Волжский университет имени В.Н. Татищева

ВЕСТНИК ПО БЕЗОПАСНОСТИ

№13 декабрь 2020

В НОМЕРЕ:

ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск тринадцатый

Тольятти 2020

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 тринадцатый. – Тольятти: ВУиТ, 2020. - 112 с.

20-21 декабря 2020 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

© Авторский коллектив, 2020
© Волжский университет имени В.Н. Татищева, 2020

ВНЕСУДЕБНОЕ БАНКРОТСТОВ ФИЗИЧЕСКИХ ЛИЦ

Воровко К.Я., студент
Научный руководитель: Галеева Г.Р., к. ю. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Институт несостоятельности (банкротства) имел свое начало (законодательное закрепление) еще со времен существования свода законов Русская Правда (XI век), в котором содержались правила о несостоятельности купцов[1]. С тех пор законодательство Российской Федерации, регулирующее данный институт, находится в непрерывном развитии и совершенствовании.

Законом, регулирующим в настоящее время вопросы несостоятельности (банкротства) является Федеральный закон РФ от 26 октября 2002 года (в ред. от 31.07.2020) «О Несостоятельности (банкротстве)» (далее Закон о банкротстве).

Важность Института несостоятельности (банкротства) в Российской Федерации заключается в том, что он является одним из основных регуляторов экономических процессов в обществе, который обеспечивает стабильность хозяйственного оборота.

Несмотря на это, стоит отметить, что долгое время нормы закона о банкротстве распространялись лишь на юридических лиц и на индивидуальных предпринимателей. Однако, в период сложный экономический ситуации и граждане (физические лица) сталкиваются с проблемой неплатежеспособности. В связи с этим с 1 октября 2015 года в Российской Федерации введена процедура, которая называется банкротство гражданина, банкротство физических лиц, банкротство должника гражданина (Федеральный закон от 29 июня 2015 г. № 154 ФЗ, (далее Закон о банкротстве физических лиц)). В действительности же, закон о банкротстве физических лиц 2015 года, это глава X в Федеральном законе от 26 октября 2002 г. № 127 ФЗ «О несостоятельности (банкротстве)» (далее Закон «О несостоятельности (банкротстве)»), определяющая: особенности, условия, процедуру, порядок и последствия банкротства физического лица.

Данные дела, о банкротстве физических лиц, разрешаются в арбитражных судах в несколько стадий таких как: подача заявления, рассмотрение заявления, назначение финансового управляющего, процедура реструктуризации, процедура реализации имущества, признание банкротства и списание долгов.

Развитие современной российской экономики осуществляется в условиях сохраняющейся геополитической нестабильности, в связи с чем, в целях социальной поддержки неплатежеспособности граждан, законодателем наряду с процедурой банкротства в общем порядке, была предусмотрена и введена новая процедура, такая как: внесудебное банкротство физических лиц.

В чем же заключается отличие внесудебной процедуры от банкротства в общем порядке? Новая процедура внесудебного банкротства доступна только для граждан с небольшой задолженностью, поэтому она осуществляется в упрощенном порядке без участия суда и арбитражного управляющего, а право на поиск актов, оспаривание сделок и т.д. предоставлено кредиторам.

Гражданин, общий размер денежных обязательств и обязанностей по уплате обязательных платежей которого (без учета предусмотренных абзацем четвертым пункта 2 статьи 4 ФЗ о несостоятельности (банкротстве)), в том числе обязательств, срок исполнения которых не наступил, обязательств по уплате алиментов и обязательств по договору поручительства независимо от просрочки основного должника, составляет не менее пятидесяти тысяч

[1] Хрестоматия по истории отечественного государства и права, X век – 1917 год / Сост.: Томсинов В.А. – М, 2013. С. 13.

рублей и не более пятисот тысяч рублей, имеет право обратиться с заявлением о признании его банкротом во внесудебном порядке, если на дату подачи такого заявления в отношении его окончено исполнительное производство в связи с возвращением исполнительного документа взыскателю на основании пункта 4 части 1 статьи 46 Федерального закона от 2 октября 2007 года N 229-ФЗ "Об исполнительном производстве" (независимо от объема и состава требований взыскателя) и не возбуждено иное исполнительное производство после возвращения исполнительного документа взыскателю[1].

Из этого следует, что закон содержит всего два условия, совокупность которых позволяет гражданину подать заявление о признании его банкротом во внесудебном порядке, такими условиями являются:

- общий размер денежных обязательств и обязанностей по уплате обязательных платежей, в том числе обязательств, срок исполнения которых не наступил, обязательств по уплате алиментов и обязательств по договору поручительства независимо от просрочки основного должника, составляет не менее 50 тысяч и не более 500 тысяч рублей (при этом не учитываются подлежащие применению за неисполнение или ненадлежащее исполнение обязательства неустойки, проценты за просрочку платежа, убытки в виде упущенной выгоды и иные имущественные или финансовые санкции, в том числе за неисполнение обязанности по уплате обязательных платежей);

- на дату подачи заявления в отношении гражданина окончено исполнительное производство в связи с возвращением исполнительного документа взыскателю из-за отсутствия у него имущества, на которое может быть обращено взыскание (независимо от объема и состава требований взыскателя) и после возвращения исполнительного документа взыскателю не возбуждено иное исполнительное производство (п. 1 ст. 223.2 Закона о банкротстве)[2].

В п.2 ст. 223.2 Закона о несостоятельности (банкротстве) указано, что заявление о признании гражданина банкротом во внесудебном порядке подается им по месту жительства или месту пребывания в многофункциональный центр предоставления государственных и муниципальных услуг. При этом в п. 4 ст. 223.2 настоящего ФЗ, гражданин обязан представить список всех известных ему кредиторов, оформленный в соответствии с абзацем четвертым пункта 3 статьи 213.4 ФЗ о несостоятельности (банкротстве).

Многофункциональным центром предоставления государственных и муниципальных услуг (далее по тексту МФЦ) может быть возвращено заявление о признании гражданина банкротом во внесудебном порядке, в таком случае гражданин имеет право повторно обратиться с указанным заявлением не ранее чем через один месяц со дня возврата такого заявления[3].

Возврат гражданину поданного им заявления о признании его банкротом во внесудебном порядке с указанием причины возврата может быть обжалован в арбитражный суд по месту жительства гражданина.

Гражданин вправе подать заявление о признании его банкротом во внесудебном порядке повторно не ранее чем по истечении десяти лет после дня прекращения процедуры внесудебного банкротства в соответствии со статьей 223.5 настоящего Федерального закона или дня ее завершения в соответствии с пунктом 1 статьи 223.6 настоящего Федерального закона.

Важной особенность внесудебного банкротства граждан является бесплатность данной процедуры, связано это с тем, что введение процедуры внесудебного банкротства гражданина изначально задумывалось в целях социальной поддержки неплатежеспособных граждан и возврата их в экономический оборот.

---

[1] Федеральный закон от 26.10.2002 № 127-ФЗ (ред. от 31.07.2020) «о Несостоятельности (банкротстве)» п.1 ст. 223.2.

[2] Сайт статистики дел по банкротству физических лиц в сети Интернет [Электронный ресурс]. – Режим доступа: https://finzdor.ru/ (дата обращения 21.11.2020).

[3] Портал МФЦ Самарской области [Электронный ресурс]. – Режим доступа: https://mfc63.samregion.ru/#city (дата обращения: 22.11.2020).

Как указано в ст. 223.7 ФЗ о несостоятельности (банкротстве) рассмотрение заявления о признании гражданина банкротом во внесудебном порядке в МФЦ, а также включение сведений в Единый федеральный реестр сведений о банкротстве осуществляется без взимания платы.

Таким образом, институт банкротства в целом можно воспринимать, как нечто иное, что послужило началом избавления от пережитков прошлого, таких как каторга, холопство, то есть применявшихся к должникам санкций в давние времена. Однако, в российских условиях, лежащая в основе современной формулировке Федерального Закона № 127-ФЗ концепция, подразумевающая «прощение долгов», может привести к некоему злоупотреблению со стороны должников. Подобная ситуация и конкретно с внесудебным банкротством физических лиц, с одной стороны законодателем достигнуты все цели, вытекающие из формулировки норм, а именно экономическая поддержка граждан и возвращение их в экономический оборот, но с другой стороны, это также может стать поводом для злоупотребления.

Библиографический список

1. О несостоятельности (банкротстве): ФЗ от 26 окт. 2002 г. № 127-ФЗ // Собр. законодательства Рос. Федерации. – 2002. - №43. – Ст. 4190.

2. Постановление Пленума Верховного суда РФ от 13.10.2015 г. № 45 «О некоторых вопросах, связанных с введением в действие процедур, применяемых в делах о несостоятельности (банкротстве) граждан».

3. Хрестоматия по истории отечественного государства и права, X век – 1917 год / Сост.: Томсинов В.А. – М, 2013. 280 с.

4. Сайт статистики дел по банкротству физических лиц в сети Интернет [Электронный ресурс]. – Режим доступа: https://finzdor.ru/ (дата обращения 21.11.2020).

5. Портал МФЦ Самарской области [Электронный ресурс]. – Режим доступа: https://mfc63.samregion.ru/#city (дата обращения: 22.11.2020).

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СОВМЕСТНЫХ ЗАВЕЩАНИЙ СУПРУГОВ В РОССИИ

Ганюшова Е., студент
Научный руководитель: Галеева Г.Р., к. ю. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Правовой институт завещания известен еще со времен Византийской империи, он выступает основанием наследования как в наследственном праве зарубежных сран, так и наследственном праве России.

Традиционно в России завещание рассматривалось как одностороннее (индивидуальное), волевое, самостоятельное распоряжение гражданина на случай смерти своим имуществом в виде односторонней сделки, облеченной в законную форму[1]. Реформирование отечественного наследственного права связано с появлением такого нового для российского законодательства института, как совместное завещание супругов. С 01 июня 2019 года вступил в силу Федеральный закон от 19.07.2018 № 217-ФЗ «О внесении изменений в статью 256 части первой и часть третью Гражданского кодекса Российской Федерации», который ввел в Гражданский кодекс новый правовой институт – совместное завещание супругов[2].

[1]Родионова О.М. Гражданско-правовая сущность совместного завещания супругов // Вестник СГЮА. – 2019. – №5 (130). – С. 99.

[2]Собрание законодательства РФ. – 2018. – № 30. – Ст. 4552.

Как указывается в п. 4 ст. 1118 Гражданского кодекса РФ совместным завещанием признается завещание, совершенное гражданами, состоящими между собой в момент его совершения в браке[1]. В совместном завещании супругов они в праве:

1. по обоюдному усмотрению завещать общее имущество супругов, а равно имущество каждого из них любым лицам;

2. любым образом определить доли наследников в соответствующей наследственной массе;

3. определить имущество, входящее в наследственную массу каждого из супругов, если определение имущества, входящего в наследственную массу каждого из супругов, не нарушает прав третьих лиц;

4. лишить наследства одного, нескольких лиц или всех наследников, не указывая причин такого лишения;

5. включить в совместное завещание супругов иные завещательные распоряжения, возможность совершения которых предусмотрена Гражданским кодексом РФ.

Условия совместного завещания супругов действуют в части, не противоречащей правилам об обязательной доле в наследстве (в том числе об обязательной доле в наследстве, право на которую появилось после составления совместного завещания супругов), а также о запрете наследования недостойным наследниками (ст. 1117 Гражданского кодекса РФ)[2].

Совместное завещание супругов оформляется в письменной форме, только полностью дееспособными супругами с их взаимного согласия на порядок распределения наследственным имуществом. Примечательно, что совместные завещания, согласно п. 5 ст. 1126 ГК РФ, не могут быть закрытыми, а также не могут быть заключены в чрезвычайных ситуациях (п. 4 ст. 1129 ГК РФ)[3]. Кроме того, совместные завещания супругов могут быть удостоверены только нотариусом. Несоблюдение данных требований влечет ничтожность указанных завещаний.

В соответствии с п. 1 и 2 ст. 1125 Гражданского кодекса РФ совместное завещание супругов должно быть предано нотариусу обоими супругами или записано с их слов нотариусом в присутствии обоих супругов[4]. Если совместное завещание написано одним из супругов, то до его подписания оно должно быть полностью прочитано другим супругом в присутствии нотариуса. При удостоверении совместного завещания супругов нотариус обязан осуществлять видеофиксацию процедуры совершения совместного завещания супругов, если супруги не заявили возражения против этого (п. 5.1 ст. 1125 и Гражданского кодекса РФ)[5].

Законодатель наделяет каждого из супругов правом в любое время, в том числе после смерти другого супруга, совершить последующее завещание, а также отменить совместное завещание. В таком случае при удостоверении последующего завещания одного из супругов, распоряжения одного из супругов об отмене совместного завещания при жизни обоих супругов, а также принятия закрытого последующего завещания одного из супругов нотариус обязан направить другому супругу в порядке, предусмотренном законодательством о нотариате и нотариальной деятельности, уведомление о факте совершения таких последующих завещаний или об отмене совместного завещания супругов[6].

Также стоит отметить тот факт, что в случаях, когда супруги заключили брачный договор, в котором установлен раздельный режим на все имущество, очевидно, что совместное завещание не может быть ими составлено.

Совместное завещание супругов утрачивает силу в случае расторжение брака или признания брака недействительным как до, так и после смерти одного из супругов. Кроме того,

---

[1] Собрание законодательства РФ. – 2018. – № 30. – Ст. 4552.

[2] Там же.

[3] Там же.

[4] Там же.

[5] Там же.

[6] Родионова О.М. Гражданско-правовая сущность совместного завещания супругов // Вестник СГЮА. – 2019. – №5 (130). – С. 102.

на основании положений п. 2 ст. 1131 Гражданского кодекса РФ совместное завещание супругов может быть оспорено по иску любого из супругов при их жизни[1]. После смерти одного из супругов, а также после смерти пережившего супруга совместное завещание супругов может быть оспорено по иску лица, права или законные интересы которого нарушены этим завещанием.

В настоящее время тенденция к составлению совместного завещания супругов неуклонно растет. Значительный интерес к совместным завещаниям проявляют именно пожилые пары, которые прожили в браке достаточно долгий отрезок времени и готовы выразить последнюю волю совместно. По мнению многих экспертов, определенное количество граждан заинтересовано именно в форме совместного завещания как способе определить имущественный режим супругов на случай смерти.

Библиографический список

1. Гражданский кодекс Российской Федерации (часть первая) от 26.11.2001 № 146-ФЗ (ред. от 18.03.2019) // Собрание законодательства РФ. – 2018. – № 30. – Ст. 4552.

2. Родионова, О.М. Гражданско-правовая сущность совместного завещания супругов // Вестник СГЮА. – 2019. – №5 (130). – С. 99-103.

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Желюк П.С., студент
Научный руководитель: Карлов В.П., к. ю. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Кто владеет информацией, тот владеет миром. Данную крылатую фразу Натана Ротшильда слышали многие, и она никогда не потеряет актуальности. Информация всегда давала преимущество в борьбе за власть и богатство, а в нашем современном информационном веке, она стала мощным и главным оружием, с помощью которого злоумышленники могут собирать данные и использовать их во вред. В настоящее время, активно возрастает количество атак на персональные данные, тем самым возрастает угроза нарушения прав и законных интересов человека.

Законодательство Российской Федерации в целом регулирует обеспечение прав граждан на частную жизнь и защиту личной информации. Приняты законодательные и иные нормативные акты, но при этом остаются нерешенными некоторые вопросы в этой сфере, так как действующее законодательное регулирование имеет ряд пробелов. Частично это можно объяснить относительной новизной правового регулирования данной сферы, а также стремительным развитием информационных технологий и поправки в законы просто не успевают вноситься.

Российские аналитические компании и крупные исследовательские лаборатории ежегодно публикуют отчеты об утечках данных в сеть. Это связано в первую очередь с проблемами в сфере защиты персональных данных: правовыми, организационно-техническими и финансовыми.

Проблемы правового характера возникли в связи с неоднозначностью положений федерального закона о защите персональных данных, которые по-разному трактуются государственными законодательными и исполнительными органами и операторами. В том числе это относится к самому понятию «персональные данные», месту персональных данных в системе информации ограниченного доступа и др.

Организационные проблемы обусловлены недостаточным уровнем организации сбора, хранения, защиты персональных данных на предприятиях, не имеющих для этого финансо-

[1] Собрание законодательства РФ. – 2018. – № 30. – Ст. 4552.

вых средств. Обычно финансовые и организационные проблемы взаимосвязаны между собой.

В федеральном законе «О персональных данных» проблема их защиты рассматривается только с точки зрения обработки данных. Под обработкой подразумеваются все возможные действия с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение (ч. 3 ст. 3), то есть действия по непосредственной защите данным законом не охватываются (например, снятие и наложение конфиденциальности, хранение сведений для аутентификации и идентификации пользователей электронных порталов и др.). Очевидно, что такая постановка вопроса является слишком узкой, в связи с чем аспекты защиты персональных данных фактически остаются за рамками правового регулирования.

Система защиты персональных данных является комбинацией технических и технологических мер, а также мер по ее организации и администрированию. Общие технологические требования к обеспечению безопасности установлены действующим законодательством, однако в отношении организационных мер в законе ничего не сказано. Тем не менее безопасность информационных систем возможна только в случае эффективной взаимосвязи технической и организационной составляющей. Как отмечается специалистами по информационной безопасности, камнем преткновения любой, даже самой технически совершенной, автоматизированной информационной системы являются профессионализм и ответственность обслуживающего ее персонала. При построении автоматизированных информационных систем необходимо учитывать человеческий фактор и иметь подсистему разграничения доступа к информации. Так как основными причинами нарушения конфиденциальности или массовой утечки персональных данных через Интернет, являются недостаточная компетентность и пренебрежение своими должностными обязанностями, служащими, ответственными за сохранение тайны данных.

Еще одной немаловажной проблемой является отсутствие в УК РФ состава преступления, который бы напрямую касался персональных данных, что делает проблематичным привлечение виновных лиц к уголовной ответственности за преступления в сфере оборота и защиты персональных данных. Предусмотренные УК РФ составы (в том числе ст. 137, 138, 272, 273) носят неопределенный характер и только частично охватывают деяния, нарушающие правила работы в рассматриваемой области. Разобщенность норм, сложности в квалификации преступлений не способствуют эффективному поддержанию законности в сфере охраны персональных данных. Решением данной проблемы может быть введение нового состава преступления, который описывал бы противоправные деяния и предусматривал уголовную ответственность за совершение противоправных деяний с персональными данными гражданина.

Сделаем акцент еще на одной проблеме, связанной с защитой и оборотом персональных данных. Большинство вопросов применения законодательства о персональных данных пересекаются с трудовыми отношениями. Основная проблема в данной сфере касается оборота и защиты персональных данных соискателей, то есть лиц, которые только устраиваются на работу. Специальная правовая регламентация таких процедур в ТК РФ отсутствует.

Закрепленное в п. 4 ст. 86 ТК РФ требование об обязательном согласии работника на обработку своих персональных данных правомочно только в отношении работника, но не соискателя. Данная проблема требует законодательного решения.

Нельзя не отметить проблему правовой грамотности населения в сфере персональных данных. Очень часто сами граждане, не осознавая последствий, добровольно предоставляют свои персональные данные и дают согласие на их обработку третьим лицам. Решением данной проблемы является повышение правовой грамотности населения и квалификации операторов, осуществляющих обработку персональных данных.

Также, следует особо выделить проблему самостоятельной защиты своих личных данных в сети интернет. Сейчас практически у каждого человека есть электронная почта, аккаунты в различных социальных сетях, электронные кошельки и различные банковские при-

ложения, где пользователь вводит определенные данные. А также сами сайты, поисковые системы, приложения и социальные сети осуществляют постоянный сбор информации о пользователях, чтобы анализировать интересы посетителей страниц и их покупательского спроса, изучение целевой аудитории, настройка рекламы. Все это очень удобно на первый взгляд, так как браузеры хранят пароли, введенные данные и поисковые запросы, но в тоже время все эти данные в результате хакерской атаки или при потере электронного устройства станут доступны злоумышленникам. Взлом аккаунта может привести к потери данных, как опубликованных в самом профиле, так и тех, которые находятся во вложениях, которые когда-либо пересылались с помощью данного сервиса, а это могут быть и паспортные данные, и иная важная информация. Тем самым полученная информация может быть использована в мошеннических или других преступных целях.

Чтобы самостоятельно обезопасить свои персональные данные в сети Интернет, нужно придерживаться определенных правил:

- Пароли, как основной способ защиты личных данных в интернете. Сложные пароли, их регулярная смена, надежность их хранения повысят надежность защиты аккаунтов;

- Изучение политики конфиденциальности при установке приложений, расширений браузера, регистрации в социальных сетях, поможет узнать какими личными данными они смогут распоряжаться;

- Разрешение для приложений. Не выдавать автоматических разрешений, следить за тем, какую информацию запрашивает приложение;

- Настройки браузера. Запрет на автоматическое сохранение паролей, так как это повышает риск взлома личных данных, среди которых могут оказаться номера документов и банковских карт, которые вводились на каких-либо сайтах. А также отключение синхронизации между устройствами. При утере телефона все личные страницы и аккаунты станут доступны для посторонних;

- Отключение геолокации. Данные о местоположении пользователя позволяют многое узнать о предпочтениях человека, его хобби, привычках, финансах и социальном статусе;

- Чистка cookies. Файлы cookies - это временные файлы интернета, которые хранятся на устройстве и содержат информацию о сайтах, которые вы посещаете. Благодаря cookies сайты помнят логины, пароли, электронную почту, историю интернет-заказов или состав корзины в интернет-магазине. С помощью cookies можно взломать почтовый ящик и получить доступ к личной информации. Время от времени нужно удалять файлы cookies на компьютере и в смартфоне;

- Осуществлять блокировку рекламы;

- Проверять защищенность соединения при переходе на сайт;

- Не пользоваться общественными сетями Wi-Fi для передачи конфиденциальной информации;

- Соблюдать правила общения в интернете: не отвечать на агрессивные сообщения, так как против вас может вестись кибербуллинг (травля по интернету), занесите пользователей в черный список, обратитесь в техническую поддержку сервиса, делайте скриншоты переписки, содержащей оскорбления и угрозы, чтобы в случае необходимости использовать её как доказательство травли против вас; ограничьте контакты в сети с незнакомыми людьми;

- Проверяйте всю информацию, полученную по электронной почте или в сообщениях социальных сетей и мессенджеров, не сообщайте незнакомым людям и не публикуйте в открытом доступе личные данные.

