся под новости, в последние годы достигло критической отметки. Люди, в большинстве случаев, обращают внимание на острые материалы и пропускают аналитику, совсем не «жареные» факты. К сожалению, это приводит к фейковым новостям.

Понятие «фейк» (от англ. fake – «подделка», «фальшивка», «обман») включает в себя ряд самых разнообразных явлений медиасреды: от поддельных текстов, а также фото-, видео- или аудиозаписей до искусственно созданной по заданию заказчика популярность личности, произведения, проекта (как правило, при помощи интернет-ботов и (или) тех же фальшивых аккаунтов, выставляющих «лайки» и постящих одобрительные комментарии).

Fake news представляет собой ложь от начала до конца. Такая «новость», основанная на непроверенных показаниях лиц, якобы являвшихся свидетелями каких-либо событий и содержит ложь на фоне в целом достоверной информации, представленной выборочно. В ее основе лежат реальные события, отдельные фрагменты которые искажены. Это могут быть, к примеру, измененные в нужном для фальсификаторов русле аудиозаписи, видеозаписи, отредактированные фотографии и цитаты, вырванные из контекста.

Как отличить фейк от настоящей новости?

1. Смотрите на заголовок. Не редко уже в самом заголовке можно рассмотреть фейковую новость. Это очевидный кликбейт — заголовок, который несет искаженный смысл, чтобы увеличить количество просмотров статей. В таких названиях часто используются слова «скандальный» или «невероятный», многоточия, вопросительные и восклицательные знаки, излишне эмоциональные высказывания

2. Проверяйте дату публикации и первоисточник. Фейковые новости не редко выдают старые материалы за свежую новость. Попробуйте перейти по ссылкам к источнику и узнать,

когда действительно была опубликованна новость.

3. Заведомо смотрите у авторитетных ресурсах. Сенсационную новость, опубликованную в одном месте не стоит воспринимать серьезно. Если авторитетные новостные агентства об этом не сообщают, то весьма вероятно, что это фейк.

4. Проверяйте сомнительные фотографии и цитаты. Относитесь критически к подозрительным цитатам. Часто высказывания приписываются людям ошибочно. Точно так же фейковые страницы используют для новости фотографии из другого события или могут быть даже изменить их для определенного сюжета.

Фейковые новости несут опасность, представляя собой этот медиафеномен в современных условиях развития информационных технологий. Если не контролировать распростронения фейковых новостей можно спровоцировать своего рода «информационные теракты» огромной разрушительной силы. Поэтому, в эпоху переизбытка самой разной информации следует «фильтровать» предложенную информацию, применять свое критическое мышление, смотреть на первоисточник информации и опираться только на факты.

Библиографический список

1. Информационная безопасность. Влияние средств массовой информации на здоровье и поведение людей. Компьютерная безопасность. Безопасность в сети Интернет / URL: https://narodna-osvita.com.ua/5078-informacionnaya-bezopasnost-vliyanie-sredstv-massovoy-informacii-na-zdorove-i-povedenie-lyudey-kompyuternayabezopasnost-bezopasnost-v-seti-internet.html

2. Лозовской, Б. Журналистика и средства массовой информации [Электронный ресурс] / Б. Лозовской // URL: https://docplayer.ru/52852127-Boris-lozovskiy-zhurnalistika-i-sredstva-massovoy-informacii-kratkiy-slovar.html

3. Феномен речевого мошенничества [Электронный ресурс] / URL: https://studopedi-a.net/ 6_100268_fenomen-rechevogo-moshennichestva.html

МАССОВО-ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ОСОБЕННОСТИ ЕЕ РАЗВИТИЯ НА СОВРЕМЕННОМ ЭТАПЕ

Труфанова Н.Ю., студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Средства массовой информации в настоящее время играют значительную роль в становлении национальной безопасности, поскольку именно они в первую очередь, предоставляют информацию населению для ее анализа различных ситуаций. Сущностная характеристика массово-информационной безопасности (МИБ) состоит в том, чтобы обеспечивать актуальной, достоверной и полной информацией всех субъектов, кому она нужна для анализа и принятия каких-либо решений, либо синтеза на ее основе новых знаний.

Сегодня такие понятия, как "экономическая безопасность" и "иформационная безопасность" являются базовыми составляющими принятой в стране "Концепции национальной безопасности РФ", а также в таких документах, как "Доктрина информационной безопасности Российской федерации".