Таким образом, все вышеперечисленные проблемы свидетельствуют о том, что действующее законодательство нуждается в существенной доработке. Требуются определенные подходы и решения, а также совершенствование правового регулирования в области обработки и защиты персональных данных, которое должно осуществлять государство. Общественность и специалисты в области права и информационной безопасности также должны принимать активное участие в усовершенствовании законодательства в данной области.

Кроме того, сами граждане должны стремиться обеспечивать безопасность своих персональных данных.

Новейшие технологии не только упростили сбор, обработку, хранение, передачу данных, но и создали очевидные угрозы их незаконного оборота, что приводит к нарушениям прав личности. А если государство и граждане будут взаимодействовать, будут созданы условия для повышения правовой грамотности граждан, то будут все предпосылки для того, чтобы качественно усовершенствовать действующее законодательство и решить имеющиеся проблемы.

Библиографический список

1. Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) // СПС «Консультант Плюс».

2. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // СПС «Консультант Плюс».

3. Крюкова, Д.Ю., Мокрецов, Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России / Д.Ю. Крюкова, Ю.В. Мокрецов // Пенитенциарная наука. – 2017.

4. Масалков, А.С. Особенности киберпреступлений инструменты нападения / А.С. Масалков. М.: «ДМК», 2018.

О МЕРАХ БЕЗОПАСНОСТИ, ПРИМЕНЯЕМЫХ ДЛЯ ЗАЩИТЫ СВИДЕТЕЛЯ (ПОТЕРПЕВШЕГО)

Журавлева Д.Д., студент
Научный руководитель: Шутемова Т.В., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Свидетель (потерпевший) имеет право на безопасность в уголовном судопроизводстве, этому праву соответствует обязанность государства в лице его компетентных органов и должностных лиц обеспечить им безопасность.

В Российской Федерации на законодательном уровне меры безопасности свидетеля (потерпевшего) определены в УПК РФ (ст. 11 УПК РФ и др.)[1], а также в ФЗ РФ от 20.08.2004 N 119-ФЗ (ред. от 07.02.2017) "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства"[2].

В рамках выполнения положений указанного Федерального закона Правительством Российской Федерации утверждаются Государственные программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства» (далее — Программа защиты). Первая такая Программа была утверждена на 2006-2008 гг., следующие Программы принимались на 5 лет, соответственно: 2009-2013, 2014-2018, 2019-2023. Рассмотрим кратко эти Программы.

В первой Программе защиты на 2006-2008 гг. отмечалось, что «криминальные группы не стесняются в выборе средств и методов, совершают противоправные деяния, сопровождающиеся особой жестокостью и цинизмом, действуют открыто и нагло, так как уверены в своей безнаказанности. К добросовестным участникам уголовного судопроизводства все чаще применяются изощренные, тщательно спланированные и умело реализуемые приемы физического и психологического воздействия. Результатом этого стали многочисленные случаи

[1] Уголовно-процессуальный кодекс Российской Федерации // СПС «Консультант-плюс».

[2] ФЗ РФ от 20.08.2004 N 119-ФЗ (ред. от 07.02.2017) "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства"// СПС «Консультант-плюс».

отказа и уклонения потерпевших и свидетелей от участия в уголовном судопроизводстве»[1]. Предполагалось, что меры государственной защиты будут применены в отношении свыше 60 тыс. участников уголовного судопроизводства по таким направлениям: личная охрана, охрана жилища и имущества, приобретение для защищаемых лиц специальных средств индивидуальной защиты, связи и оповещения об опасности, обеспечение конфиденциальных сведений о защищаемых лицах, переселение защищаемых лиц на другое место жительства, замену документов, изменение внешности защищаемых лиц, временное перемещение защищаемых лиц в безопасное место, применение дополнительных мер безопасности в отношении защищаемых лиц, содержащихся под стражей или находящихся в местах лишения свободы, применение мер социальной поддержки, научно-исследовательские и опытно-конструкторские работы — при общей сумме 948,72 млн руб.[2]

По итогам реализации этой Программы было установлено, что, в основном, применялись такие меры безопасности, как личная охрана, охрана жилища и имущества и обеспечение конфиденциальности сведений о защищаемом лице. Всего применено 3842 меры безопасности к 3296 участникам уголовного судопроизводства (в том числе, к свидетелям 63,2%, потерпевшим- 23%)[3].

В новой Программе защиты на 2009-2013 годы предполагаемое число защищаемых лиц было снижено до 10 тыс. человек с мерами защиты по тем же направлениям при обшей сумме 1331,36 млн рублей[4]. Результаты применения этой Программы показали, что по сравнению с предыдущими годами число лиц, которыми воспользовались мерами защиты, Б существенно возросло. Так, только в 2012 году защищаемых лиц было более 2800 (на 17% больше, чем в 2011 году), в отношении них было принято более 5600 мер безопасности (на 27% больше, чем в 2011 году). Преимущественно применялись такие меры безопасности, как личная охрана, охрана жилища и имущества и временное помещение в безопасное место[5].

Третья Программа защиты на 2014-2018 годы была рассчитана на применение мер защиты в отношении более 20 тыс. участников уголовного судопроизводства с общей суммой финансирования - 1405,55 млн рублей, распределенной между применением мер безопасности и мер социальной поддержки[6]. В период действия этой Программы в среднем ежегодно меры защиты применялись в отношении от 3,3 до 3,9 тыс. человек, а всего применено более 33 500 мер безопасности, среди которых больше всего использовались такие меры, как личная охрана, охрана жилища и имущества, выдача специальных средств индивидуальной защиты, связи и оповещения об опасности, обеспечение конфиденциальности сведений о защищаемом лице и временное помещение в безопасное место[7].

Ныне действующая Программа зашиты на 2019-2023 годы имеет общее финансирование 1 059 256 ,1 тыс. рублей, большая часть которых (1041316 тыс. рублей) должна исполь-

---

[1] Постановление Правительства Российской Федерации от 10.04.2006 № 200 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2006-2008 годы» // СПС «Консультант-плюс».

[2] Там же.

[3] Там же.

[4] Постановление Правительства Российской Федерации от 02.10.2009 № 792 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2009-2013 годы» // СПС «Консультант-плюс».

[5] Постановление Правительства Российской Федерации от 13.07.2013 № 586 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2014-2018 годы» // СПС «Консультант-плюс».

[6] Там же.

[7] Постановление Правительства Российской Федерации от 25.10.2018 № 1272 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2019-2023 годы» // СПС «Консультант-плюс».

зоваться на применение мер безопасности к защищаемым лицам, которых планируется свыше 20 тыс. человек[1].

Сравнение Программ показывает, что выделяемое финансирование находится, в основном, в пределах 1- 1,5 млрд руб., последние 10 лет эта сумма рассчитана на применение мер защиты примерно к 20 тыс. чел.

Важное значение для осуществления мер защиты имеют такие подзаконные акты Правительства РФ, как Постановление Правительства РФ от 11.11.2006 № 664 (ред. 10.02.2020) «Об утверждении Правил выплаты единовременных пособий потерпевшим, свидетелям и иным участникам уголовного судопроизводства, в отношении которых в установленном порядке принято решение об осуществлении государственной защиты», Постановление Правительства РФ от 27.10. 2006 № 630 (в ред. 10.07.2020) «Об утверждении Правил отдельных мер безопасности в отношении потерпевших, свидетелей и иных участников уголовного судопроизводства», Постановление Правительства РФ от 21.09.2012 № 953 «Об утверждении Правил применения меры безопасности в виде переселения защищаемого лица на другое место жительства в отношении потерпевших, свидетелей и иных участников уголовного судопроизводства», Постановление Правительства РФ от 14.07.2015 № 705 «О порядке защиты сведений об осуществлении государственной защиты, предоставления таких сведений и осуществления мер безопасности в виде конфиденциальности сведений о защищаемом лице».

Приведенное показывает, что в Российской Федерации в настоящее время имеется достаточная нормативная и финансовая основа для применения мер государственной защиты к участникам уголовного судопроизводства, в том числе к свидетелям и потерпевшим.

Между странами СНГ в настоящее время действует Соглашение государств-участников Содружества Независимых Государств о защите участников уголовного судопроизводства от 28 ноября 2006 года.

Библиографический список

1. Постановление Правительства Российской Федерации от 10.04.2006 № 200 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2006-2008 годы» // СПС «Консультант-плюс».

2. Постановление Правительства Российской Федерации от 02.10.2009 № 792 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2009-2013 годы» // СПС «Консультант-плюс».

3. Постановление Правительства Российской Федерации от 13.07.2013 № 586 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2014-2018 годы» // СПС «Консультант-плюс».

4. Постановление Правительства Российской Федерации от 13.07.2013 № 586 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2014-2018 годы» // СПС «Консультант-плюс».

5.Постановление Правительства Российской Федерации от 25.10.2018 № 1272 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2019-2023 годы» // СПС «Консультант-плюс».

6. Уголовно-процессуальный кодекс Российской Федерации // СПС «Консультант-плюс».

7. ФЗ РФ от 20.08.2004 N 119-ФЗ (ред. от 07.02.2017) "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства"// СПС «Консультант-плюс».

[1] Постановление Правительства Российской Федерации от 25.10.2018 № 1272 об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2019-2023 годы» // СПС «Консультант-плюс»

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ПРАВ ИЗБИРАТЕЛЕЙ В РОССИИ

Карлов В.В., магистрант
Научный руководитель: Абалян А.И., к. п. н, доцент
Санкт-Петербургский государственный университет
г. Санкт-Петербург, Россия

Электоральная практика последних лет в России показывает, что избирательные кампании и их результаты приобретают всё более острый и конфронтационный характер. Есть множество примеров, когда политические объединения или сами избиратели требовали признания результатов выборов недействительными и использовали для этого различные механизмы: от жалоб и судов до уличной и протестной активности. Сочетание этих форм защиты избирателями своих прав нередко приводит к желаемому. Например, целый ряд обращений в Центральную Избирательную Комиссию и проведение протестных мероприятий самыми различными политическими силами в связи с неудовлетворённостью ходом проведения муниципальной избирательной кампании в Санкт-Петербурге в 2019 году в итоге привели к тому, что ЦИК признал работу горизбиркома северной столицы неудовлетворительной целых три раза, а Элла Памфилова – глава ЦИК, потребовала с главы городской избирательной комиссии увольнения (поскольку снять его может либо суд, либо он покидает эту должность по своей смерти, либо по увольнению по собственному желанию).

И неудовлетворённость электоральными кампаниями (их проведением, результатами) становится всё более явной и в других регионах. В этой связи особую значимость приобретает проблема защиты прав избирателей и стоит обозреть теоретико-правовую основу данной проблематики.

Самыми главными теоретико-правовыми основами, регулирующие избирательные права российских граждан, являются Конституция РФ, а именно статья 32, а также ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». В нём защита избирательных прав граждан регулируется Главой 10. Кроме того, сюда же можно отнести статьи 141 (воспрепятствование осуществлению избирательных прав или работе избирательных комиссий); 141.1 (нарушение порядка финансирования избирательной кампании кандидата, избирательного объединения, деятельности инициативной группы по проведению референдума, иной группы участников референдума) и ст. 142 (фальсификация избирательных документов, документов референдума), ст. 142.1 (фальсификация итогов голосования) УК РФ.

Специалисты в науке конституционного права выделяют следующие виды ответственности за нарушение избирательных прав: административная и уголовная, иногда также выделяют и конституционно-правовую ответственность [5]. Относят к средствам и методам защиты конституционных прав и свобод, в том числе для защиты избирательных прав конституционно-судебный механизм (конституционный суд); судебная защита (суды общей юрисдикции); административные действия органов исполнительной власти; законная самозащита человеком своих прав; международно-правовой механизм [4]. В связи с тенденцией последних лет, сюда также можно отнести уличные протестные акции (митинги, пикеты, демонстрации).

Под защитой избирательных прав принято понимать принудительный механизм реализации права граждан избирать и быть избранными в органы государственной власти, органы местного самоуправления, их участие в иных избирательных действиях, а также их должностными лицами, иными организациями, устранения препятствий их реализации либо восстановления нарушенного права и иными способами [5].

В рамках судебной защиты прав избирателей, статья 75 ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» гласит, что действия избирательной комиссии, нарушающие избирательные права граждан (например, удаление избирателя с участка для голосования, отказ в выдачи бюллетеня,

требование голосовать вне кабинки или предъявить бюллетень с отметкой, снятие кандидата с выборов без оснований и т.д.) обжалуются в суде, и в зависимости от уровня комиссии зависит то, в какой суд подавать жалобу, а на Центральную Избирательную Комиссию можно подать жалобу только в Верховный суд.

11 пункт 75 статьи также гласит, что жалоба должна быть рассмотрена своевременно, однако до сих пор нигде не указан конкретный срок, в который суд должен её рассмотреть. И зачастую сроки затягиваются и жалобы могут рассматриваться уже после выборов или перед ними самим, что не всегда удовлетворяет заявителя (например, жалоба на безосновательное снятие кандидата с выборов, рассмотренная и удовлетворённая за день до самих выборов, уже не даст кандидату возможности провести агитацию и победить, что делает избирательный процесс и его последствия ещё острее и может привести к локальному политическому кризису).

Представляется, что основным механизмом защиты избирательных прав в России, является пресечение фальсификаций во время голосования и во время подсчёта голосов. На данный момент, это самая распространённая причина подачи жалоб в суды и народного возмущения на площадях. О попытках фальсификаций выборов как на местном, так и на федеральном уровне говорят каждые выборы, но практически никогда за это никто не несёт наказание, а если это и случается, то оно несоразмерно содеянному, поскольку фальсификация выборов, де-факто – узурпация власти, вне зависимости от уровня выборов. Однако, согласно статье 142.1 УК РФ, наказание за данное преступление следующее: штраф в размере от двухсот тысяч до пятисот тысяч рублей, либо принудительные работы на срок до четырех лет, либо лишением свободы на тот же срок. То есть, за попытку захвата власти, максимум можно получить 4 года тюрьмы. При этом наказание понесёт исполнитель, т.е. избирательная комиссия, которая работала с бюллетенями, либо же, в редких случаях, пойманные за руку люди, вбрасывающие бюллетени в урны. Заказчик же уйдёт от ответственности.

В связи с этим представляется, что для более полного и функционирующего механизма защиты прав избирателей следует, во-первых, ужесточить наказание за фальсификацию выборов, приравняв данное деяние к государственной измене и узурпации власти, а во-вторых, ввести дополнительную ответственность заказчика фальсификаций и также ужесточить наказание за данное преступление, в-третьих ввести конкретные сроки рассмотрения жалоб и заявлений в период избирательной кампании, чтобы суды всё делали оперативно и не назначали бы заседания за день до выборов.

Необходимость ужесточения наказания за фальсификацию выборов обусловлено тем, что отдельные личности или организации пытаются нарушить одно из главных прав граждан Российской Федерации – право избирать и быть избранными. Выборы – способ осуществления народом своей власти (ведь по Конституции главным источником власти является именно народ) и управления государством, и значит тот, кто подтасовывает результаты выборов – посягает на сам конституционный строй государства и должен караться как государственный преступник.

В целом, механизм защиты прав избирателей в нашей стране, хоть и имеется, но нуждается в ряде доработок, поскольку от этого зависит стабильность конституционного строя России и это гарант дальнейшего политического развития страны без серьёзных политических кризисов, а потому российским законодателям следует взяться за проработку этого вопроса.

Библиографический список

1. Конституция РФ с изменениями от 01.07.2020.
2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 31.07.2020).
3. Федеральный Закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002.

4. Насыбуллин, А.А. Методы совершенствования административно-правовых средств защиты избирателей https://cyberleninka.ru/article/n/metody-sovershenstvovaniya-administrativno-pravovyh-sredstv-zaschity-prav-izbirateley

5. Тульжанов, Р.С., Архипова, И.И. Правовая защита избирательных прав https://cyberleninka.ru/article/n/pravovaya-zaschita-izbiratelnyh-prav

О МЕРАХ БЕЗОПАСНОСТИ, ПРИМЕНЯЕМЫХ В ОТНОШЕНИИ ЛИЦА, С КОТОРЫМ ЗАКЛЮЧЕНО ДОСУДЕБНОЕ СОГЛАШЕНИЕ О СОТРУДНИЧЕСТВЕ

Сафин И.В., студент
Научный руководитель: Шутемова Т.В., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

С 2009 года в Российской Федерации действует глава 40.1 УПК РФ «Особый порядок принятия судебного решения при заключении досудебного соглашения о сотрудничестве». Появление нового уголовно-процессуального института было обусловлено требованиями усиления борьбы с организованной преступностью, незаконным оборотом наркотиков, коррупцией.

Основные действия по заключению досудебного соглашения о сотрудничестве: заявление подозреваемым (обвиняемым) ходатайства, его рассмотрение следователем и прокурором, непосредственное заключение этого соглашения, выделение уголовного дела в отношении лица, заключившего досудебное соглашение о сотрудничестве, расследование выделенного уголовного дела — осуществляются во время досудебного производства. Размещение же главы 40.1 в части 3 УПК РФ «Судебное производство» связано с особенностями направления этого уголовного дела в суд и особенностями судебного разбирательства по этому уголовному делу, сходными с особенностями судебного заседания согласно положениям главы 40 УПК РФ «Особый порядок принятия судебного решения при согласии обвиняемого с предъявленным ему обвинением».

В досудебном соглашении о сотрудничестве должны быть конкретно указаны те действия, которые подозреваемый (обвиняемый) обязуется совершить, оказывая содействие органам следствия, для изобличения соучастников, для розыска имущества, добытого преступным путем и др. Изобличаемые соучастники из показаний, данных против них, как правило, могут понять, кто именно из их группы это делает, поэтому всегда в такой ситуации перед лицом, которое желает заключить досудебное соглашение о сотрудничестве стоит сложный вопрос: стоит ли ради возможности снижения наказания подвергать опасности себя, своих родных и близких.

Степень угрозы личной безопасности, которой могут подвергаться или подвергались указанные лица, выясняется при проведении предварительного следствия, направлении выделенного уголовного дела в суд и при рассмотрении этого дела в суде (ч. 3 ст. 317.4, п. 4 ч. 1 ст. 317.5, п. 4 ч. 4 ст. 317.7 УПК РФ). Обращение к ст. 11 УПК РФ показывает, что круг угроз не ограничен — это могут быть угрозы убийством, применением насилия, уничтожением или повреждением их имущества либо иными опасными противоправными деяниями (ч. 3). Мы согласны с мнением А.А. Дмитриевой, что угроза причинения вреда правам и интересам защищаемого должна быть реальной, но при этом не ограничиваться перечислением составов преступлений, а может иметь неопределенный характер[1].

Вопросы обеспечения безопасности для такого лица начинают рассматриваться с момента заключения соглашения о сотрудничестве. Защите подлежат не только сам подозреваемый (обвиняемый), его близкие родственники (п. 4 ст. 5 УПК РФ), родственники (п. 37 ст. 5 УПК РФ), но и его близкие лица, к которым закон относит иных лиц, состоящих в свойстве, а

[1]Дмитриева А.А. Теоретическая модель безопасного участия личности в Российском уголовном судопроизводстве: автореферат дисс... доктора юрид. наук. М., 2017. С. 17

также лиц, жизнь, здоровье и благополучие которых дороги в силу сложившихся личных отношений (п. 3 ст. 5 УПК РФ) (далее - защищаемые лица). После вынесения приговора по выделенному уголовному делу осужденный участвует в рассмотрении других уголовных дел, изобличая своих соучастников и этот его процессуальный статус длительное время четко не был определен. Только с введением в 2018 году ст. 56.1 УПК РФ это лицо стало считаться участником уголовного судопроизводства, привлекаемым к участию в процессуальных действиях по уголовному делу в отношении соучастников преступления (ФЗ от 30.10.2018 № 376-ФЗ), с правом ходатайствовать о применении мер безопасности, предусмотренных ч.3 ст. 11 УПК РФ (ч. 2 ст. 56.1 УПК РФ).

Ст. 317.9 УПК РФ не раскрывает меры безопасности, применяемые к защищаемым лицам, а отсылает либо к статьям УПК РФ (ст.ст. 11, 241) либо к законодательству о государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства.

К мерам безопасности, непосредственно указанным в УПК РФ, относятся: сохранение в тайне данных о личности такого лица, использование псевдонимов, помещение документов о личности таких лиц в опечатанные конверты и хранение в условиях, исключающих возможность ознакомления с ними иных участников уголовного судопроизводства (ч. 9 ст. 166, ч. 3 ст. 317.4 УПК РФ), контроль и запись переговоров по письменному заявлению указанных лиц (ч. 2 ст. 186 УПК РФ), проведение опознания в условиях, исключающих визуальное наблюдение опознающего опознаваемым (ч. 8 ст. 193 УПК РФ), проведение закрытого судебного разбирательства (п. 4 ч. 2 ст. 241 УПК РФ), проведение допроса в суде без оглашения подлинных данных о личности в условиях, исключающих визуальное наблюдение допрашиваемого другими участниками судебного разбирательства (ч. 5 ст. 278 УПК РФ).

Федеральный закон от 20.08.2004 N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" (далее ФЗ РФ № 119 — ФЗ от 20.08.2004) содержит перечень мер обеспечения безопасности защищаемых лиц, начиная от личной охраны и охраны жилища до замены документов, переселения в другое место и изменения внешности.

Законодательная регламентация обеспечения безопасности указанных защищаемых лиц, как отмечают многие исследователи, требует более тщательного подхода, исходя из интересов защиты жизни, здоровья и иных личных и имущественных прав защищаемых лиц. Так, стоит согласовать тексты статей 11, 56.1, 317.9 УПК РФ, внести в УПК РФ поводы и основания применения мер безопасности к защищаемым лицам, при этом, как пишет А.А. Дмитриева, «факт заключения досудебного соглашения о сотрудничестве должен рассматриваться как самостоятельный повод к решению вопроса о применении мер государственной защиты, установленных в ФЗ РФ № 119 — ФЗ от 20.08.2004, а также мер уголовно-процессуальной защиты, перечисленных в ч. 3 ст. 11 УПК РФ»[1].

Лицо, заключившее досудебное соглашение о сотрудничестве и выполнившее все обязательства, должно иметь гарантии защиты его самого, близких и иных родственников, близких лиц не только в период следствия, судебного разбирательства, но и во время отбывания наказания и в дальнейшей перспективе — после отбывания наказания. В этой связи права Х.Г. Дациева, говоря о необходимости «разработать комплекс специальных мер, направленных на защиту лица, сотрудничающего со следствием на всех стадиях уголовного процесса, начиная со стадии предварительного расследования, но также и во время отбывания наказания в местах лишения свободы и после отбытия наказания, которые будут закреплены в соответствующих федеральных законах»[2]. Представляется, что такой комплекс мер, подкрепленный законодательно и финансово, будет весомым аргументом при принятии решений о заключении досудебных соглашений о сотрудничестве.

В настоящее время в Российской Федерации действует Государственная программа "Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судо-

[1] Дмитриева А.А. Указ.соч. С. 15.

[2] Дациева Х.Г. Обеспечение безопасности обвиняемого в ходе реализации досудебного соглашения о сотрудничестве //Юридический вестник ДГУ. Т.30. 2019. № 2. С. 143.

производства на 2019 - 2023 годы», утвержденная Постановлением Правительства РФ № 1272 от 25.10.2018. На выполнение Государственной программы в 2020, 2021, 2022 и 2023 годах выделено по 211866,9 тыс. рублей, ожидаемыми результатами ее реализации являются исключение фактов гибели и причинения телесного повреждения или иного вреда здоровью, а также уничтожения (повреждения) имущества защищаемых лиц в связи с их участием в уголовном судопроизводстве; повышение эффективности отправления правосудия[1].

Выполнение целей и задач этой программы зависит от многих факторов, включая качеств уголовно-процессуального законодательства, касающегося мер безопасности защищаемых лиц.

Библиографический список

1. Дациева, Х.Г. Обеспечение безопасности обвиняемого в ходе реализации досудебного соглашения о сотрудничестве // Юридический вестник ДГУ. Т. 30. 2019. № 2. С. 141-145.

2. Дмитриева, А.А. Теоретическая модель безопасного участия личности в Российском уголовном судопроизводстве: автореферат дисс... доктора юрид. наук. М., 2017. 53 с.

3. Постановление Правительства РФ № 1272 от 25.10.2020 «Об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2019-2023 годы» // СПС «Консультант плюс» (дата обращения 11.11.2020).

ПРОБЛЕМЫ КВАЛИФИКАЦИИ НАРУШЕНИЙ ТРЕБОВАНИЙ ПОЖАРНОЙ БЕЗОПАСНОСТИ

Сафин И.В., студент
Научный руководитель: Шутемова Т.В., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

На сегодняшний день при рассмотрении уголовных дел органами предварительного следствия остается проблемным вопрос квалификации преступлений, связанных с нарушением требований пожарной безопасности.

Зачастую помехой этому является сложные и неординарные ситуации, в расследовании которых следственный орган должен быть на высоком уровне и иметь большую практику расследуемых дел.

По статистическим данным в России за 2019 год зарегистрировано 471357 пожаров, в которых погибло 8567 человек, и получили травмы 9477 человек, прямой материальный ущерб составил 18170 млн. рублей. Органами дознания за 2019 год рассмотрено свыше 149,4 тыс. сообщений, что на 14% больше по сравнению с прошлым годом. Возбуждено 981 уголовное дело, то есть на 0,8% больше, чем за прошлый год[2].

Участилась тенденция возникновения пожаров с большим числом жертв, к примеру, трагедия с массовой гибелью людей при пожаре в здании ГУВД в г. Самара, где жертвами стали 57 человек, недавние трагические событии в г. Кемерово ТРЦ «Зимняя вишня», когда погибло 53 человека. Такие трагедии усиливают актуальность изучения проблем о нарушениях требований пожарной безопасности.

Органы предварительного расследования при рассмотрении таких сложных дел сталкиваются с проблемами квалификации преступлений, связанных с нарушением пожарной безопасности, при большом числе смежных преступлений, конкуренции общих и специальных норм права, причем юридическое значение многих правил неопределенно.

[1] Постановление Правительства РФ № 1272 от 25.10.2020 «Об утверждении Государственной программы «Обеспечение безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства на 2019-2023 годы» // СПС «Консультант плюс» (дата обращения 11.11.2020).

[2] Официальный сайт Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий // https://www.mchs.gov.ru/dokumenty/4602

Согласно Федеральному закону РФ «О пожарной безопасности» от 21 декабря 1994 года № 69-ФЗ, пожарная безопасность – это состояние защищенности личности, имущества, общества и государства от пожаров. Этот нормативный акт регламентирует гарантии защиты жизни, здоровья и имущества населения от пожара[1].

В Уголовном кодексе преступления, связанные с пожарами, насчитывают 35 составов, из которых относятся к общим составам преступления, предусмотренные ст. 109, ст. 118, ст. 293 УК РФ, а к специальным - ст. ст. 215-217, 217.1, 218 УК РФ. При этом образуется сложная ситуация, связанная с конкуренцией правовых норм, например, для большого числа общих составов - ст. 219 УК РФ является специальной, тогда как для специальных эта статья является общей[2].

Основным объектом преступления, предусмотренного ст. 219 УК РФ, является сама пожарная безопасность, дополнительным обязательным объектом будет здоровье человека (ч. 1 ст. 219 УК РФ), факультативным - жизнь человека (ч. 2, ч. 3 ст. 219 УК РФ).

В объективную сторону этого преступления входит нарушение требований пожарной безопасности. Действие, связанное с нарушением пожарной безопасности, встречается, например, когда руководитель организации незаконно осуществил при строительстве ликвидацию запасных выходов, а бездействие обычно характеризуется невыполнением предписаний инспектора государственного пожарного надзора о замене средств пожаротушения.

По мнению Г.С. Лиснова, очень важным аспектом является необходимость разграничения этого состава по объективным признакам с нарушениями в смежных отраслях права. Преступление в сфере нарушения пожарной безопасности выражено в осознанных действиях должностных лиц по нарушению как специальных норм, так и норм не совершения действий, необходимых для обеспечения общественной безопасности либо ненадлежащего исполнения своих должностных обязанностей, повлекшим возникновение опасности жизни и здоровью человека[3].

Многие ученые в своих работах предложили законодателю обратить внимание на подход стран СНГ, где причинение крупного имущественного ущерба включено в число обязательных признаков состава.

Признаки субъективной стороны характеризуются как умышленностью, так и по неосторожности. Основная трудность в установлении признаков субъективной стороны состоит в необходимости установить психическое отношение лица не только к деянию, но и к последствиям нарушения требований пожарной безопасности.

Субъект преступления, предусмотренного ст. 219 УК РФ, - специальный, то есть, кроме общих признаков (физическое лицо, вменяемое, достигшее 16 лет), он должен иметь дополнительный признак — на этом лице лежала обязанность по соблюдению требований пожарной безопасности. В соответствии с Постановлением Пленума Верховного Суда РФ от 5 июня 2002 года № 14 «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждения имущества путем поджога либо в результате неосторожного обращения огнем» такими субъектами могут быть руководители организаций и уполномоченными ими лица, имеющие в пользование на праве собственности объекты, в том числе наниматели, арендаторы помещений[4].

---

[1] О пожарной безопасности: Федеральный закон от 21 декабря 1994 г. № 69-ФЗ (ред. от 27 декабря 2019 г.). – URL: http://www.consultant.ru.

[2] Косякова Н.С. Конкуренция уголовно-правовых норм при квалификации пожаров, возникших в результате нарушения требований пожарной безопасности: Журнал Право. Безопасность. Чрезвычайные ситуации. № 2 СПб. 2018 С. 102.

[3] Лиснов П.С. Объективные признаки нарушения требований пожарной безопасности: Журнал Экономика, Политика, Право. Пнз. С. 117.

[4] Постановление Пленума Верховного суда РФ от 5.06.2002 г. № 14 «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждения имущества путем поджога либо в результате неосторожного обращения огнем».

Таким образом, система уголовного права, регулирующая преступления, связанные с нарушением требований пожарной безопасности, не совсем-таки идеальна и имеет очень много вопросов, требующих решения.

Библиографический список

1. Косякова, Н.С. Конкуренция уголовно-правовых норм при квалификации пожаров, возникших в результате нарушения требований пожарной безопасности//Право. Безопасность. Чрезвычайные ситуации. № 2. СПб. 2018. С. 80-86.

2. Лиснов, П.С. Объективные признаки нарушения требований пожарной безопасности // Экономика, политика, право: Актуальные вопросы, тенденции и перспективы развития: Сборник статей VI Международной научно-практической конференции. Пенза. 2020. С. 116-118.

3. О пожарной безопасности: Федеральный закон от 21 декабря 1994 г. № 69-ФЗ (ред. от 27 декабря 2019 г.). //URL: http://www.consultant.ru.

4. Официальный сайт Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий // https://www.mchs.gov.ru /dokumenty/4602.

5. Постановление Пленума Верховного суда РФ от 5.06.2002 г. № 14 «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждения имущества путем поджога либо в результате неосторожного обращения огнем» // URL: http://www.consultant.ru.

АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА О ПРИЕМНОЙ СЕМЬЕ В ЗАРУБЕЖНЫХ СТРАНАХ (СТРАНЫ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ)

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

Анализ законодательства некоторых стран СНГ, регулирующего положение и деятельность приемной семьи, свидетельствует о существовании, как общих черт, так и различий в подходах к правовому регулированию отношений по данному вопросу.

Главной общей чертой является то, что для всех стран приемная семья является одной из приоритетных форм устройства на воспитание детей-сирот и детей, оставшихся без попечения родителей. Приемная семья образуется на основании договора (соглашения) о передачи ребенка на воспитании в семью, который заключается между органами опеки и попечительства и приемными родителями.

Следует отметить, что материальное обеспечение и финансирование содержания детей, переданных на воспитание приемной семье, и заработной платы приемных родителей осуществляется за счет средств республиканского бюджета, что позволяет обеспечить своевременное финансирование приемной семьи. Согласно п. 47. Положения о приемной (фостерной) семье Республики Киргизия[1] и п. 35 и 37 Положения о приемной семье Республики Белоруссия[2] приемным родителям предусматривается ежемесячная заработная плата, размер которой утверждается Правительством данных республик, и выплачивается непосредственно за счет средств республиканского бюджета. В тоже время, в соответствии с п. 29 Положения о приемной семье Приднестровской Молдавской Республики[3], в отличие от вышеназванных республик, устанавливает, что материальное стимулирование труда приемных родителей

[1] Положение о приемной (фостерной) семье от 1 октября 2012 года № 670 [Электронный ресурс] // http://cbd.minjust.gov.kg/act/view/ru-ru/93736

[2] Постановление Совета министров Республики Беларусь 28 октября 1999 г. N 1678 «Об утверждении положения о приемной семье». [Электронный ресурс] // http://www.expert.by/EC/monitorings/27275.txt

[3] Приказ Министерства просвещения Приднестровской Молдавской Республики от 7 октября 2010 года № 1050 "Об утверждении Положения о приёмной семье" [Электронный ресурс] // http://minjust.org/web.nsf/All/28.06.11.

производится за счет средств местных бюджетов в виде ежемесячных выплат денежного вознаграждения в размере, установленном действующим законодательством Приднестровской Молдавской.

В Статье 256-2. СК Украины сказано, что приемные родителями могут быть супруги и лицо, которое не находится в браке, которые взяли для совместного проживания и воспитания детей-сирот и детей, лишенных родительской опеки, за исключением лиц, указанных в ст. 212 СК Украины[1]. Данное определение можно назвать «общим» для всех стран СНГ. Между тем в Положении о приемной семье Республики Белоруссия и Молдавской Республики имеется уточнение, что в первую очередь дети передаются на воспитание в полные семьи, которые имеют постоянный источник доходов.

Кроме того, в основных документах стран СНГ, за исключением Узбекистана, закрепляющих правовое положение приемной семьи, говорится о том, что органы опеки и попечительства, уполномоченные ими органы и организации, организуют в порядке, установленном органами образования, обучение лиц, в отношении которых принято положительное заключение о возможности стать приемными родителями.

Согласно п.1 Положения о принятии детей в семью на воспитание Узбекистана «общее число детей в приемной семье, включая родных и усыновленных, не должно превышать, как правило, 8 человек»[2].

В статье 256-1 Украины установлено, что приемная семья может взять на воспитание и совместное проживание от одного до четырех детей-сирот и детей, лишенных родительской опеки.

Солидарны в данном вопросе законодатели республики Белоруссия и Молдавской Республики, они считают, что общее число детей в приемной семье, включая родных и усыновленных, как правило, не должно превышать, 4 человек.

Промежуточное «положение» в этом вопросе занимают киргизские законодатели, по их мнению, в приемную семью может быть взято на воспитание до 3 детей в возрасте до 16 лет. При этом общее число несовершеннолетних детей, включая родных, усыновленных и подопечных, не должно превышать 5 детей.

Сходством в нормах, которые предусматривает законодательство Республики Белоруссия и Молдавской Республики, является следующее:

1. При подборе лиц, желающих взять детей на воспитание в приемную семью, орган опеки и попечительства учитывает опыт воспитания ими родных и усыновленных детей и отражает в заключении о возможности быть приемными родителями информацию об уровне воспитанности и социализации родных и усыновленных детей. (п. 7 Положения о приемной семье Белоруссии и п. 8 Положения о приемной семье Молдавской Республики).

2. Орган опеки и попечительства, уполномоченные им органы и организации, определяют число детей, которые могут быть переданы на воспитание в данную приемную семью, очередность и сроки их передачи, продолжительность адаптационного периода ребенка в приемной семье (п. 4 Положения о приемной семье Белоруссии и п. 4 Положения о приемной семье Молдавской Республики).

3. В случае госпитализации приемных родителей либо длительного их отсутствия в семье по иным уважительным причинам в соответствии с законодательством Приднестровской Молдавской Республики орган опеки и попечительства обеспечивает временное устройство ребенка (детей) на воспитание (п. 17 Положения о приемной семье Молдавской Республики). При этом п.19 Положения о приемной семье Белоруссии, в этом случае, предусматривает также возможность заключение договора с другими приемными родителями на время отсутствия основного приемного родителя.

---

[1] СІМЕЙНИЙ КОДЕКС УКРАЇНИ Документ 2947-III, чинний, поточна редакція, підстава - 2475-VIII [Электронный ресурс] // https://zakon.rada.gov.ua/laws/show/2947-14

[2] Постановление Кабинета Министров от 12 апреля 1999 г. № 171 ПОЛОЖЕНИЕ об усыновлении (удочерении) несовершеннолетних детей и принятии детей в семью на воспитание (патронат) [Электронный ресурс] // http://www.minjustuz.ru/ru/section.scm_sectionId=17474&contentId=17282.html

В правовых актах остальных стран СНГ, регулирующих деятельность приемной семьи, данные нормы не предусмотрены.

Отличительной чертой Положения о приемной семье Республики Беларусь можно назвать тот факт, что приемная семья образуется не только на основании договора о передачи ребенка на воспитание в приемную семью, но и трудового договора, который заключается между управлением (отделом) образования местного исполнительного и распорядительного органа и приемным родителем (п. 3 Положения о приемной семье). Стоит отметить, что трудовой договор заключается на срок, который предусмотрен в договоре о передаче ребенка на воспитание в приемную семью.

Согласно п. 31 данного положения трудовой отпуск приемным родителям предоставляется согласно графику трудовых отпусков, который составляется управлением (отделом) образования местного исполнительного и распорядительного органа, заключившим с ними трудовой договор. На период трудового отпуска органы опеки и попечительства организуют летний отдых приемных детей.

Существенные отличия можно проследить в Положении о приемной семье Республики Киргизия.

Во-первых, оно предусматривает следующие виды устройства детей:

- экстренное устройство - на срок от нескольких часов до одних суток, если ребенок находится в опасности или брошен (оставлен) родителями;
- краткосрочное устройство - на срок до одного месяца;
- среднесрочное устройство - на срок до шести месяцев;
- долгосрочное устройство - на срок более шести месяцев;
- периодическое устройство - на несколько дней, на выходные дни, на каникулы (п. 2 Положения о приемной семье).

Отличительной особенностью можно назвать и то, что для ребенка, передаваемого на воспитание в приемную семью, составляется письменный план мероприятий предоставления заботы ребенка. В его основу ложатся результаты оценки потребностей ребенка. В свою очередь, план и связанные с этим мероприятия составляются территориальным подразделением совместно с приемными родителями, по результатам оценки, проводимой до устройства ребенка (п. 12-14 Положения о приемной семье).

В список документов, необходимых для представления заявителем в территориальные подразделения для получения статуса приемного родителя п. 15 Положения о приемной семье включены письменные рекомендации от не менее трех поручителей. Поручителем может быть гражданин Республики Киргизия, который не состоит с кандидатом в приемные родители в родстве и знающий его не менее одного года. Рекомендации собираются сотрудниками территориальных подразделений путем письменного интервьюирования выбранных поручителей.

Можно выделить и тот момент, что при поступлении заявления от лица, который изъявил желание взять ребенка на воспитание, работник территориального подразделения проводит собеседование с кандидатом. К тому же территориальное подразделение должно организовать не менее трех посещений на дому у лица, желающего взять ребенка на воспитание, с целью проведения собеседования со всеми членами семьи, совместно проживающими с кандидатом, выяснить мотивы и причины желания взять ребенка в семью. Причем как минимум одно из таких посещений должно быть незапланированным, т.е. без уведомления кандидата (п. 17 Положение о приемной семье).

В соответствии с ч. 2 ст. 256-3 СК Украины при передаче ребенка в приемную семью необходимо согласие ребенка, если он достиг такого возраста и уровня развития, что может его выразить. Аналогичное правило содержится в норме ч. 2 ст. 135 Семейного кодекса Республики Армения и т. д. Однако, п. 25 Положения о приемной семье Республики Беларусь устанавливает, что при выборе приемной семьи учитывается, «если это возможно, желание подопечного», если ребенок, достиг возраста 10 лет, передача в приемную семью осуществ-

ляется только с его письменного согласия. Такое же условие предусматривает п. 22 Положения о приемной семье Молдавской Республики.

Согласно Положению о приемной семье Украины устройство детей в приемную семью проводится с учетом возраста приемных родителей и детей в законодательстве других стран СНГ, данная норма не предусмотрена. На время достижения обеими приемными родителями пенсионного возраста все приемные дети должны достичь возраста выбытия из приемной семьи. В случае достижения пенсионного возраста одним из приемных родителей время пребывания детей определяется по возрасту младшего из родителей. В некоторых случаях, по соглашению сторон, семья может функционировать и после достижения приемными родителями пенсионного возраста, но не более чем в течение 5 лет.

ПСИХОЛОГО-ПРАВОВАЯ БЕЗОПАСНОСТЬ ЖЕНЩИН И ДЕТЕЙ В УСЛОВИЯХ СОВРЕМЕННОЙ СЕМЬИ

Снегирёва М.В., к. п. н., доцент
Российский государственный профессионально-педагогический университет
г. Екатеринбург, Россия

Современная молодёжь в самое ближайшее время станет основным мобилизационным ресурсом российского общества, от неё ожидают технологического прорыва, высокого профессионализма, трудовой активности, мобильности, творчества. Именно от молодёжи зависит в дальнейшем социально-политическое, экономическое, культурное развитие регионов Российской Федерации, стратегическая безопасность всей страны. Преподаватели вузов сегодня должны чувствовать ритм и нерв времени, понимать тенденции в молодёжной среде, которые могут быть и противоречивыми и не до конца нами, старшим поколением, понятыми. Сегодня нужно искать как традиционные, так и инновационные подходы в работе с молодёжью. Следует использовать, в том числе, информационные технологии, доступность статистики, открытость официальных сайтов государственных и муниципальных органов, умело дополнять теорию практическими навыками, делясь опытом, не уходя при общении от острых проблем, существующих в обществе, которое мы наблюдаем.

Нельзя будет назвать прогрессивным общество, в котором нарастают социальные риски и девиации, где наблюдается дезинтеграция (разложение) семейных отношений. Профессор Б.С. Павлов в монографии «Воспроизводство человеческого потенциала в регионе: теоретические и методические аспекты социально-экономического анализа (на примере Урала)» подчёркивает: «В последние годы в условиях трансформации российского общества всё чаще наблюдаются кризисные явления в семейно-брачных отношениях. Они дают о себе знать в участившихся распадах брачных союзов, обострении семейных конфликтов, росте неблагополучных семей и т.п. Особенно страдают дети. Вообще, уровень семейного благополучия в первую очередь определяется качеством отношений в системе «семья – ребёнок». Семейные конфликты ведут к семейному неблагополучию, при котором, как правило, ребёнок становится разменной монетой во взаимоотношениях родителей. Здесь мы рассматриваем такие феномены семейного неблагополучия, как развод и насилие в семье» [1, с. 319]. Продолжается кризис семьи как социального института и малой группы, что сказывается на моральной атмосфере всего российского общества.

Сегодня в центре общественного внимания психолого-правовая безопасность женщин и детей, в Государственной Думе проходит доработку законопроект о противодействии насилию в семье. То, что проблема давно назрела, говорили многие криминалисты, юристы, правозащитники, обсуждалось это на конференциях и в средствах массовой информации в разных регионах России. К слову, автор ещё в 2007 году на Международной научно-практической конференции «Человеческая жизнь: ценности повседневности в социокультурных программах и практиках» выступала сообщением «Целесообразность принятия закона о предотвращении насилия в семье», а также на Международной научно-практической конфе-

ренции «Семья и будущее России» с сообщением «Насилие в семье – фактор снижения демографического развития современной России».

Некоторые положения тех статей до настоящего времени остаются актуальными. «Финансовые проблемы, отсутствие жилья, низкая заработная плата основной массы работающих, мизерные пособия на детей, неопределённость жизненных перспектив отбивают желание создавать семью и растить собственное потомство. При этом дети бывают бездумно брошены взрослыми на произвол судьбы. Россия, являясь социальным государством, не всегда справляется со своими функциями, не защищает в полной мере семью, женщину, ребёнка, откладывая решение самых острых проблем на далёкое будущее» [2, с. 155]. Хотя, надо признать, материальное положение семей с детьми должно было измениться после выплат, которые предусмотрело Правительство Российской Федерации в последние годы, но события 2020 года, связанные с пандемией, показали недостаточность этих усилий. Трудности не сплачивают семью, а часто разрушают её изнутри, девиантное поведение некоторых членов семьи становится определяющим.