Можно заметить, что сегодня через средства массовой информации протекает много дезинформации, ложной или недостоверной информации, отвлекающей, либо, заранее избыточной, скрывающей истинный смысл. В этом аспекте можно говорить о проявлении в сфере массового сознания угрозы национальной безопасности посредством ее манипулирования (через сокрытие или искажение информации, навязывание ложной информации).

Поэтому, можно сделать вывод, что массово-информационная безопасность должна обеспечивать такое состояние системы СМИ и характера ее функционирования, когда все социальные субъекты (государственные органы, негосударственные социальные институты, социальные группы, отдельные граждане) независимо от различных объективных и субъективных препятствий, обеспечены полной, достоверной, оперативно поступающей и актуальной информацией, обеспечивающей информированность населения.

Анализируя множество имеющихся в стране средств, в частности, информационных каналов, по которым распространяется информация, в том числе, и компьютерных каналов связи, отметим следующее:

1. Обеспечение информационной безопасности в средствах МИБ невозможно без знания о потенциальных и реальных опасностях и угрозах, возникающих в процессе их функционирования.

2. Для обеспечения МИБ необходимо наличие в стране соответствующих организационных структур для проведения мониторинга представляемой информации, выявления факторов угроз безопасности и анализа выявленных ситуаций в информационных службах средств массовой информации.

3. Необходимо обеспечение организационных структур соответствующими методиками для оценки рисков возникновения угроз информационной и экономической безопасности, для поступающих сведений через каналы СМИ.

Важнейшим аспектом информационной безопасности сегодня в нашей стране является обеспечение объективности и достоверности информации, получаемой населением посредством информационных передач, передаваемых теле- и радиовещательными организациями. Недостаток информации создает благоприятные условия для манипуляций.

Например, в различных странах выработаны специальные законодательные нормы для телевещателей. Например, в Великобритании действует норма, требующая от частных телерадиокомпаний обеспечения беспристрастности информационного вещания. Беспристрастность программ содержательно интерпретируется как запрет на комментарии в обзорах свежих новостей и документальных передачах, а также обеспечение сбалансированности в освещении жизненно важных событий политического, экономического и социального характера.

Нами выделены ключевые аспекты профессионально-этического кодекса работников медиасферы в разрезе трех базовых принципов (таблица 1).

Таблица 1 - Базовые принципы профессиональных компетенций работников медиасферы

Принцип демократизации	Принцип гуманизации	Принцип объективности и достоверности
Отсутствие "языка вражды", способного привести к возникновению национальной или религиозной вражды	Использование четкого профессионально-понятийного аппарата для явлений, способных вызвать экстремистские волнения среди населения	Отсутствие дескриминации граждан и их групп по определенным критериям

В современной России недостаточно, на наш взгляд, раскрыт вопрос о правовом обеспечении информационной безопасности в массово-информационном пространстве. Например, отсутствует положение о необходимости информационной защиты территориальной целостности России в радио- и телепередачах.

Таким образом, анализ изученных источников показал, что сегодня средства массовой информации претендуют на то, чтобы стать частью власти в стране, от которой будут зависеть происходящие изменения. Именно поэтому проблема ведения информационных войн и создания систем информационной безопасности российского государства является столь актуальной и востребованной на современном этапе.

Библиографический список

1. Указ Президента Российской Федерации от 24 июля 2013 г. № 1753. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». [Электронный ресурс] / URL: http:// www.consultant.ru/ document/cons

2. Резолюция ГА ООН от 20 декабря 2002 г. № 57/295 «Использование информационно-коммуникационных технологий в целях развития». [Электронный ресурс] / URL: http://www. consultant.ru/document/ cons_doc_LAW_121270/ c62807581.

3. Алексенцев, А.И. Сущность, и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность». М., 2007. 176 с.

4. Загинайлов, Ю.Н. Основы информационной безопасности. М.: 2015. с. 45.

5. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. М.: 2015.

6. Поцепцов, Г. Информационные войны. Новый инструмент политики. М., 2015.

СОДЕРЖАНИЕ

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ В СМИ

В е с т н и к
по безопасности

Выпуск двенадцатый

Компьютерная верстка и дизайн О.Ю. Федосеева, И.А. Чиргадзе

Сдано в набор 14.12.2019.
Подписано к печати 16.12.2019.
Формат 60х84/16. Бумага офсетная.
Гарнитура Times ET.
Печать офсетная. Усл. п.л. 16,4.
Тираж 500 экз. Заказ № 147.