Подчеркнём, о психолого-правовой безопасности женщины и детей можно забыть, если рядом находится близкий, но агрессивный человек. «Девиантное поведение – совершение поступков, которые противоречат нормам социального поведения в том или ином сообществе. К основным видам девиантного поведения относятся, прежде всего, преступность, алкоголизм и наркомания, а также самоубийства, проституция. По мнению Э.Дюркгейма, вероятность девиаций поведения существенно возрастает при происходящем на уровне социума ослаблении нормативного контроля. В контексте теории социализации, к девиантному поведению склонны люди, социализация которых проходила в условиях поощрения или игнорирования отдельных элементов девиантного поведения (насилие, аморальность)» [3]. Если годами общество не реагирует на неблагополучие в семье, то это не с лучшей стороны характеризует само общество, так как проблемы могут нарастать, приобретая необратимый характер. «Девиантное поведение – следствие неудачного процесса социализации личности: в результате нарушения процессов идентификации и индивидуализации человека, такой индивид легко впадает в состояние «социальной дезорганизации», когда культурные нормы, ценности и социальные взаимосвязи отсутствуют, ослабевают или противоречат друг другу. Такое состояние называется аномией и является основной причиной отклоняющегося поведения. Девиантное поведение может принимать самые разные формы» [3]. К сожалению, криминальная хроника показывает эти примеры каждый день, суды во всех регионах России выносят тысячи обвинительных приговоров семейным насильникам.

Педагоги школ и вузов прилагают усилия, проводят с обучающимися беседы просветительского, воспитательного характера. Автор сама вела занятия по дисциплине «Этика и психология семейной жизни», особенно привлекая внимание юношей и девушек к темам: «Ответственное материнство и отцовство», «Профилактика абортов», «Профилактика подростковой беременности», «Радость материнства», «Психологическое сопровождение молодых семей», «Недопустимость насилия в семье», «Социальная поддержка государством семей с детьми» и пр. Но этих усилий недостаточно, так как учебный курс незаметно исчез из школы, а спецкурсов в вузах практически нет. Добрая воля преподавателей, осознающих серьёзность проблем для будущего молодых людей, позволяет им заниматься темой насилия в семье в рамках учебных дисциплин «Административное право», «Уголовное право», «Семейное право», «Правоведение» и др.

О серьёзности проблем и глубине кризиса, а также многолетнем нежелании законодателя решить их в юридическом поле настойчиво говорят политолог Е. Шульман, депутат Государственной Думы О. Пушкина, адвокат А. Паршин, активистка А. Попова и др. Законопроект «О профилактике семейно-бытового насилия в Российской Федерации» был внесён в сентябре 2016 г., до 15 декабря 2019 г. в комиссии пришло от граждан около 11 тысяч отзывов. До настоящего времени работа над законопроектом не завершена, он по-прежнему вызывает горячую общественную полемику. Е. Шульман подчеркивает, что «уровень наси-

лия в обществе зависит от уровня насилия по отношению к самым беззащитным и уязвимым» [4], к их числу относятся и дети.

Ответственное общество через регулирование юридическими нормами обязано обеспечить безопасность всех членов семьи. Подчеркнём, что в семьях чаще всего жертвами становятся женщины, дети и старики. Уповать только на нравственные и религиозные нормы очень опрометчиво, что показывает уголовная статистика. «Особенно остро проблема депривации стоит в семьях, где родители либо не могут, либо не хотят взять на себя ответственность за воспитание детей. Здесь ребёнок сталкивается с явлениями проституции, тунеядства, экстремальным формам асоциального поведения, стяжательства и воровства. Воспитательный потенциал семьи практически сводится к нулю: дети подвергаются различным формам насилия, унижения человеческого достоинства, находятся на грани безнадзорности. Степень депривации в семьях данной группы столь велика, что в детях не только отражается, но и аккумулируются пороки родителей, приобретая агрессивно-коллапсическую, а иногда необратимую форму» [5, с. 409]. К мнению профессора Б.С.Павлова следует прислушаться, так как именно им было подготовлено большое исследование о проблемах становления и развития детских домов в системе института общественного (внесемейного) призрения детей в России. В своей монографии «Детские дома в России: опыт ретроспективно-прогностического анализа (на материалах социологических исследований)» автор рассматривал феномен сиротства как деформированного детства, а также формирование системы учреждений внесемейного воспитания (детские дома, интернаты, усыновление, патронатные семьи). Несмотря на принимаемые государством меры, мы видим консервацию проблемы, а нынешние условия пандемии могут её только усугубить. Безопасность подростков, таким образом, часто не обеспечивается, экономические (занятость, жильё), социальные (учеба, доступность к культурным учреждениям) проблемы не решаются органами государственной власти и местного самоуправления.

В качестве вывода повторяю свои слова, высказанные в 2007 г., которые, к сожалению, не потеряли своей актуальности: «Российское общество должно быть нетерпимо к любым проявлениям насилия и агрессии. Современной России, стремящейся к социально-экономическому росту, необходимо в самое ближайшее время решать острые демографические проблемы. Законодателям и рядовым гражданам нужно понять, что насилие в семье – фактор, снижающий демографическое развитие нашего государства. Подготовив и приняв закон о предотвращении насилия в семье, Федеральному Собранию, Президенту как гаранту Конституции, необходимо тем самым защитить семьи от домашних деспотов, а женщинам и детям предоставить правовую, экономическую и социальную поддержку. Свои усилия должны объединить русская православная церковь, государственные органы (в том числе, правоохранительные), общественные объединения, работа должна вестись планомерно, комплексно, среди всего населения, на всей территории Российской Федерации» [6, с. 251]. Современные правовые механизмы должны обеспечить безопасность членов семьи, а социально-культурная политика страны – смягчить нравы, подчёркивая общечеловеческие ценности.

Библиографический список

1. Павлов, Б.С. Воспроизводство человеческого потенциала в регионе: теоретические и методические аспекты социально-экономического анализа» (на примере Урала) / Институт экономики УрО РАН, Уральский федеральный университет имени Первого Президента России Б.Н.Ельцина. – Екатеринбург: Институт экономики УрО РАН, 2014. – 575 с.

2. Снегирёва, М.В. Насилие в семье – фактор снижения демографического развития современной России. Семья и будущее России: Материалы международной научно-практической конференции (1-2 марта 2007 г.) – Екатеринбург: Уральский гуманитарный институт, 2007. – 237 с.

3. Девиантное поведение. [Электронный ресурс] - Режим доступа: https://17gdp.by/document-3523.html

4. Шульман, Е. «На нас смотрит вся Россия». [Электронный ресурс] - Режим доступа: https://itsmycity.ru/2020-09-14/politolog-ekaterina-shulman-oborbe-zapryamye-vybory-mera-ekaterinburga-prava-lgbt-itradicionnyh-cennostya.

ИСТОРИЯ РАЗВИТИЯ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА О СОБСТВЕННОСТИ СУПРУГОВ

Хорошкина Е.С., студент
Научный руководитель: Галеева Г.Р., к. ю. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Сведения о семейном укладе народов, населявших территорию России до принятия христианства, по замечанию М.В. Антокольской, весьма немногочисленны и отрывочны, но по сохранившимся источникам можно сделать вывод на несколько существовавших способов заключения брака, а также формирования имущественных отношений между супругами. Так, при похищении невеста становилась собственностью мужа, поэтому в отношении нее возникали права скорее вещного, чем личного характера. При купле невесты, и особенно при заключении брака с приданым по соглашению между женихом и родственниками невесты возникали, во-первых, отношения между женихом и этими родственниками, которые несколько ограничивали власть мужа. Во-вторых, появляются уже первые признаки наделения жены личными правами. Естественно, что при таких условиях, не могло идти и речи о каком-либо регулировании вопросов собственности между супругами[1].

С принятием христианства в 988 году происходит рецепция византийского брачно-семейного законодательства: семейные дела были отнесены к компетенции православной церкви. Несмотря на большое влияние византийского права, имущественные отношения супругов в России отличались от имущественных отношений супругов Западной Европы в сторону признания за замужней женщиной большей самостоятельности. Еще в дохристианский период жены имели свое имущество. Так, княгине Ольге принадлежал собственный город, свои места птичьей и звериной ловли.

В сговорной записи при обручении могли устанавливаться условия, которые определяли права и обязанности обоих супругов по вопросу имущества в браке и после его прекращения. Невесте ее родителями или родственниками давалось приданое. Во времена до Петра I дочь не получала наследство после своих родителей, но они должны были ей дать приданое. В случае смерти родителей обязанность выделению приданого дочери переходила на их наследников. А при отсутствии наследников имение переходило к казне, но часть из него выделялась дочерям на приданое.

Относительно того, было ли в то время приданое общесемейным имуществом или раздельной собственностью жены, С.А. Муратова придерживается точки зрения, согласно которой Сборник постановлений церковного собора («Стоглав»), принятый в 1551 году, устанавливал общность имущества супругов, запрещая мужу распоряжаться приданым жены без ее согласия, разрешая при этом им владеть и пользоваться[2].

Еще в древнем памятнике «Вопрошение Кириково» растрата имущества жены считалась тяжким проступком и поводом для развода. В случае смерти жены всё её движимое имущество переходило к детям, а в случае отсутствия детей – к лицам, которые дали приданое. Содержание жены в те времена гарантировалось тем, что муж или свекор дарил имущество и земли для того, чтобы обеспечить ее на случай вдовства.

Значительное влияние на развитие русского семейного права оказал Петр I. Его реформы развернули начало так называемому имперскому периоду семейного права России. С петровских времен приданое жены рассматривается как ее раздельное имущество, которым муж не мог даже пользоваться. В соответствии с Указом 1715 года жене имела право свободно продавать и закладывать свои вотчины без согласия на то мужа.

Вот только в отношении этого права на практике поначалу допускались некоторые колебания. Например, в 1763 году Сенат признал недействительной купчую, данную мужу же-

[1] Антокольская М.В. Семейное право. М., 2006. С. 47.
[2] Муратова С.А. Семейное право. М., 2008. С. 15.

ной, указав, что жена, которая находится под властью мужа, не может спорить против его воли о выдаче купчей. Хоть это противоречие между признанием дееспособности замужней женщины в имущественной сфере и ее подчинением власти мужа сохранилось, общая тенденция развития законодательства была все же направлена на предоставление ей права свободно распоряжаться своим имуществом. Единственным исключением оставалось запрещение жене обязываться по векселю без согласия мужа по Вексельному Уставу 1832 года. Но, не имея права подписывать векселя, замужняя женщина могла свободно выдавать заемные письма.

В ст. 109 Законов гражданских говорилось о том, что «браком не создается общего владения в имуществе супругов, каждый из них может иметь и вновь приобретать отдельную собственность». Согласно ст. 115 жена имела право свободно распоряжаться имуществом, не требуя от мужа дозволительные или верительные письма. Статья 112 разрешала супругам заключать между собой любые сделки. Муж мог распоряжаться имуществом жены только по ее доверенности как обычный представитель.

Необходимо отметить, что брачное законодательство России до самой революции не было светским. Российские законодатели упорно отказывались от проведения реформ, признанных необходимыми всеми ведущими специалистами в области гражданского права.

22 октября 1918 года был принят первый отдельный кодифицированный семейно-правовой акт - Кодекс законов об актах гражданского состояния, брачном, семейном и опекунском праве[1]. В отношении имущества супругов в нем сохранился существовавший ранее режим раздельности, только теперь он был закреплен императивной нормой (ст. 105), в которой говорилось, что брак не создает общности имущества супругов, муж не имеет права пользоваться и управлять имуществом жены и не может получить такого права по брачному договору. Принимая во внимание, что режим раздельности для женщины, не работающей вне дома, не давал никаких прав на имущество семьи, запрещение на его изменение путем заключения брачного договора существенно нарушало интересы таких женщин.

Кодекс 1918 года содержал специальную норму о том, что супруги могут вступать между собой во все дозволенные законом договоры. Однако в соответствии со ст. 106 «соглашения супругов, направленные на умаление имущественных прав жены или мужа, недействительны и необязательны для третьих лиц, так и для супругов, которым предоставлено право в любой момент от их исполнения отказаться».

В связи с императивным регулированием, исключающим возможность изменения законного режима супружеского имущества соглашением сторон, супруги были лишены права выбора для себя модели регулирования имущественных отношений, которая в большей степени соответствовала их общим интересам. Исходя из положений Кодекса 1918 года, положено начало тенденции, которая со временем станет определяющей в российском семейном праве советского периода: законодатель ставит имущественные отношения супругов в неоправданно жесткие рамки, предоставляя им достаточно прав в сфере личных отношений. Опасение перед тем, что возможно злоупотребление правом (например, умаления имущественной свободы женщин) в итоге на практике приводил к еще большему умалению их прав. С помощью договора женщина не могла закрепить за собой право на часть общего имущества семьи, в случае развода ничего не получала.

Режим совместной собственности в советской России впервые появился в 1926 году в Кодексе законов о браке, семье и опеке (КЗоБСО)[2]. Потребность в данной мере заключалась в том, что принцип раздельности не давал женщинам, которые не имели самостоятельного дохода и занимались домашним хозяйством, права на имущество семьи. В связи с тем, что все имущество приобреталось на доходы мужа, то оно считалось его собственностью.

При разработке Кодекса о браке и семье РСФСР от 30 июля 1969 года встал вопрос о том, какой правовой режим супружеского имущества должен быть избран в качестве закон-

[1] Собрание узаконений и распоряжений рабоче-крестьянского Правительства РСФСР. 1918. № 76. С. 818.
[2] Собрание узаконений и распоряжений рабоче-крестьянского Правительства РСФСР. 1926. № 82. С. 612.

ного[1]. Был выбран режим совместной собственности супругов, а также закреплен принцип равенства долей супругов в общем имуществе; появились отдельные нормы о личной собственности каждого из супругов.

С 1985 года в России начинается курс перестроечных реформ, что повлекло внесение изменений в действующее семейное законодательство. Законом от 22 мая 1990 года «О внесении изменений и дополнений в некоторые законодательные акты СССР по вопросам, касающимся женщин, семьи и детства» судам было предоставлено право признавать имущество, нажитое каждым из супругов во время их раздельного проживания при фактическом прекращении брака, собственностью каждого из них[2].

Совместная собственность была признана оптимальной и в Семейном кодексе Российской Федерации (далее - СК РФ) от 29 декабря 1995 года № 223-ФЗ без скольких-нибудь серьезных сомнений[3]. Следует отметить, что в полной мере удовлетворить интересы всех супружеских пар не может ни один правовой режим. Бесполезно пытаться построить порядок, который эту задачу выполнит. Один лишь выход из ситуации – это выбрать в качестве законного порядок, который будет отвечать интересам большинства населения, и в то же время предоставить супругам возможность иначе урегулировать имущественные отношения с помощью брачного договора. В связи с этим условия, существовавшие до принятия СК РФ, нуждались в срочном изменении: законодательство, которое действовало ранее, предусматривало лишь законный режим супружеского имущества и не разрешало возможности с помощью брачного договора его изменения.

Вопрос совместной собственности, как и прежде, отвечает интересам большинства супружеских пар. Несмотря на значительные изменения, которые произошли в последние десятилетия, доход большинства женщин ниже дохода их мужей потому, что женщины должны сочетать профессиональную деятельность с воспитанием детей и ведением домашнего быта. Для женщин режим общей совместной собственности крайне неблагоприятен, так как они на них идет двойная нагрузка – на работе и дома. Женщины вкладывают гораздо больше труда и времени, чем их мужья, а при разделе имущества получают лишь половину. Действующее семейное законодательство позволяет женщинам защититься от данной несправедливости путем заключения брачного договора и избрав для себя иной режим супружеского имущества.

Нельзя не согласиться с Э.А. Абашиным, что введение в повседневную практику понятия «Брачный договор» — «исключительное достижение Семейного кодекса Российской Федерации, объективно отражающее реальность, выраженную в изменении принципиально новых правоотношений»[4].

Библиографический список

1. Абашин, Э.А. Брачный договор. М., 2007. С. 5.
2. Антокольская, М.В. Семейное право. М., 2006. С. 47.
3. Ведомости Съезда народных депутатов и Верховного Совета РСФСР. 1969. № 32. С. 1086.
4. Ведомости Съезда народных депутатов и Верховного Совета СССР. 1990. № 23. С. 422.
5. Муратова, С.А. Семейное право. М., 2008. С. 15.
6. Собрание законодательства Российской Федерации. 1996. № 1. С. 16.
7. Собрание узаконений и распоряжений рабоче-крестьянского Правительства РСФСР. 1918. № 76. С. 818.
8. Собрание узаконений и распоряжений рабоче-крестьянского Правительства РСФСР. 1926. № 82. С. 612.

[1] Ведомости Съезда народных депутатов и Верховного Совета РСФСР. 1969. № 32. С. 1086.
[2] Ведомости Съезда народных депутатов и Верховного Совета СССР. 1990. № 23. С. 422.
[3] Собрание законодательства Российской Федерации. 1996. № 1. С. 16.
[4] Абашин Э.А. Брачный договор. М., 2007. С. 5.

АРХИТЕКТУРА СЕРВЕРНЫХ ПРИЛОЖЕНИЙ

Горбатов Н.Д., студент
Научный руководитель: Плюснина Е.В., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Аннотация: Создание нового продукта всегда связано с риском. И выбор правильной архитектуры — важный шаг на пути успеху. В статье речь идет о видах архитектур приложений. Выделяются и описываются характерные особенности монолитной архитектуры. Описана проблема взаимодействия клиентов с микросервисной системой. Значительное внимание уделяется взаимодействию сервисов и работе с базами данных при использовании микросервисных систем.

Ключевые слова: микросервисы, монолит, архитектура, веб-приложения, архитектура программного обеспечения, база данных.

Корпоративные приложения обычно состоят из трех частей: базы данных (состоящей из множества таблиц, обычно в системе управления реляционными базами данных), клиентского пользовательского интерфейса (состоящего из HTML-страниц и JavaScript, выполняемых в браузере) и серверной части.

Серверное приложение обрабатывает HTTP-запросы, выполняет логику, зависящую от домена, извлекает и обновляет данные из базы данных, а также заполняет HTML представления для отправки в браузер.

При проектировании нового приложения необходимо выбрать архитектуру серверной части приложения, руководствуясь задачами, которые должно решать приложение. Самыми распространенными архитектурами серверных приложений являются монолитная и микросервисная архитектура.

Монолитная архитектура

Монолитное приложение строится как единое целое. Концепция монолитного программного обеспечения заключается в том, что различные компоненты приложения объединяются в одну программу на одной платформе. Все части программного обеспечения унифицированы, и все его функции управляются в одном месте [1].

Монолитная архитектура имеет ряд преимуществ:

1) Простота разработки. В начале проекта гораздо проще начать с монолитной архитектуры.

2) Согласованность. При монолитной архитектуре легко поддерживать согласованность кода, обрабатывать ошибки и т. д.

3) Межмодульный рефакторинг. Единая архитектура облегчает работу в ситуациях, когда несколько модулей должны взаимодействовать между собой или, когда необходимо переместить классы из одного модуля в другой [2].

4) Легкость развертывания. Чтобы внести какие-либо изменения в работающую систему, разработчику достаточно развернуть обновленную версию приложения [3].

Недостатки монолитной архитектуры:

1) Если приложение слишком велико, это создает проблемы при обслуживании и изменении.

2) Размер приложения может замедлить время запуска, сборки и развертывания.

3) При каждом обновлении любой части приложения необходимо развертывать всё приложение целиком.

4) Ошибка в любом модуле (например, утечка памяти) может потенциально вывести из строя всё приложение.

5) Независимо от того, насколько простыми могут показаться начальные этапы разработки, монолитные приложения испытывают трудности с внедрением новых и передовых технологий. Поскольку изменения в языках или фреймворках влияют на все приложение, это требует усилий для тщательной работы с деталями приложения, следовательно, это становится дорого с учетом как времени, так и усилий.

6) Изменения в одной части приложения могут негативно повлиять на другие части приложения.

Микросервисная архитектура

Микросервисы — это тип сервисно-ориентированной архитектуры программного обеспечения, ориентированный на создание ряда автономных компонентов, составляющих приложение. В отличие от монолитных приложений, созданных как единое целое, микросервисные приложения состоят из нескольких независимых компонентов, которые объединены посредством API [4].

Таким образом, каждый сервис представляет собой узко ограниченный, сильно инкапсулированный, слабо связанный, независимо развертываемый и независимо масштабируемый компонент приложения.

Целью микросервисов является достаточная декомпозиция, разделение приложения на слабо связанные сервисы/модули в отличие от монолитных приложений, в которых модули сильно связаны и развертываются как единый большой кусок. Это разделение будет полезно по следующим причинам:

1. Каждый сервис можно развертывать, обновлять, масштабировать, обслуживать и перезапускать независимо от других сервисов в приложении.

2. Микросервисы позволяют применять подход Agile.

3. Гибкость в использовании технологий и масштабируемости.

Различные слабо связанные сервисы развертываются на основе их собственных специфических потребностей, где каждый сервис имеет свою детализированную модель API для обслуживания различных клиентов (веб, мобильные и сторонние API)

Взаимодействие клиента с микросервисами

Размышляя о том, как клиентская часть приложения будет напрямую взаимодействовать с каждым из развернутых сервисов, следует принимать во внимание следующие проблемы:

1. В случае, когда микросервис предоставляет клиенту детализированные API-интерфейсы, клиент должен сделать запрос к каждому микросервису. Может потребоваться несколько циклических обращений к серверу для выполнения запроса. Это может быть еще хуже для мобильных устройств с низким уровнем сети.

2. Различные коммуникационные протоколы (gRPC, REST, AMQP), применяемые в микросервисах, усложняют использование клиентами.

3. Общие функции, такие как аутентификация, авторизация, ведение журнала, должны быть реализованы в каждом сервисе.

4. Вносить изменения в микросервисы, не прерывая клиентское соединение, будет сложно. Например, при объединении или разделении микросервисов может потребоваться изменить способ подключения клиентов к измененным сервисам.

Для решения вышеупомянутых проблем вводится дополнительный уровень, который находится между клиентом и сервером, действуя как обратный прокси. Подобно паттерну фасада из объектно-ориентированного проектирования, он предоставляет единую точку входа для API-интерфейсов, инкапсулирующих базовую архитектуру системы, который называется API шлюзом.

Функциональные возможности API шлюза:

1) Маршрутизация. Инкапсулируя базовую систему и отделяя ее от клиентов, шлюз обеспечивает единую точку входа для клиента для связи с системой микросервисов.

2) Разгрузка. API шлюз консолидирует пограничные функции, а не заставляет реализовывать их каждому микросервису. Такие функции как аутентификация и авторизация, кеши-

рование ответов, балансировка нагрузки, централизованное ведение журнала реализуются на уровне API шлюза.

Паттерн Backend for Frontend (BFF)

Это разновидность паттерна API шлюза. Вместо единой точки входа для клиентов он предоставляет несколько шлюзов на основе клиента. Цель состоит в том, чтобы предоставить индивидуальные API-интерфейсы в соответствии с потребностями клиента, устраняя множество ненужных вещей, вызванных созданием общих API-интерфейсов для всех клиентов.

Базовая концепция BFF - разработка нишевых бэкэндов для каждого пользовательского опыта. Если требования клиентов (IOS клиент, Android клиент, веб-браузер и т. д.) значительно различаются, BFF - хорошее решение.

Обмен данными и коммуникация между сервисами

Еще одной проблемой является передача данных между сервисами. Разные сервисы, ориентированные на различный контекст и цели, могут общаться с помощью разных механизмов. В зависимости от протокола, механизм передачи информации может быть синхронным или асинхронным.

При использовании подхода «запрос-ответ» (синхронном) вызывающему сервису необходимо знать, куда именно нужно отправить запрос, и оба (вызывающий и вызываемый) сервисы должны быть запущены и работать в данный момент. В данном случае хоть протокол и является синхронным, операция может быть асинхронной, когда клиенту не обязательно ждать ответа. Подход «запрос-ответ» включает в себя REST, GraphQL и gRPC (google remote procedure call).

При использовании асинхронного протокола, вызывающему сервису не обязательно знать, куда нужно отправить запрос. Такой подход позволяет отправлять запрос нескольким получателям и более того, если сервис-получатель не работает, он сможет получить сообщение позже. Это особенно важно с точки зрения слабой связи между сервисами и преодоления сбоев приложения. Асинхронные протоколы, такие как MQTT, AMQP, обрабатываются такими платформами как Apache Kafka, RabbitMQ.

Общий механизм в асинхронной коммуникации – это обмен сообщениями и потоковая передача событий.

Сообщение – это элемент данных, который инкапсулирует намерение или действие (что должно произойти) и распространяется через такие каналы, как обмен сообщениями. В очереди сообщения хранятся до тех пор, пока не будут обработаны и удалены. Получатели сообщений ждут прибытия сообщений и реагируют на них, в противном случае они бездействуют.

Событие инкапсулирует изменение состояния (что произошло) и слушатели могут реагировать на это изменение, в момент, когда оно происходит. Производители событий отказоустойчивы и не имеют представления о своих потребителях.

Различают события домена и события изменений. События домена - события, связанные с бизнес-доменом приложения (создан заказ, заказ отправлен). События изменений – события, созданные базой данных, указывающие на изменение состояния [5].

Распределение данных при использовании микросервисной архитектуры

Традиционные монолитные приложения имеют одну общую базу данных, и данные часто используются совместно разными компонентами. С таким дизайном базы данных легко работать, поскольку данные хранятся в одном хранилище. Но такой подход является антипаттерном в случае с микросервисной архитектурой.

При таком подходе возникают проблемы:

1. Традиционный дизайн общей базы данных для нескольких сервисов создает тесную связь и невозможность независимого развертывания изменений сервиса. Если к одной и той же базе данных обращается несколько сервисов, любые изменения схемы необходимо будет координировать между всеми сервисами, что в реальном мире может вызвать дополнительную работу и задержку развертывания изменений.

2. Сложно масштабировать отдельные сервисы, так как придется масштабировать общую базу данных целиком.

3. Повышение производительности сервисов становится проблемой, так как через некоторое время накапливается большое количество данных. Это затрудняет извлечение данных, поскольку нужно объединить несколько таблиц большого размера для получения необходимых данных.

4. В большинстве случаев в качестве монолитной базы данных используется реляционное хранилище. Это ограничивает все сервисы на использование реляционной базы данных. Однако возможны сценарии, в которых некоторым сервисам может лучше подходить другая реализация хранилища.

Одним из подходов к проектированию микросервисной архитектуры является индивидуальная база данных для каждого сервиса. При таком подходе каждый сервис управляет своими данными. Это означает, что никакой другой сервис не может получить прямой доступ к этим данным. Связь или обмен данными возможны только с использованием набора, четко определенного API.

Преимущества индивидуальных баз данных для каждого сервиса:

1. Независимость сервисов. Все сервисы зависят от собственной базы данных. Если все сервисы зависят от одной и той же базы данных, и она выйдет из строя, все сервисы будут отключены.

2. Легкость изменения схемы базы данных. Если несколько команд разрабатывают одну и ту же базу данных, и одна команда решает изменить схему одной из таблиц, то это никак не повлияет на работу остальных сервисов.

3. Некоторые сервисы могут работать более эффективно с другими реализациями баз данных. Например, для некоторых сервисов лучше подойдет база данных «ключ-значение».

Преимущества и недостатки использования микросервисной архитектуры

В использовании микросервисной архитектуры можно выделить следующие преимущества:

1) Такой подход к проектированию решает проблему сложности путем декомпозиции приложения на набор управляемых сервисов, которые гораздо быстрее разрабатываются, и которые гораздо легче понять и поддерживать.

2) Частичное развертывание. Микросервисы позволяют по мере необходимости обновлять приложение по частям. Если нагрузка на модуль возрастает, соответствующий сервис можно масштабировать, не затрагивая остальные. Это позволяет гибко распределять нагрузку и экономить ресурсы. В монолитной архитектуре приходится заново развёртывать приложение целиком, что влечёт за собой куда больше рисков.

3) Доступность. У микросервисов доступность выше в сравнении с монолитом: даже если один сервис недоступен, это не приводит к сбою всего приложения.

4) Мультиплатформенность/гетерогенность. Микросервисы позволяют разным командам/разработчикам использовать разные технологии и языки, в соответствии с решаемыми задачами [2, 6].

5) Независимая разработка. Разные сервисы могут разрабатываться силами разных команд [6].

Сложности использования микросервисной архитектуры:

1) При использовании такой архитектуры часто применяют подход разделенных баз данных. Бизнес-транзакции, которые обновляют несколько бизнес-объектов в приложении, должны обновить несколько баз данных, принадлежащих разным сервисам.

2) Такая архитектура приложения усложняет разработку, так как приложение будет являться распределенной системой. Необходимо выбрать и реализовать механизм взаимодействия сервисов между собой, либо через обмен сообщений, либо через вызов удаленных процедур (RPC).

3) Тестировать приложение намного сложнее, чем в случае с монолитом. Для тестирования одного сервиса потребуется еще запустить сервисы, от которых он зависит.

4) Сложность развертывания и управления распределенной системой, состоящей из различных сервисов, сильно возрастает по сравнению с монолитной системой. Монолитное приложение просто развертывается на наборе некоторого количества серверов за балансировщиками нагрузки. Напротив, микросервисное приложение обычно состоит из большого количества сервисов. Каждый сервис будет иметь несколько экземпляров среды выполнения. И каждый экземпляр должен быть настроен, развернут, масштабирован и отслежен. Так же успешное развертывание приложения микросервисов требует высокого уровня автоматизации.

Заключение

Каждая из представленных архитектур имеет свои преимущества и недостатки, и чтобы определить, какая архитектура подойдет конкретному проекту, нужно проанализировать предметную область, примерный размер приложения и область применения. Например, для старта разработки нового проекта подойдет монолитная архитектура. И по необходимости, при увеличении размера и сложности приложения, можно перейти на микросервисную архитектуру, которая позволит повысить производительность разработки, применить новые технологии и повысить качество продукта в целом.

Библиографический список

1. Лучшая архитектура для MVP часть 1 [электронный ресурс]: - Режим доступа: https://habr.com/ru/company/otus/blog/476024/ (дата обращения: 11.11.2020).

2. Архитектура микросервисов [электронный ресурс]: - Режим доступа: https://habr.com/ru/company/mailru/blog/320962/ (дата обращения: 11.11.2020).

3. Microservices vs Monolithic Architecture [электронный ресурс]: - Режим доступа: https://www.mulesoft.com/resources/api/microservices-vs-monolithic (дата обращения: 11.11.2020).

4. Лучшая архитектура для MVP часть 2 [электронный ресурс]: - Режим доступа: https://habr.com/ru/company/otus/blog/477930/ (дата обращения: 11.11.2020).

5. Microservice Architecture — Communication & Design Patterns [электронный ресурс]: - Режим доступа: https://medium.com/dev-genius/microservice-architecture-communication-design-patterns-70b37beec294 (дата обращения: 11.11.2020).

6. Пара слов в защиту монолита [электронный ресурс]: - Режим доступа: https://habr.com/ru/company/simbirsoft/blog/453932/ (дата обращения: 11.11.2020).

РАССЫЛКА ИНФОРМАЦИОННЫХ ФАЙЛОВ КАК ЧАСТНЫЙ СЛУЧАЙ КИБЕРМОШЕННИЧЕСТВА

Захарчук А.Р., студент, Тарасов Д.А., старший преподаватель
МГТУ имени Н.Э. Баумана
г. Москва, Россия

Согласно Обзору [1] Банка России по отчётности об инцидентах информационной безопасности при переводе денежных средств за 1 и 2 кварталы 2020 года, выросла доля операций по переводу денежных средств, совершенных без согласия клиентов. Проведенный ЦБ анализ показывает, что в условиях пандемии, роста в этой связи числа онлайн-переводов и покупок, отсутствии у граждан опыта противодействия мошенникам, проявилась повышенная уязвимость граждан к методам социальной инженерии.

С начала компьютерной эры мошенничества правоохранительной практике известно достаточно способов хищения (незаконного перевода) денежных средств с банковских счетов, выманивания персональных данных и банковских реквизитов клиентов российских банков.

В данной статье хотелось бы привести и проанализировать на очередном примере способ получения персональных данных клиента банка с целью их дальнейшего неправомерного использования.

Итак, на электронную почту человека с определенной периодичностью приходят аналогичные письма от пользователя, например, «Служба компенсаций» с темой «Без темы» и вложением «Документация о выплате средств # 61689.pdf». Анализ метаданных письма показывает наличие в заголовке стандартных строк, свидетельствующих об участии в отправке письма ресурсов Яндекса:

«**Received: from mxback7q.mail.yandex.net** (localhost [127.0.0.1])
by mxback7q.mail.yandex.net with LMTP id l9BAwbnTc4-CG7jHLUx;
Fri, 25 Sep 2020 19:13:03 +0300
Received: from mxback7q.mail.yandex.net (localhost [127.0.0.1])
by mxback7q.mail.yandex.net (Yandex) with ESMTP id 35E09115E0EBA;
Fri, 25 Sep 2020 19:13:03 +0300 (MSK)
X-Yandex-Internal: 1
Received: from vla5-47b3f4751bc4.qloud-c.yandex.net (vla5-47b3f4751bc4.qloud-c.yandex.net [2a02:6b8:c18:3508:0:640:47b3:f475])
by mxback7q.mail.yandex.net (mxback/Yandex) with ESMTP id SPGG5kozmD-D3G8qSnL;
Fri, 25 Sep 2020 19:13:03 +0300
X-Yandex-Front: mxback7q.mail.yandex.net
X-Yandex-TimeMark: 1601050383.154
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yandex.ru; s=mail; t=1601050383;
bh=VA53tZPXQFbk3rOBdFhKHrRgtP8+Q5RsFManDl+uJoA=;
h=To:From:Date:Message-Id;
b=klNGGXRfSede/G3ZpaGkri1UxoQYtTzVemQK2Wz8n2h7zurZJmnQoDiNrCGrNza8V
jP+ipRGmmg0+LvGUtkk/9yg2R0dtMpNnsIKios5dQ9ol19b3ZNKWUeKOs2NfNJfi1x
SWHKnJVLpQwCyI5g+52XmzzXQzkdNGo2h0Ebx21c=
Authentication-Results: mxback7q.mail.yandex.net; dkim=pass header.i=@yandex.ru
Received: by vla5-47b3f4751bc4.qloud-c.yandex.net (smtp/Yandex) with ESMTPSA id wvrKsjaCLF-D0n8a7uu;
Fri, 25 Sep 2020 19:13:02 +0300
(using TLSv1 with cipher ECDHE-RSA-AES128-SHA (128/128 bits))
(Client certificate not present)…»

Отправитель письма: **monopoly2004@yandex.ru**
Получатель письма: **islam.israilov2012@yandex.com**
В письме имеется вложение - файл формата PDF «Документация о выплате средств # 61689.pdf».

PDF представляет собой многопотоковый файл, в который могут быть включены практически любые объекты и метаданные. Структура PDF-документа состоит из: заголовка, тела, таблицы перекрестных ссылок (xref table), завершающей части.

Первая строка в ПО FileTypeVerificator указывает на версию, при помощи которой был создан PDF-файл. В данном случае %PDF-1.4 означает, что файл был создан в четвертой версии (рисунок 1).

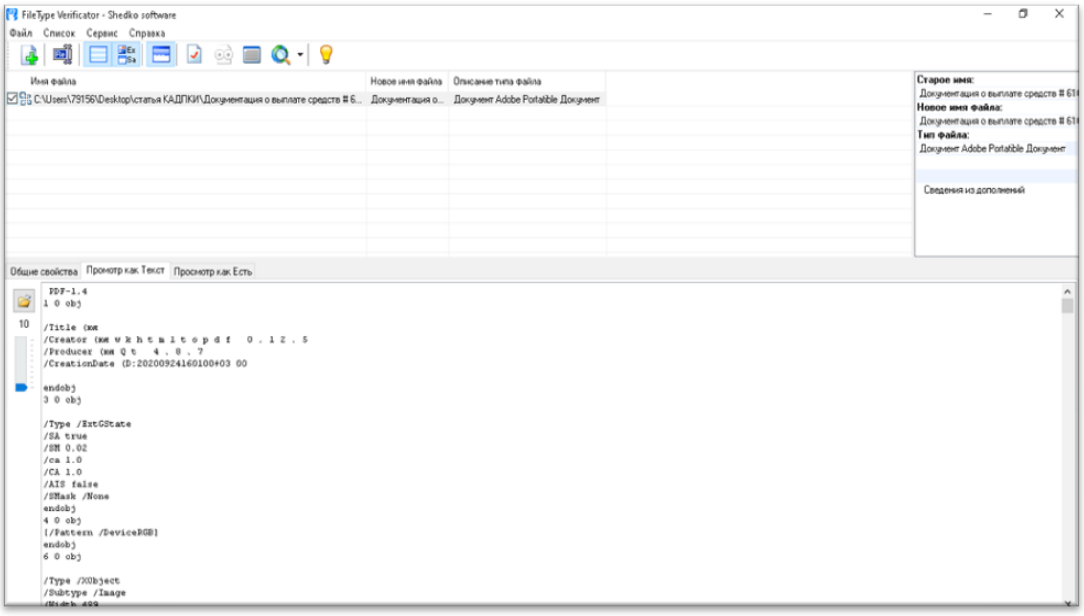

Рисунок 1 - PDF-документ в FileTypeVerificator

В ПО «FileTypeVerificator» были определены форматы данных, присутствующие в файле: Link («ссылка на сайт»), Font («шрифт»), Page («страница»), Image («изображение»), Text («текст»).

Далее в ПО «FileTypeVerificator» указана таблица перекрестных ссылок (xref table), которая содержит все ссылки на объекты и элементы, поддерживаемые форматом PDF. Кроме того, таблица перекрестных ссылок позволяет просматривать содержимое остальных страниц. Когда пользователь изменяет файл, таблица обновляется автоматически. В завершающей части содержатся ссылки на таблицу перекрестных ссылок, заканчивающейся словом %%EOF, которое означает, что файл закончился.

В программе PDF-Analyzer 5.0 были выведены все доступные метаданные файла. Например, автор файла – eDx14031, файл создан 24.09.2020 / 16:01:00 (рисунок 2). Подтвердилось, что файл имеет изображение и активную ссылку на сайт.

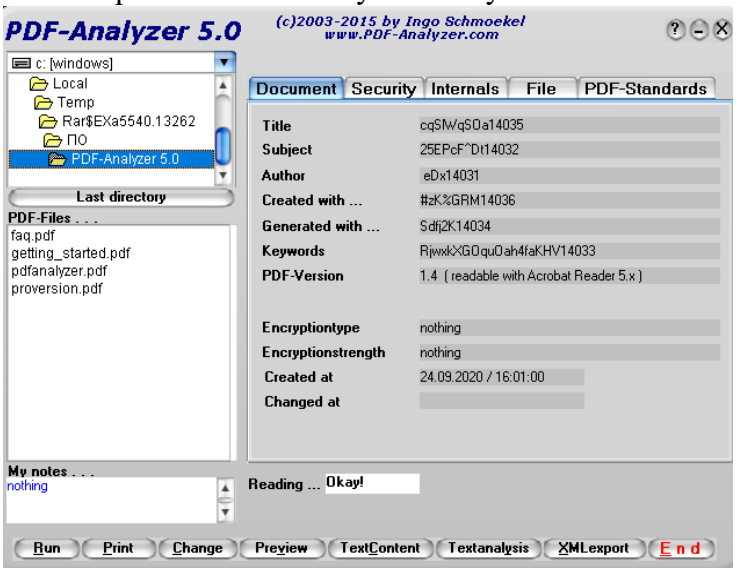

Рисунок 2 - PDF-документ в PDF-Analyzer 5.0

С помощью «PDF Mate Converter» были выделены данные внутри файла: изображение, представляющее собой некое уведомление о компенсации денежных средств и HTML данные. После анализа PDF-документа можно сделать вывод о его структуре и содержащихся

внутри файлах. В данном случае было выяснено, что документ содержит изображение и ссылку на сайт. Проанализируем ее.

В структуре файла «Документация о выплате средств # 61689.pdf» содержится активная: **https://tinyurl.com/y4bjwa9j** (один из известнейших сервисов сокращения ссылок), переход по которой происходит при нажатии на содержащееся в файле изображение (рисунок 3).

Рисунок 3 – Страница сайта

Сайт содержит несколько частей: название – «Официальный компенсационный центр возврата невыплаченных денежных средств», форму для заполнения, указание на постановление, условия выплаты денежных средств, раздел с «важными новостями» и комментарии граждан, получивших компенсацию.

На сайте Федеральной налоговой службы данная организация не значится, постановление № 34/16325к, на которое ссылается данный сайт, является фейковым - не указан орган, вынесший данное постановление или иная информация, позволяющая проверить достоверность документа.

Форма для заполнения представляет собой окошко, где необходимо ввести ФИО и данные банковской карты (рисунок 4).

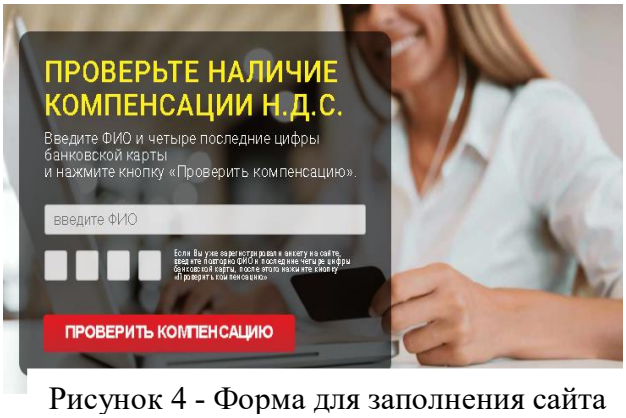

Рисунок 4 - Форма для заполнения сайта

Далее на основании введенных данных «высчитывается» сумма компенсации в размере 270 120 рублей (рисунок 5).

После заполнения более подробной анкеты сайт предлагает получить указанную ранее выплату (рисунок 6).

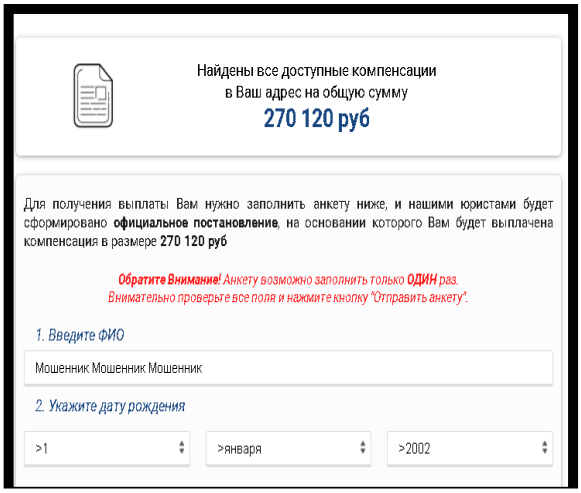

Рисунок 5 – Страница сайта

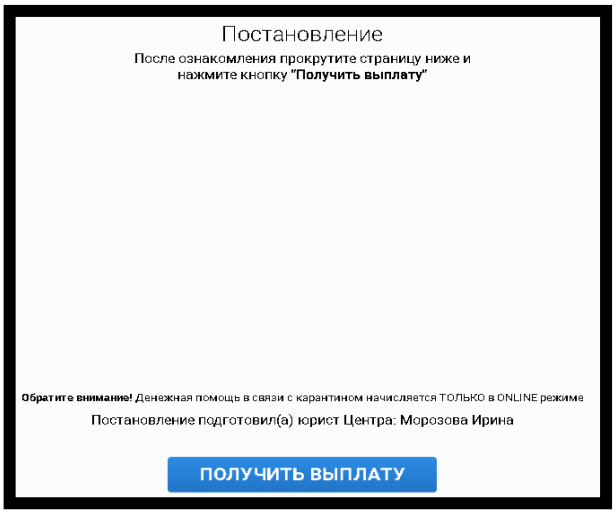

Рисунок 6 – Страница сайта

В конечном итоге предлагается оплатить 365 рублей за добавление записи в единый реестр (рисунок 7).

На основании проведенного анализа сайта можно сделать вывод, что он вероятнее всего является мошенническим. В данном случае, помимо выманивания денежных средств за выплату несуществующей компенсации, не исключено также, что сведения о ФИО, дате

рождения, номере телефона и цифрах банковской карты, введенные пользователем при заполнении анкеты, будут использованы мошенниками при воздействии на потенциальных жертв методами социальной инженерии.

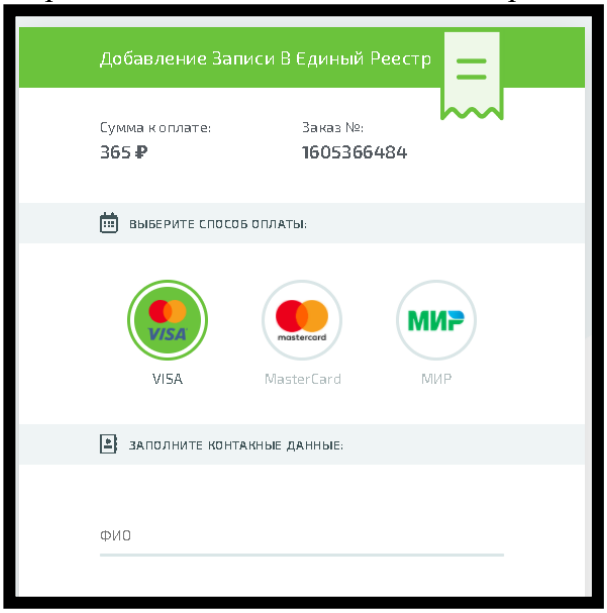

Рисунок 7 – Страница сайта

Таким образом, способы завладения мошенниками денежными средствами и персональными данными граждан в расчёте на их невнимательность и доверчивость не только разнообразны, но и постоянно трансформируются в зависимости от текущей социально-экономической обстановки.

Библиографический список

1. Обзор отчётности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс] // URL: https://cbr.ru/analytics/ib/review_1q_2q_2020 (дата обращения 12.11.2020).

2. Бычков, В.В., Вехов, В.Б. Электронное следообразование преступной деятельности в сети Интернет. // Журнал «Расследование преступлений: проблемы и пути их решения, Изд-во: Московская академия Следственного комитета Российской Федерации, №1 (27), 2020.

3. Вехов, В.Б. Электронная криминалистика в XXI веке: тенденции развития // В сборнике: Криминалистика - наука без границ: традиции и новации. Материалы ежегодной всероссийской научно-практической конференции. Составитель О.С. Лейнова. 2019. С. 51-54.

4. Тарасов, Д.А. Роль специалиста в производстве следственных действий, связанных с обнаружением и изъятием компьютерной информации. // Технико-криминалистическое обеспечение раскрытия и расследования преступлений. Сборник материалов Всероссийской научно-практической конференции. Изд-во: Московский университет МВД России имени В.Я. Кикотя, М.: 2011.

ФОРМИРОВАНИЕ ПРЕДСТАВЛЕНИЙ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ О СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВОЗМОЖНЫХ УГРОЗ

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

Проблема обеспечения защиты информации от несанкционированного доступа, умышленного изменения, кражи, уничтожения, негативного психологического воздействия на человека и других преступных действий не теряет своей актуальности, и становится делом не только профессионалов, но и всех граждан [1]. Использование сети Интерне во всех сферах жизни общества приводит к необходимости формирования у пользователей данной сети знаний о способах защиты информации от выше перечисленных угроз.

В ноябре 2019 года нами было проведено исследование представлений пользователей сети Интернет о способах защиты информации от возможных угроз [2]. Мы предположили, что современный человек, зная о существующих правилах, зная, что эти правила нужно соблюдать, тем не менее, эти правила нарушает. Не исключение и правила информационной безопасности.

Для проверки выдвинутой гипотезы нами была разработана анкета при помощи Google-формы и распространена нами через социальные сети, мессенджеры и электронную почту. Участникам исследования было предложено ответить на ряд вопросов по проблеме кибербезопасности. В исследовании приняли участие 146 человек из Российской Федерации и

стран ближнего и дальнего зарубежья. Граждане Российской Федерации составили 73% респондентов, граждане зарубежных стран – 27% соответственно. География участников выглядит следующим образом:

Российская Федерация: Тольятти (29), Москва и Московская область (10), ЯНАО г. Ноябрьск (5), Санкт-Петербург (6), Екатеринбург (3), Челябинск (3), Геленджик (2) Сызрань (1), Казань (1), Оренбург (1), Ростов (1), п. Рыздвянный Ставропольского края (1), Сургут (1) и др.

Украина: ЛНР, Луганская область, г. Луганск (31), Брянка (1), Ровеньки (1).

Дальнее зарубежье: Швеция г. Мальмо (2); Канада: г. Монреаль (1); Австралия: г. Мельбурн (1).

В ходе проведенного исследования 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.

В 2020 году мы продолжили исследование данной проблемы и предположили, что несоблюдение правил кибербезопасности обусловлено следующим:

1. Пользователи знают о существующих угрозах, о способах защиты от этих угроз, но не верят в эффективность этих средств защиты. Например, знают о вредоносном ПО, вирусах, но не верят в эффективность антивирусных программ.
2. Пользователи знают, что есть угроза доступа злоумышленников к личной конфиденциальной информации, но полагают, что данная угроза их не коснется, т.е. недооценивают величину этой угрозы.

Как известно, если у человека уже сложились какие-то взгляды, установки, то переубедить его сложно, а, иногда, и невозможно. Поэтому важно изначально формировать систему знаний об информационной безопасности, положительное отношение средствам защиты информации, и умение эти знания применять на практике в повседневной жизни. Иными словами, безопасное поведение с сети Интернет должно войти в привычку и стать нормой. Начинать это формирование нужно в школе на уроках информатики.

В 2020 году в связи с распространением коронавирусной инфекции обучение во многих школах ведется дистанционно. Мы решили разработать учебный курс по информационной безопасности для дистанционного обучения. При разработке курса нам необходимо было решить две задачи: техническую (на какой платформе разработать и разместить данный курс) и содержательную (сформировать контент).

При формировании контента мы ориентировались на содержание учебника по Информатике для учащихся 10-х классов[4].

В учебный курс были включены следующие темы:

- Основные понятия информационной безопасности.
- Вредоносные программы. Защита от вредоносных программ.
- Шифрование. Современные алгоритмы шифрования.
- Хэширование и пароли.
- Стенография.
- Безопасность в Интернете.

При формировании контента мы учитывали требования к убеждающему тексту. Во-первых, эффективность убеждения зависит от авторитетности коммуникатора. Поэтому нам необходимо было включить информацию от экспертов в области кибербезопасности. Во-вторых, информация должна содержать сведения о тех «страшных» последствиях, которые произойдут, если человек не изменит свою установку и о реальных путях выхода из сложившейся ситуации. Поэтому все тексты курса включают в себя два компонента: описание угрозы и рекомендации по защите от данной угрозы.

Для решения технической задачи мы использовали образовательную платформу и конструктор онлайн-курсов Stepik. Данная платформа позволяет бесплатно конструировать и размещать учебные курсы, а также редактировать их содержание.

Дальнейшее исследование мы планируем вести по пути совершенствования средств и методов защиты информации от киберугроз, а также по пути разработки средств и методов формирования навыков безопасного поведения в сети Интернет.

Библиографический список

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

2. Исаков, Р.О. Кибербезопасность: исследование представлений пользователей сети Интернет о способах защиты информации от возможных угроз // Вестник по безопасности. Выпуск двенадцатый. – Тольятти: ВУиТ, 2019. – С. 21 – 26.

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

4. Поляков, К.Ю. Информатика. Углубленный уровень: учебник для 10 класса: в 2 ч. Ч. 2 \ К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ, 2018. – 304 с.

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

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WEB-САЙТОВ И WEB-ПРИЛОЖЕНИЙ

Кононов Д.Н., студент
Научный руководитель: Плюснина Е.В., старший преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Аннотация: В статье описаны самые распространенные виды атак и различные уязвимости, с помощью которых хакерам удается проникнуть и взломать программный продукт. Актуальность данной тематики обусловлена тем, что, глядя на высокий прогресс в области безопасности систем, все равно многие системы, в том числе сайты и веб-приложения, могут быть взломаны злоумышленниками.

Ключевые слова: уязвимость, защита, защита информации, Dos-атака, сервер, информационная безопасность.

В настоящее время большая часть современных информационных систем создаются в виде Web-сайтов или Web-приложений, поэтому их безопасности надо уделить особое внимание.

Общедоступные веб-приложения интересны хакерам как ресурсы или инструменты заработка. Спектр применения полученной в результате взлома информации широкий: платное предоставление доступа к ресурсу, использование в бот-сетях и т. д. Личность владельца не важна, так как процесс взлома автоматизирован и поставлен на поток. Стоимость информации пропорциональна известности и влиятельности компании.

Разработчики зачастую не уделяют особое внимание полной защите и безопасности созданных сайтов и приложений, хотя она и играет очень важную роль, потому что любой веб-продукт может быть так или иначе подвергнут взлому хакеров. Распространение атак на веб-приложения связаны с двумя основными факторами: халатное отношение к безопасности сайта и низкий порог входа потенциальных злоумышленников.

Первостепенно, нужно уделить внимание безопасности веб-сервера, потому что именно он ответственен за прием и обработку HTTP-запросов от клиентов к веб-продукту. Именно он гарантирует функционирование бесчисленных веб-сайтов по всему миру, а также отвечает за базовые услуги и хранит персональные данные пользователей и посетителей сайта. Защищенность серверов – это одна из самых главных задач любой организации.

Нынче, количество кибер инцидентов стремительно растет. Сейчас производится достаточно большое количество кибератак, причем в основном атаки направлены преимущественно на государственные учреждения, промышленные предприятия, финансовую отрасль и медицинские организации. Это обуславливается тем, что на таких приложениях можно «заработать» большое количество денег или же получить/изменить информацию, которая способна каким-то образом повлиять важные для государства события.

Немало важным моментом является то, что географическое местоположение веб-сервера, совершенно не влияет на его защиту. Совершить атаку на него можно с любой точки мира. Это связано с тем, что Web-серверы в силу своей открытости рассчитаны на передачу информации между пользователями и вследствие этого имеют множество уязвимостей. К примеру, злоумышленник может внести какие-то изменения (модификации) в код HTTP сервера или сервера базы данных, либо самих страниц веб-сайта, поменяв его изначальную функциональность.

Самые частые действия злоумышленников над взломанными веб-продуктами:

– публикация недостоверной информации на сайте;

– получение незаконного доступа к серверам, с секретными сведениями;

– атака базы данных с информацией о владельцах пластиковых карт банка; кража данных, касающиеся номеров счета основных держателей банковской карты, их имен, фамилий, контактной информации, а затем похищение крупного количества денег;

– создание вирусов, для взлома паролей, использование зараженных устройств для спама или как базы для хранения украденной информации;

– атаки на интернет-сайты государственных учреждений различных стран;

– распространение вирусов, которые приводят к значительному замедлению скорости работы интернета;

– DoS-атаки (Denial of Service— “отказ в обслуживании”) на сеть с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён;

– получение доступа к информации, связанной с технологией SecurID, которая применяется для обеспечения безопасности корпоративных компьютерных сетей (утечка этих сведений может привести к «снижению эффективности» текущей реализации SecurID, что, в свою очередь, может стать основой для осуществления атак на защищенные ресурсы).

Сегодня примерный коэффициент безопасности и надежности сайта можно определить с помощью специальных различных программ, а также специального Web-тестирования. В результате такого тестирования можно заблаговременно оценить безопасность сайта и его уязвимость.

Предположительно, каждый третий сайт отслеживается злоумышленниками. Это довольно досадный и настораживающий факт для каждого разработчика, агентства или владельца сайта. Зная информацию об уязвимостях сайта, можно с легкостью его взломать, поэтому главная задача разработчиков в вопросе о надежности и защите сайта состоит в том, чтобы предотвратить как можно больше этих уязвимостей или хотя бы как следует их спрятать.

Лаборатории по предотвращению различных вирусов больше всего стали уделять внимание разработке средств противодействия DDoS атакам (Denial of Service — «отказ в обслуживании») (рисунок 1).

Так же существует кибершпионаж, т.е. когда злоумышленники не атакуют информационную систему (или сайт), а просто происходит несанкционированное, часто незаконное получение доступа к защищённой информации с различными целями.

Более крупные предприятия подходят к информационной безопасности (ИБ) со значительно большей ответственностью, чем компании малого и среднего бизнеса (СМБ), из-за чего эти компании и страдают больше всех. По статистике, именно у них возникает больше инцидентов в контексте информационной безопасности.

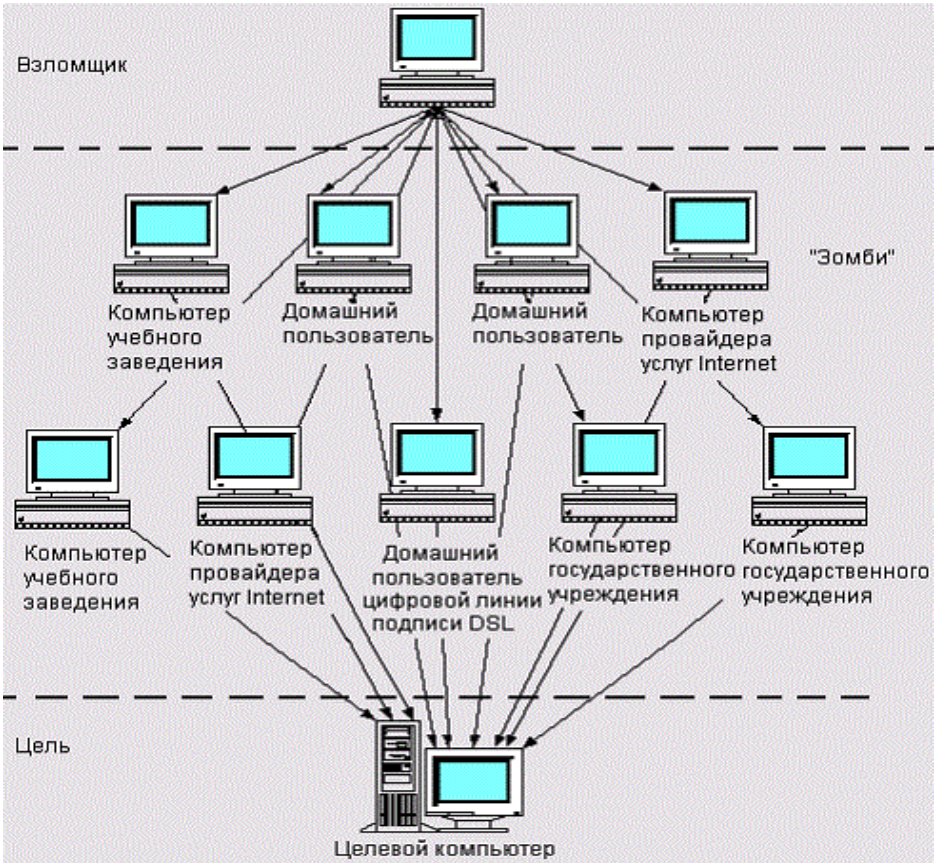

Рисунок 1 - Принцип осуществления Dos-атаки

Согласно исследованию, проведённому в области взломов сайтов, в среднем каждые 39 секунд в сети происходит атака, а используемые незащищенные имена пользователей и пароли дают злоумышленникам больше шансов на успех.

Таблица 1 и рисунок 2 показывают вероятность обнаружения уязвимостей разного уровня риска, обнаруженных в ходе аудитов и автоматического сканирования.

Таким образом, автоматическое сканирование выявляет до 86% сайтов с одной или несколькими уязвимостями среднего (или более высокого) уровня риска (Срочно-Высокий). Методы анализа «черный ящик» и «белый ящик» увеличивают его до 92-98% соответственно.

Эти результаты во многом зависят от того факта, что подробный анализ оценки рисков более адекватен и учитывает не только тип уязвимости, но и ее последствия эксплуатации, а также дизайн и реализацию приложения. Еще одним важным фактом является то, что автоматическое сканирование производилось для сайтов хостинг-провайдеров, которые в некоторых случаях не имеют активного контента, тогда как оценка безопасности обычно проводится для приложений со сложной бизнес-логикой. То есть результаты автоматического сканирования можно интерпретировать как типичные результаты сканирования веб-сайтов, а результаты методов черного и белого ящиков - это результаты сканирования интерактивных корпоративных веб-приложений.

Наиболее распространенными уязвимостями являются межсайтовые сценарии, утечка информации, внедрение SQL, недостаточная защита транспортного уровня, снятие отпечатков пальцев и разделение HTTP-ответа (рисунок 3). Как правило, уязвимости межсайтовых сценариев, внедрения SQL и разделения HTTP-ответа вызваны ошибками проектирования, а утечка информации, недостаточная защита транспортного уровня и снятие отпечатков пальцев часто вызваны недостаточным администрированием (например, контролем доступа).

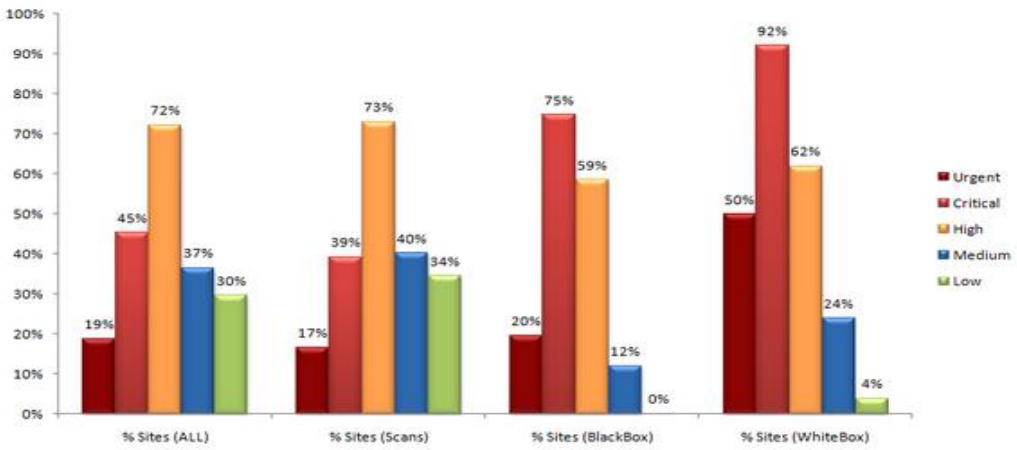

Рисунок 2 - Вероятность обнаружения уязвимостей разного уровня риска

Таблица - 1 Вероятность обнаружения уязвимостей разных классов риска

	ВСЕ	Сканирование	Черный ящик	Белая коробка
Срочно	18,77%	16,70%	19,69%	50,00%
Критический	45,22%	39,25%	74,76%	92,00%
Высоко	72,27%	73,09%	58,51%	62,00%
Средняя	36,56%	40,19%	12,05%	24,00%
Низкий	29,69%	34,45%	0,10%	4,00%
U + C	55,50%	49,40%	79,73%	96,00%
U + C + H	87,66%	86,30%	95,66%	98,84%

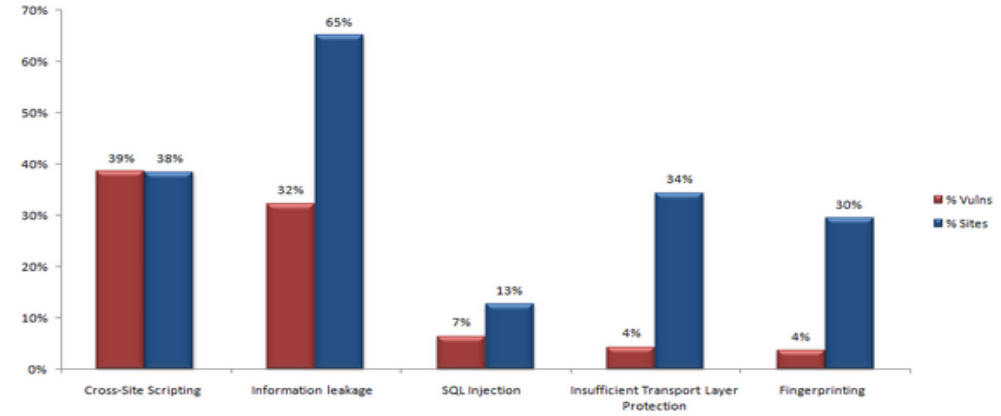

Рисунок 3 - Вероятность обнаружения наиболее распространенных уязвимостей в веб-приложениях

Подробный анализ веб-приложений методами черного и белого ящика показывает, что значительный процент сайтов уязвим для Content Spoofing и Path Traversal (рисунок 4), а вероятность обнаружения уязвимости типа SQL Injection достигает 19%.

При создании нового сайта разработчики могут использовать либо уже существующие платформы CMS (система управления контентом), либо написать все с нуля, но чаще всего малые компании предпочитают пользоваться готовыми инструментами. В действительности же практически в каждой CMS или в скрипте существуют уязвимости. Часть из них опубликована в открытом доступе (публичные уязвимости), другая не доступна широкой аудитории и используется злоумышленниками для целевых атак на сайты. Для того чтобы программная часть сайта была надёжна и неприступна, нужно уделить особое внимание проблеме безопасности.

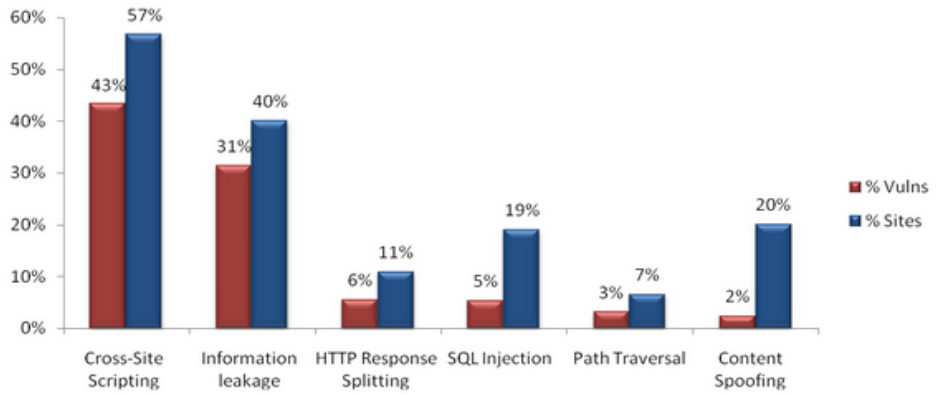

Рисунок 4 - Вероятность обнаружения наиболее распространенных уязвимостей в веб-приложениях (% Сайтов BlackBox и WhiteBox)

Каждый год выходят новые обновления CMS, а вместе с тем возникают новые уязвимости: хотя нужно так же отметить и на то, что старые уязвимости предотвращаются.

Основные функции CMS:

– предоставление инструментов для создания контента и его совместного редактирования;

– управление содержимым: хранение данных, контроль за различными версиями контента, соблюдение режимов доступа, управление потоком материалов и т. п.;

– публикация материалов на сайте;

– представление информации в удобном для чтения виде.

Для проверки сайта на собственных скриптах, можно проверять его доступными средствами поиска уязвимостей (SecurityHeaders, Observatory by Mozilla, One button scan, CSP Evaluator, SSL Server Test, ASafaWeb, Snyk). Так же можно проверить исходный код сайта с помощью приложений и фреймворков (OpenVAS, OWASP Xenotix XSS Exploit Framework, Approof от Positive Technologies) и, при обнаружении уязвимости, исправить её. Кроме регулярных обновлений скриптов и CMS есть ещё один важный момент, усиливающий безопасность и надёжность скриптов — это правильная конфигурация сайта.

Правила правильного конфигурирования сайта:

– грамотно распределить права доступа к файлам

– закрыть доступы к внутренностям сайта (каталогам с резервными копиями, конфигурационным файлам и пр.)

– запретить выполнение скриптов в директориях загрузки

– поставить дополнительную защиту на вход в панель администратора и др. Данные меры позволяют значительно снизить вероятность взлома сайт, даже при наличии уязвимостей в программной части.

– проверять и шифровать пароли

Несмотря на все опасения, не следует считать, что защита веб-сервер не достижимая цель, нужно всего лишь приложить некоторые усилия для обеспечения его безопасности. Для достижения этой цели потребуются совместные действия администраторов веб-сайтов, проектировщиков и программистов, а также нужно помнить, что антивирусное программное обеспечение, операционные системы и права доступа всегда требуют к себе особого внимания.

Внедрение современных средств защиты является неотъемлемой частью мероприятий по обеспечению информационной безопасности.

Обеспечение безопасности веб-ресурса — это процесс, сочетающий в себе определённый набор действий. Сложившаяся система сначала исследуется на предмет безопасности, затем определяется ряд мер и работ, проделываемых для достижения этой безопасности. Это могут быть и услуги программистов, разрабатывающих или оптимизирующих сайт, и услуги инженеров, решающих технические вопросы, и, безусловно, некий набор организационных

мер. Таким образом, главный совет разработчикам и администраторам Web-приложений — неоднократно проверять уровень его надежности и безопасности.

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Мартюшева Н.Ю., студент
Научный руководитель: Третьякова Т.И., ст. преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Большинство web-приложений уязвимы для хакеров. Многие помнят нашумевшие случаи взлома аккаунтов политиков в Twitter. При коммуникации на уровне «клиент – сервер», когда пользователь с ПК или мобильного устройства обращается к серверу, на котором размещено приложение, происходит обмен информацией. При этом не всегда применяются современные способы обеспечения информационной безопасности.

Защита веб-приложений становится задачей и разработчиков, и пользователей. Если несколько лет назад меры защиты ограничивались настройкой веб-сервера, тщательной очисткой жесткого диска от лишних и устаревших файлов и кодов, регулярным контролем за неизменностью файлов, то по мере усиления активности хакеров и учащения DDoS-атак нужны более серьезные меры безопасности.

Понятие

Веб-приложение – это техническое решение, с помощью которого клиент (пользователь) коммуницирует с сервером в режиме реального времени, например, через личный кабинет в электронном банке или страницу в социальной сети.

В формате веб-приложений, работают:

– социальные сети;
– поисковики;
– почтовые клиенты;
– онлайн-программы для бизнеса, выстроенные по модели «клиент – сервер» (CRM-система Bitrix-24 и аналоги);
– интернет-магазины.

Исходя из технических характеристик и модели работы, приложения делятся на следующие типы:

1. **Back-end.** Под этим термином понимается серверная часть программного продукта, установленная на сервере, располагающемся на любом удалении от пользователя. Программа пишется на любом популярном языке программирования – PHP, Python, Ruby, C#.

2. **Front-end.** Этот тип приложения запускается в браузере пользователя. Программа пишется на языке Javascript и от back-end отличается тем, что данные пользователя не хранятся дольше одной сессии. К такому варианту относятся фоторедакторы и игры.

3. **Single-page application.** Этот вариант совмещает клиентскую и серверную версии.

От типа приложения зависит модель угроз, от которых его следует защищать.

Основные угрозы

Злоумышленники интересуются способами взлома веб-приложений в различных целях. Взлом учетной записи помогает получить ценный ресурс без оплаты, похитить чужого игрока в популярной игре, изменить контент в Twitter известного политика, использовать аккаунт как участника в бот-сети. Для взломщика обычно не имеют значения персональные данные лица, чей аккаунт взламывается, ему интересен лишь факт доступа к ресурсу.

Особенность взлома ресурсов – он не персонифицирован, а автоматизирован, производится массово при помощи специальных программ. Полученная информация продается или используется в целях взломщика. Владелец ресурса, работающего с клиентами по модели веб-приложения, должен уметь защитить сайт от самых распространенных способов взлома.

Популярные способы защиты

Простые методики защиты приложения от хакеров не требуют серьезных финансовых вливаний и доступны большинству владельцев интернет-магазинов и аналогичных ресурсов.

Среди них самые популярные:

- аудит (превентивная мера);
- использование защищенных протоколов передачи данных;
- применение ПО, обеспечивающего безопасность.

Все способы необходимо применять в комплексе.

Проверка сайта на уязвимости

Прежде чем разрабатывать методику защиты веб-приложения от потенциальных угроз, сайт следует проверить на уязвимости. Проверка проводится ручным или автоматизированным способом. Программы, доступные в платной и бесплатной версиях, протестируют приложение на основные риски. Такие программные продукты существуют в двух вариантах: Black hat, моделирующие действия взломщиков, и White hat, планомерно выявляющие все недочеты системы методом сканирования.

Среди самых эффективных бесплатных инструментов-приложений следует назвать:

- **OpenVAS** сканирует локальные сети на уязвимости;
- **OWASP Xenotix XSS Exploit Framework** проверяет сайт на XSS-уязвимость, – возможность внедрения в веб-страницу вредоносного кода, похищающего данные аккаунтов пользователей и иную информацию. Код внедряется через уязвимости на сервере или устройстве пользователя;
- **Approof от Positive Technologies** изучает конфигурацию веб-приложения и находит лишний или вредоносный код.

Также с аудитом справятся бесплатные онлайн-сервисы:

- **SecurityHeaders.io** проанализирует ответы сервера на запросы и выявит уязвимые места;
- **Observatory by Mozilla** – бесплатный сервис с открытым кодом для выявления брешей в безопасности. Может привлекать ресурсы других сервисов проверки безопасности и добавлять их данные к отчету. Оценивает степень безопасности по шкале от A до F, где F – самый низкий уровень. В 2016 году 91% проверенных сайтов был на уровне F;
- **One button scan** отвечает за сканирование таких элементов сервера, как DNS, HTTP-заголовки, SSL, проверяет на уязвимости используемые сервисы;
- **SSL Server Test** проверяет наличие SSL-уязвимостей;
- **Snyk** проконтролирует наличие уязвимостей в JavaScript, Ruby и Java-приложениях, самостоятельно исправляет недочеты в безопасности. Успешно работает вместе с GitHub-репозиторием.

Платные ресурсы дадут больше возможностей для проверки сервиса на уязвимости, они быстрее обновляются по мере изменения структуры и характера угроз.

По результатам аудита IT-специалист может испытать шок – так много угроз будет выявлено, но не все они одинаково важны или реализуемы, хакеры используют самые простые методы взлома.

После исправления серьезных уязвимостей сканирование следует провести повторно. Закончив автоматическую проверку, можно организовать взлом веб-приложения вручную. Для этого нужно изменить значение запросов POST (отправка данных на ресурс) и GET (запрос данных у ресурса) в HTTP. Лучше использовать прокси-сервер, перехватывающий HTTP-запросы. Также необходимо обойти валидацию данных (проверку соответствия запроса заданным требованиям) и внедрить на сайт SSL-инфекцию, перехватывающую данные пользователей. Если системы мониторинга показывают существенные уязвимости, необходимо усиливать защиту в выявленных областях.

Используя платные или бесплатные ресурсы мониторинга систем безопасности необходимо проверить гипотетическую возможность хакера обойти требования обязательной аутентификации, предусмотренные для некоторых страниц веб-приложения. Для этого нуж-

но использовать такие традиционные способы взлома как смена параметров URL (в частности, ID пользователя) или смена Cookie.

HTTPS

Вторым по популярности способом защитить данные пользователя после идентификации является применение защищенного протокола передачи данных HTTPS. Hyper Text Transfer Protocol Secure защищает информацию о пользователе веб-приложения при помощи шифрования трафика. Он обеспечивает сохранение конфиденциальности и целостности информации, не допуская утечку или подмену данных.

Большинство ресурсов использует технологию давно, это стало хорошим тоном, подтверждающим готовность их владельцев защищать интересы клиентов. Поисковик Google поднимает в выдаче сайты, использующие эту технологию.

HTTPS необходим, если пользователи передают сервису такие сведения, как:

- номера кредитных карт;
- персональные данные;
- адреса страниц, на которые они заходят.

При генерации запроса с формы авторизации применяются cookie-файлы, они подлежат отправке на сервер при каждом запросе. При слабой защите веб-приложения ничего не мешает злоумышленнику перехватить файлы и подделать запрос, получив права пользователя. Применение HTTPS для каждой страницы сайта снизит степень этого риска.

Решить задачу несложно, потребуются следующие шаги:

- сгененировать SSL-сертификат, на некоторых ресурсах это делается бесплатно;
- получить и установить сертификат;
- подключить для веб-приложения поддержку HTTPS.

Дополнительной возможностью после настройки HTTPS станет применение Hyper Strict Transport Security (HSTS). Это опция принудительного использования протокола HTTPS, даже если сервер не поддерживает его применение. Однако и защищенные протоколы не спасут веб-приложение, если само программное обеспечение устарело.

Обновление ПО

Владелец приложения должен держать руку на пульсе обновлений программного обеспечения. Хакеры тестируют все обновления и находят в них уязвимости иногда раньше, чем разработчики. Особенно активно взламываются операционные системы, технологии управления HTTP и системы управления контентом (CMS).

В ситуации, когда сервис установлен на чужом хостинге, задача своевременной замены операционной системы ложится на плечи провайдера. Если хостинг собственный, ОС требуется менять сразу после выхода обновлений. Сайт может работать на операционной системе, предназначенной для этого типа веб-приложений (движка), стороннего производителя, особенно это характерно для интернет-магазинов. Необходимо отслеживать все обновления ПО и устанавливать новую версию сразу после ее выхода. Разработчики оповестят об этом владельца ресурса рассылкой, а наиболее популярные авторы движков, WordPress и Umbraco, сообщают об обновлениях в момент входа в панель управления сайтом.

Web-сайты часто имеют зависимые компоненты (программные модули менеджмента контента). Для управления ими используются менеджеры пакетов, например, Composer, NPM или RubyGems. За их обновлениями во избежание проблем безопасности также необходимо следить.

Защита от SQL-инъекций

Безопасность веб-приложения зависит от того, насколько эффективно владельцу удается избежать SQL-инъекций. Этот метод хакерской атаки выглядит как запрос к сайту и его базе данных при помощи поля формы или параметра URL. Если при конструировании ресурса применялся язык Transact SQL, в запрос вставляется вредоносный код, с легкостью меняющий или уничтожающий данные, содержащиеся в таблицах.

Избежать риска получится, если применять параметризованные запросы, в которых задействовано несколько языков программирования.

Дополнительные способы обеспечения безопасности

Работа с веб-сервисами требует использования широкого инструментария для обеспечения безопасности. Помимо основных перечисленных методов, часто применяются:

- шифрование паролей;
- избегание межсайтового скриптинга;
- контроль загрузки файлов на сервер.

Совместное применение всех доступных решений обеспечит безопасность на максимально доступном уровне.

Обучение персонала

Обязательным пунктом обеспечения информационной безопасности является обучение персонала, особенно новичков. Необходимо рассказывать обо всех известных угрозах, кибер-рисках и о методах социальной инженерии, которыми пользуются хакеры для взлома систем.

Вывод

Рассмотренные в данной статье методы по информационной защите нельзя назвать полностью законченным. Все потому, что каждый веб-проект или веб-приложение уникальны, и даже сам создатель не всегда может со стопроцентной уверенностью сказать, что его проект полностью защищен от внешних угроз. Однако соблюдение даже части рассмотренных методов защиты, может уменьшить кибер-риски, которые исходят из интернета.

Библиографический список

1. Андрианов, В.В., Зефиров, С.Л., Голованов, В.Б., Голдуев, Н.А. Обеспечение информационной безопасности бизнеса / Под ред. Курило А.П. М.: Альпина Паблишерз, 2015.

2. Вайнштейн, Ю.В., Демин, С.Л., Кирко, И.Н., Кучеров, М.М., Сомова, М.В. Основы информационной безопасность. Учебное пособие по дисциплинам «Основы информационной безопасности», «Информационная безопасность и защита информации» для студентов направления подготовки дипломированных специалистов 090100 - «Информационная безопасность», 230200 - «Информационные системы и технологии». - Красноярск: СФУ.

3. Бубнов, В.П., Тырва, А.В., Хомоненко, А.Д. Обоснование стратегии отладки программ на основе нестационарной модели надежности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2016. № 3(97). с. 85-92.

4. Сафонов, Л. Риски информационной безопасности веб-приложений. [Электронный ресурс] – Режим доступа: https://habr.com/ru/

БЕЗОПАСНОСТЬ В PYTHON: АСПЕКТЫ ЗАЩИТЫ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Митричев Д.В., студент
Колледж гуманитарных и социально-педагогических дисциплин имени Святителя Алексия, Митрополита Московского
Руководитель: Сыротюк С.Д., к. п. н., доцент
Поволжский православный институт
Абросимова Е.А., студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Информационная безопасность приложения — одна из самых главных сторон разработки, поскольку при глобальной уязвимости в коде, влекущей утечку персональных данных можно потерять всех пользователей. Задача архитектора системы состоит в том, чтобы свести этот риск к минимуму. Однако абсолютной безопасности не существует. Необходимо иметь представление о том, как устроена информационная безопасность в языке Python.

Рассмотрим, что подразумевается под безопасностью в приложении. Есть три основных аспекта: конфиденциальность. целостность, доступность.

Под конфиденциальностью понимается предотвращение возможной утечки информации. Под целостностью понимается неизменность данных при выполнении операции над ними. Под доступностью понимается гарантированное обеспечение доступа к информации и связанным с ней активам авторизованным пользователям [1].

Под хэшированием понимается преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Полученный результат называется хэш-кодом, контрольной суммой или дайджестом сообщения (message digest). Каждый хэш-код является уникальным. Чтобы создать дайджест используются алгоритмы хэширования. Самые популярные алгоритмы это: MD5 (относительно ненадежен), SHA-1 (относительно ненадежен), SHA-2, SHA-3 и ГОСТ Р 34.11-2012 [2].

Для работы с хэшированием в Pyton используются следующие модули:

- hashlib для вычисления хэш-функции;
- HMAC— для проверки целостности информации;
- secrets для генерации псевдослучайных чисел;
- getpass - для создания безопасных логина и пароля.

Есть и более продвинутые варианты для работы с низкоуровневыми интерфейсами, криптографическими алгоритмами: симметричные шифры, дайджесты сообщений и функции вывода ключей, такие как PyCryptodome или Cryptography.

Обычно HMAC-аутентификация используется во внутренних системах обмена сообщениями и в межпроцессном взаимодействии. Например, можно использовать данный подход, чтобы гарантировать, что только разрешенные процессы могут подключаться к другим. Модуль muliprocessing внутри использует аутентификацию, основанную на HMAC, чтобы установить соединения с подпроцессами.

Рассмотрим два примера.

Пример № 1 "хэширования пароля". Аутентификация соединения не подразумевает последующего шифрования, здесь все сообщения передаются в открытом виде по сети. Любой, кто подключиться к сети, может перехватить нужный сетевой трафик. Чтобы этого не случилось, создаем объект хэш-суммы с набором байтов h = hashlib.md5(). Добавляем в неё данные для расчета этой самой суммы h.update(b’Code’) и выводим ее print(h.hexdigest()). HEX здесь прописываем т.к. используется шестнадцатеричная система счисления.

Чтобы вычислить хэш используется специальная конструкция pbkdf2_hmac, в которой указаны параметры — имя алгоритма шифрования (sha256), пароль в виде строки байтов (b’pswd’, наличие соли (b’salt’) и длина расширенного ключа (100000). Плюс такого подхода в том, что недопустимо изменение даже одного символа, т.е. принцип целостности информации тут сохраняется

Код:

```
import hashlib, binascii
# Наша хэш функция
# Создание объекта хэш-суммы
h = hashlib.md5()
# Добавление данных для расчета суммы - можно добавлять только строку байтов
h.update(b'Code')
# Вывод хэш-суммы
print(h.hexdigest())
#Парольный хэш
dk = hashlib.pbkdf2_hmac('sha256', b'pswd', b'salt', 100000)
# Вычисленное значение можно хранить в БД
  print(binascii.hexlify(dk))
```

Результат выполнения показаны на рисунке (рис. 1):

Рисунок 1 - Результат выполнения

Пример № 2. "шифрование данных". Для шифрования данных используется библиотека PyCrypto. Сегодня используется модернизаци PyCryptodome (PyCryptoDomeEx). Для шифрования данных в PyCryptodome есть поддержка нескольких алгоритмов — блочные шифры: AES, DES, 3DES, Blowfish и поточные шифры: Salsa20, ChaCha20. Устанавливается форк (обновление протокола или кода криптовалюты) с помощью команды pip install pycryptodomex.

В нашем примере в переменную plaintext вносим шифруемое сообщение, преобразовав его в байты. Функция [mks_highlight color="#FEFDA9"] encrypt принимает на вход текст сообщения в байтах. В переменную cipher записывается конструкция AES.new. Она создает новый шифр с использованием этого алгоритма. AES — это специальный симметричный шифр. Обратим внимание, что наша длина сообщений — 16 байт (т.к. используется AES-128). Длина ключа ASCII должна быть 16 символов (1 символ = 8 бит = 1 байт, 16 символов = 16 байт)

Код:

```
import os
from binascii import hexlify
from Cryptodome.Cipher import AES
# шифруемое сообщение
plaintext = b'The rain in Spain'
def padding_text(text):
    ''' Выравнивание сообщения до длины кратной 16 байтам.
        В данном случае исходное сообщение дополняется пробелами.
    '''
    pad_len = (16 - len(text) % 16) % 16
    return text + b' ' * pad_len
def _encrypt(plaintext, key):
    ''' Шифрование сообщения plaintext ключом key.
        Атрибут iv - вектор инициализации для алгоритма шифрования.
        Если не задаётся явно при создании объекта-шифра, то генерируется случайно.
        Его следует добавить в качестве префикса к финальному шифру,
        чтобы была возможность правильно расшифровать сообщение.
    '''
    cipher = AES.new(key, AES.MODE_CBC)
    ciphertext = cipher.iv + cipher.encrypt(plaintext)
    return ciphertext
def _decrypt(ciphertext, key):
    ''' Расшифровка шифра ciphertext ключом key
        Вектор инициализации берётся из исходного шифра.
        Его длина для большинства режимов шифрования всегда 16 байт.
        Расшифровываться будет оставшаяся часть шифра.
    '''
    cipher = AES.new(key, AES.MODE_CBC, iv=ciphertext[:16])
    msg = cipher.decrypt(ciphertext[16:])
```

```
    return msg
# Осуществим шифрование сообщения алгоритмом AES
# key (строка байтов) - секретный ключ для симметричного шифрования.
# Ключ должен быть длиной 16 (AES-128), 24 (AES-192) или 32 (AES-256) байта.
key = b'Super Secret Key'
# Длина сообщения должна быть кратна 16, поэтому выполним выравнивание.
plaintext = padding_text(plaintext)
# Выполним шифрование
cipher = _encrypt(plaintext, key)
print(hexlify(cipher))
# Выполним расшифрование
msg = _decrypt(cipher, key)
print(msg)
```

Таким образом, в статье представлены основные направления информационной безопасности в Python, рассмотрены примеры хэширования пароля и шифрования данных в Python [3-5].

Владение этими навыками позволит обеспечивать внутреннюю безопасность информации в любой организации [6].

Библиографический список

1. Лободина, А.С. Информационная безопасность / А.С. Лободина, В.В. Ермолаева. — Текст : непосредственный // Молодой ученый. — 2017. — № 17 (151). — С. 17-20. — URL: https://moluch.ru/archive/151/42898/ (дата обращения: 24.11.2020).
2. Гудков, А.А. Хеширование как метод оптимизации поиска данных // Информационные системы и технологии: управление и безопасность. 2014. № 3. С. 77-82.
3. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
4. Бэрри, Пол Изучаем программирование на Python / Пол Бэрри. - М.: Эксмо, 2016. - 332 с.
5. Васильев, А.Н. Python на примерах. Практический курс по программированию / А.Н. Васильев. - М.: Наука и техника, 2016. - 432 с.
6. Жуков Г.П., Гудков А.А. Защита информации от руткитов // Информационные технологии. Радиоэлектроника. Телекоммуникации. 2015. № 5-1. С. 264-269.

ПРОБЛЕМЫ УСТАНОВЛЕНИЯ АВТОРСТВА ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Паршин К.И., студент, Тарасов Д.А., старший преподаватель
МГТУ имени Н.Э. Баумана
г. Москва, Россия

Вредоносное программное обеспечение (далее – ВПО) представляет собой серьезную опасность для информационных систем. Недооценка её может иметь серьезные последствия для информации пользователей. Также и с точки зрения исследователей ВПО с применением специальных знаний в области судебной компьютерно-технической экспертизы оно имеет важнейшее значение как объект, способный «предоставить» информацию о его действии в связи с расследуемым делом. Наряду с прочими вопросами, идентификация автора, исследуемого ВПО, занимает лидирующие по популярности и важности для правоохранительных органов и суда места. Естественно, злоумышленники-создатели ВПО, так же осознавая это, предпринимают попытки «маскировки» своего продукта, и задача исследователя в данном случае состоит не только в поэтапном следовании методическим рекомендациям, но и в умении нестандартно мыслить и знать современную экспертную практику по схожим объектам исследования. Для наиболее полного анализа данных методов, прежде всего, необходимо обратиться к определению самого ВПО.

Вредоносная программа – это любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа.

При этом общепризнанной классификации ВПО пока не существует и во многом "вредность" или "полезность" программного обеспечения определяется самим пользователем или способом его применения. Первые попытки упорядочить процесс классификации были предприняты еще в начале 90-х годов прошлого века в рамках альянса антивирусных специалистов CARO (Computer AntiVirus Researcher's Organization). Альянсом был создан документ "CARO malware naming scheme", который на какой-то период стал стандартом для индустрии.

Но со временем стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться. Ещё более важной причиной отказа от неё стало то, что технологии детектирования систем антивирусных компаний отличаются друг от друга и, как следствие, невозможно унифицировать результаты проверки разными антивирусными программами. Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов. Последним значительным проектом подобного рода было создание стандарта CME (Common Malware Enumeration), суть которого заключается в присвоении одинаковым детектируемым объектам единого уникального идентификатора.

В настоящее время одним из наиболее приоритетных направлений в области защиты информации является борьба с вредоносным кодом ВПО. С этой целью во всем мире созданы компании, специализирующиеся на защите информации, которые занимаются анализом вредоносных программ и созданием эффективных средств защиты. И, тем не менее, новые версии вредоносного кода появляются регулярно, а общее число крупных эпидемий вирусов и червей растет из года в год.

В данной ситуации наиболее пристальное внимание нужно обращать не на следствие проблемы, а на ее причину - авторов этих программ. Здесь крайне важную роль играют поиск и наказание создателей ВПО, в первую очередь потому, что подобные акты сильно ослабляют желание других создателей вирусов заниматься данным видом преступной деятельности. Рассмотренный далее метод предназначен не для однозначного определения автора того или иного ВПО, а для значительного сужения круга наиболее вероятных авторов.

Задача определения автора ВПО состоит в следующем. Пусть имеются фрагменты образцов ВПО ряда авторов, написанные под одну платформу, на одном языке программирования, с использованием одного компилятора. О некотором анонимном фрагменте известно, что он принадлежит одному из данных авторов. Требуется узнать, кому именно. Одним из методов определения автора ВПО является теория энтропийной классификации с помощью сжатия. Суть метода в том, чтобы подклеивать анонимный текст к образцам ВПО, принадлежащим заранее известным авторам, и смотреть, насколько хорошо он сжимается. Самым вероятным автором будет тот, к чьему коду образец компилируется лучше всего. В результате получаем коэффициент, который можно использовать для определения принадлежности данного кода наиболее вероятному автору.

Однако, как уже было отмечено ранее, авторами ВПО создаются различные защитные механизмы, имеющие своей целью недопущение идентификации их автора. В начале 90-х гг. прошлого века, когда начала формироваться индустрия антивирусных программных продуктов, появились первые антивирусные программные пакеты, которые производили обнаружение вирусов на основе базы характерных участков вредоносного кода (сигнатур). В результате авторы вредоносных программ стали применять различные методы для усложнения детектирования своих продуктов появившимися программами защиты. В статье Гребенникова Н. «Технологии защиты вредоносных программ» выделяется три поколения методов защиты, придуманных авторами ВПО за прошедшее время.

К первому поколению методов защиты вредоносных программ относятся следующие: упаковка, полиморфизм, обфускация.

Упаковка - процесс уменьшения размера исполняемого файла с сохранением возможности самостоятельного выполнения. Реализуется с помощью специальных утилит - пакеров. Ранее упаковка использовалась для экономии места на жестком диске. На данный момент эта функция пакеров частично устарела, однако упаковкой активно пользовались и продолжают пользоваться авторы вредоносных программ, так как если программа-антивирус не умеет распаковывать файлы, упакованные некоторым пакером, то и найти в них вирус она также в большинстве случаев не сможет. На настоящий момент известно несколько сот упаковщиков, количество различных версий которых приближается к трем тысячам.

Полиморфизм - метод формирования экземпляров вируса, при котором код вируса формируется "на лету" - уже во время исполнения, при этом сама процедура, формирующая код, также не является постоянной и видоизменяется при каждом новом заражении. Таким образом, в большинстве случаев два образца одного и того же вируса-полиморфика не имеют ни одного совпадения.

Обфускация (от англ. "obfus-cation" - запутывание) - один из методов защиты программного кода, который позволяет усложнить процесс реверсивной инженерии кода защищаемого программного продукта. Суть метода заключается в том, чтобы запутать программный код и устранить большинство логических связей в нем, то есть трансформировать его так, чтобы он был очень труден для изучения и модификации посторонними лицами. Обфускация может применяться для защиты любого программного обеспечения, не обязательно вредоносного. Однако в настоящее время она активно применяется именно авторами вредоносных программ.

Ко второму поколению методов защиты вредоносных программ относятся методы борьбы с защитным ПО и методы защиты от удаления.

В качестве методов борьбы с защитным программным обеспечением можно выделить следующие:

- нарушение доступа к серверам обновлений защитного ПО, которое производится либо путем модификации специального файла hosts;

- завершение процессов, удаление файлов или записей реестра защитного ПО. Идея этого способа борьбы проста: зачем бороться с продвинутыми методами детектирования, если можно просто завершить процесс антивируса и делать все что угодно на незащищенной машине.

Основные методы защиты вредоносных программ от удаления.

Метод «watchdog» (двух процессов), который заключается в том, что вредоносная программа создает в памяти два процесса, которые непрерывно контролируют работу друг друга. В случае удаления одного из процессов антивирусом, второй процесс его мгновенно перезапускает.

Метод троянского потока, основанный на создании одного или нескольких потоков в системных процессах. Эти потоки выполняют восстановление стертых файлов, восстановление ключей реестра, перезапуск процессов вредоносной программы. Одним из примеров реализации метода является not-a-virus: AdWare.Win32. Better-Internet. Входящую в его состав троянскую программу nail.exe можно удалить с диска, но она будет восстановлена при помощи троянского потока (образ файла nail.exe хранится в памяти); другим примером является not-a-virus: Adware.Win32.Look2me, регистрирующийся в качестве расширения WinLogon. Зарегистрированная таким образом библиотека загружается в ходе процесса загрузки и остается в памяти в течение всего времени работы системы, что затрудняет ее удаление.

Блокировка доступа к файлу, которая сводится к открытию вредоносной программой собственных файлов в режиме монопольного доступа или к блокировке файлов при помощи функции LockFileEx. Антивирус в этом случае не может получить доступ к файлам для проверки и удаления стандартными способами.

Пересоздание ключей реестра вредоносной программы с высокой частотой, что не позволяет антивирусу исключить программу из автозагрузки.

Третье поколение методов защиты вредоносных программ - это скрытие их с помощью руктит-технологий и борьба с подсистемами проактивной защиты.

Руткит - программная техника или код, целью которых является сокрытие какой-либо деятельности или объектов в системе. Чаще всего злоумышленниками скрываются процессы, файлы, ключи реестра и сетевая активность. То есть все те объекты, которые могут демаскировать присутствие вредоносной программы в зараженной системе.

Распространение руткитов в последнее время приняло угрожающий характер. Практически все новые "серьезные" вредоносные программы семейств Worm и Trojan имеют в своем составе мощный руткит-компонент, работающий в режиме ядра операционной системы.

Основным методом борьбы с подсистемами проактивной защиты на данный момент является программное нажатие на кнопку "Разрешить" в диалоге, показываемым антивирусным продуктом в тот момент, когда он проактивно определяет подозрительную активность вредоносного процесса. В результате пользователь вряд ли заметит очень быстро промелькнувший диалог, а вредоносная программа продолжит свое исполнение.

Между тем, ряд работ как отечественных, так и зарубежных авторов посвящены проблемам исследования именно участков кода вредоносных программ на предмет их аналогичности или идентичности. Так, существуют методы, основанные на строках (разбивка программного кода на строки); метод, основанный на токенах, при котором исходный код разбивается на лексемы (выражения, операторы), образуя так называемую последовательность токенов; метод, основанный на деревьях (программный код представляется в виде абстрактного синтаксического дерева); методы, основанные на семантическом анализе, учитывающие семантическую составляющую программного кода.

Таким образом, при наличии достаточно разработанных методов идентификации программного кода, что в ряде случаев позволяет установить его авторство, существует также и немало проблем, обусловленных авторскими мерами защиты ПО от исследования, что, однако, не отменяет необходимости дальнейшей работы в этом направлении.

Библиографический список

1. Вахрушев, И.Н. Классификация методов поиска похожего программного кода // Журнал Novainfo. – 2010. – № 1.

2. Гребенников, Н. Технологии защиты вредоносных программ. [Электронный ресурс] // URL: https://lib.itsec.ru/articles2/Oborandteh/ tehnologii_zashiti_vredonosnih_programm (дата обращения: 14.11.2020).

3. Осовецкий, Л.Г., Стремоухов, В.Д. Определение авторства вредоносного кода с использованием метода сжатия данных. [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/opredelenie-avtorstva-vredonosnogo-koda-s-ispolzovaniem-metoda-szhatiya-dannyh (дата обращения: 14.11.2020).

4. Тарасов, Д.А. Проблемы установление авторства программного продукта в рамках компьютерно-технической экспертизы. // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы. Сборник научных трудов I международного форума. Изд-во: Московский университет МВД России имени В.Я. Кикотя. М., 2017.

5. Тарасов, Д.А., Войтова, О.Г. К вопросу о проблеме ограничения доступа к незаконно распространяемым объектам авторского права в сети Интернет // Международная научно-практическая конференция «Российский и международный опыт производства судебных экспертиз»: сборник материалов. М.: Московский университет МВД России имени В.Я. Кикотя. 2017. С. 168–171.

«Лекция 1: Основные понятия в области информационной безопасности. Вредоносное программное обеспечение» [Электронный ресурс] // URL: https://intuit.ru/studies/courses/ 16655/1300/lecture/25504?page=2 (дата обращения: 14.11.2020).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ОСНОВНЫЕ АСПЕКТЫ

Поколявин А.И., студент
Научный руководитель: Ремнева О.Ю., к. т. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность,
- целостность,
- конфиденциальность.

Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно;

Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации;

Конфиденциальность - данное понятие означает ввод в действие контроля, гарантирующего достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата;

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Основные угрозы информационной безопасности

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

- аппаратные средства - компьютеры и их составные части;
- программное обеспечение - приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы, утилиты, диагностические программы и т.д.;
- данные, хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- персонал - обслуживающий персонал и пользователи.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные.

Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия - это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

- недовольством служащего своей карьерой;
- взяткой;
- любопытством;
- конкурентной борьбой;
- стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;

нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД). НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов НСД, по которым можно осуществить хищение, изменение или уничтожение информации:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- дешифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Обеспечение информационной безопасности

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. законодательный (законы, нормативные акты, стандарты и т.п.);

2. морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации);

3. административный (действия общего характера, предпринимаемые руководством организации);

4. физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);

5. аппаратно-программный (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная система защиты должна соответствовать следующим принципам:

- Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.
- Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.
- Защита тем более эффективна, чем проще пользователю с ней работать.
- Возможность отключения в экстренных случаях.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать. Система защиты должна предоставлять доказательства корректности своей работы.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.

Надежная система защиты должна быть полностью протестирована и согласована.

Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

Система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения.

Наиболее важные и критические решения должны приниматься человеком.

Существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

Заключение

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности,

Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Библиографический список

1. Информационная безопасность. [Электронный ресурс] – Режим доступа: http://protect.htmlweb.ru

2. Информационная безопасность. [Электронный ресурс] – Режим доступа: http://wikipedia.org.

3. Фигурнов, В.Э. IBM PC для пользователя.

4. Информационная безопасность и защита информации. Учебное пособие – М.: 2004 – 82 с. [Электронный ресурс] – Режим доступа: http://bezopasnik.org›article/book/23.pdf.

5. Сальников, Д.А. Информационная безопасность: Реферат / Алтайский государственный университет, 2011 г. [Электронный ресурс] – Режим доступа: https://works.doklad.ru/view/64ZKFOqS1eI.html.

6. Информационная безопасность. [Электронный ресурс] – Режим доступа: https://pirit.biz/reshenija/informacionnaja-bezopasnost.

РАЗНОВИДНОСТИ DDOS АТАК И МЕРЫ ПРОТИВОДЕЙСТВИЯ ИМ

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

Аннотация: Проанализированы современные тенденции в области развития защиты от DDoS-атак в информационной среде и рассмотрены потенциальные меры по защите данных от правонарушителей.

Ключевые слова: DDoS-атака, информационная безопасность.

Вступление

DDoS-атаки – актуальная проблема в информационном мире, с которой людям пришлось столкнуться еще 20 лет назад, и которая побудила специалистов в области информационной безопасности искать способы эффективной защиты и противодействия этой напасти. В данной работе рассматриваются понятия DDoS атак, их разновидности и возможные меры защиты от DDoS атак.

DDoS (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании») – хакерская атака на вычислительную технику исполняемая одновременно с большого числа устройств.

Теперь, когда мы имеем представление о том, что именно такое DDOS, стоит разобраться в разновидностях этих атак, выделить наиболее распространенные и рассмотреть возможные варианты защиты и методы противодействия им.

Одними из самых распространенных являются TCP SYN flood атаки, ботнет атака, Smurf-атаки, DNS-атаки с усилением, TCP Reset. Данные типы атаки схожи между собой тем, что их объединяет общая цель, которую ставят злоумышленники и связана она с нанесением ущерба жертве атаки, либо с целью выявления потенциальных уязвимостей серверной системы.

SYN flood

SYN flood (полуоткрытая атака) представляет собой сетевую атаку типа «отказ в обслуживании» (DDoS), целью которой является намерение вызвать перерасход ресурсов системы и сделать сервер недоступным для легитимного трафика с помощью отправки большого количества SYN-запросов на подключение к серверу, тем самым умышленно забивая очередь полуоткрытыми соединениями, ожидающими подтверждения от клиента на подключение к серверу для легитимных пользователей, что приводит к потреблению всех до-

ступных ресурсов сервера и к техническим неполадкам, по типу невозможности установления связи и наличию существенных задержек в работе сервера. По истечении определенного тайм-аута эти подключения отбрасываются. Происходит это вследствие того, что на каждый входящий SYN-пакет система резервирует определенные ресурсы в памяти, генерирует ответ SYN+ACK (synchronize+acknowledges), содержащий криптографическую информацию, выполняет поиск в таблицах сессий и т. д. Это и затрачивает процессорное время. Наступление отказа в обслуживании возможно при потоке SYN Flood от 100 до 500 тыс. пакетов за секунду. Но сейчас правонарушителю, имеющему хотя бы гигабитный канал, представляется возможным направить поток до 1,5 млн пакетов в секунду, тем самым вызывая долговременный перебой в работе системы.

Предложенным решением было использование SYN cookie, принцип работы которого заключался в том, что использование данной техники позволяет серверу избегать сброса новых соединений, когда очередь TCP-соединений переполнена. Сервер просто отправляет обратно клиенту правильную последовательность SYN+ACK, но при этом не сохраняет новое соединение в очереди. Если сервер затем получит ACK-ответ от клиента, то он сможет восстановить своё значение SYN-последовательности по принятому от клиента значению.

Однако такой способ имел два недостатка: возможность использовать только 8 различных значений для MSS и вынужденное игнорирование сервером всех TCP опций (увеличенный размер окна, метки времени и др.), так как они отправляются в первоначальном SYN-запросе.

Также нередко применяются DPI-системы (Deep Packet Inspection), способные анализировать и контролировать проходящий через них трафик. Сама система сперва обнаруживает атаку по превышению заданного порога неподтвержденных клиентом SYN-запросов, а затем самостоятельно, вместо защищаемого сайта, на них отвечает. TCP-сессия организуется с защищаемых сайтов после подтверждения запроса клиентом. Стоит отметить и такой способ как -ограничение запросов на новые подключения от конкретного источника за определенный промежуток времени. Сетевой протокол транспортного уровня SCTP, который является более современным по сравнению с TCP, использует SYN cookie и не подвержен SYN-флуд-атакам. Особенностями является то, что простые межсетевые экраны, которые разрешают любой исходящий трафик и разрешают входящий трафик только к определённым портам, будут блокировать SYN-запросы только к закрытым портам. Если SYN cookie включены, то необходимо сосредоточить внимание на том, что злоумышленник не может обойти такие межсетевые экраны отправкой ACK-пакетов с произвольным номером последовательности пока не подберёт правильный. SYN cookies нужно включать только для публично доступных портов.

Ботнет атака

Ботнет представляет собой компьютерную сеть, которая состоит из некоторого числа хостов с запущенными ботами (автономным программным обеспечением). Установка на компьютер жертвы зачастую происходит незаметно, что дает возможность злоумышленнику выполнять определенные действия с использованием ресурсов зараженного устройства. В целом, используется для нелегальной и неодобряемой деятельности, по типу рассылки спама, атак на отказ в обслуживании и перебор паролей на удаленной системе, использование вычислительных мощностей устройства с целью добычи криптовалют. Таким образом, сформировав представление о том, что такое ботнет и с какими целями его используют, стоит рассмотреть возможные методы противодействия данному типу атаки. Наиболее часто затрудненное обнаружение ботов на устройстве обусловлено тем, что боты работают абсолютно свободно без участия пользователя. Однако существуют некоторые признаки, которые можно выделить и которые являются доказательством наличия бот-инфекции на компьютере. Например, IRC-трафик (ботнеты используют IRC-каналы для связи); Соединения с серверами, замеченными в составе ботнетов; Высокий исходящий SMTP-трафик; Несколько компьютеров в сети, выполняющие одинаковые DNS-запросы; Медленная работа компьютера; Большая нагрузка процессора; Резкое увеличение трафика, особенно на портах 6667 (исполь-

зуется для IRC), 25 (SMTP-порт), 1080 (используется прокси-серверами); Подозрительные исходящие сообщения, которые были отправлены не пользователем; Проблемы с доступом в интернет.

Ботнет как таковой обладает собственной архитектурой, которая включает в себя клиент-серверную и децентрализованную модель.

Клиент-серверная модель - первые ботнеты в ней использовали модель клиент-сервер для выполнения своих задач. В настоящее время централизованные сети по-прежнему широко используются. Среди них наиболее популярными являются сети на базе интернет-ретрансляции, которые используют IRC для того, чтобы облегчить обмен данными между ботами и управляющим компьютером. Сети с такой архитектурой легко создавать и поддерживать, также они позволяют эффективно распределять команды управляющего компьютера между клиентами.

В централизованной сети боты подключаются к одному или нескольким серверам, а затем ждут управляющих команд от сервера. Управляющий компьютер посылает команды на серверы, а те в свою очередь отправляют их клиентам. Клиенты выполняют команды и посылают на сервер сообщение о результатах. Такая модель имеет один существенный недостаток. В случае отказа сервера управляющий компьютер потеряет связь со своими ботами и не сможет ими управлять.

Децентрализованная модель

В последнее время существует тенденция к увеличению числа одноранговых бот-сетей. В ботнете P2P не существует централизованного сервера, боты подключены друг к другу и действуют одновременно как сервер и как клиент. Чтобы отыскать другой зараженный компьютер, бот проверяет случайные IP-адреса до того момента, пока не свяжется с другим зараженным устройством. Найденный бот отсылает информацию о своей версии программного обеспечения и список известных ботов. Если существует различие в версиях ПО, то незамедлительно начнется передача файла для обновления на более новейшую версию ПО. Итак, каждый бот пополняет список зараженных машин и обновляет ПО до более новейшей версии. Эти сети являются устойчивыми к динамическому оттоку, то есть боты могут стремительно присоединяться к сети и также быстро покидать её. Также нарушения связи не произойдет в случае потери или выхода из строя нескольких ботов, ботнет P2P являются более надежными и скрытными, что снижает шансы на обнаружение, в отличие от централизованных сетей.

Теперь имея представление об архитектуре ботнета, рассмотрим способы противодействия ботнет-атаке. Наиболее часто для управления ботнетом используется один или несколько командных (часто центральных) серверов, называемых Command & Control, или C&C. Они взаимодействуют с конечными узлами ботнета по разным протоколам. Наиболее часто в качестве протокола управления используется IRC. В целом, в последнее время появилась тенденция к резкому увеличению применения P2P-протоколов (peer-to-peer) как более стабильной, хотя и технологически сложной альтернативы. Нетипичным решением в последнее время стало использование для управления ботнета файлообменных сетей и передача управляющих команд в теле фотографий, опубликованных в социальных сетях. Таким образом, для борьбы с ботнетом можно предпринять несколько определенных действий: Захватить или вывести из строя C&C-узлы; DDoS на C&C-узлы; жалобы провайдеру, где хостятся C&C-узлы; захват DNS-имен, используемых C&C; блокирование IP-адресов; арест владельца ботнета; судебный иск, нарушение обмена DNS/HTTP-командами; нарушение peer-to-peer механизмов обмена управляющими командами. К сожалению, не все из этих способов оказываются действенными, а некоторые и вовсе за чертой закона. Между тем некоторые из них нам благополучно удалось использовать. Результатом применения данных мер является уничтожение ботнет-сетей Rustock и Coreflood. Это удалось сделать с помощью захвата C&C-серверов правоохранительными органами (по предварительному решению суда), после которого на все зараженные машины, которые входят в ботнет, была передана команда удаления Malware, которая была предусмотрена разработчиком ботнета.

Атака широковещательными ICMP ECHO пакетами (SMURF атака) относится экспертами к наиболее опасной разновидности DoS-атаки, так как имеет эффект усиления, который является результатом отправки широковещательных ping-запросов к системам, которые обязаны отсылать ответ. Суть данной атаки заключается в том, что атакующий посылает поддельный пакет ICMP Echo по адресу широковещательной рассылки. При этом адрес источника пакета заменяется адресом жертвы, с целью «подставить» целевую систему. Так как пакет Echo послан по широковещательному адресу, то все машины усиливающей сети возвращают жертве свои ответы. Отправив один пакет ICMP в сеть из 100 систем, атакующий подстраивает усиление DDoS-атаки в сто раз.

В целом, существует множество методов защиты от Smurf. Как и с большинством атак пакетными наводнениями, в качестве первостепенной защитной меры необходимо удостовериться в том, что особо существенные системы имеют адекватную пропускную способность и избыточные линии связи. Если произошло обнаружение того, что сеть является частой жертвой Smurf, то стоит задуматься о фильтрации ICMP-сообщений в пограничном маршрутизаторе, хотя эта тактика вероятнее всего затруднит прозвон систем пользователями. Не лишним будет убедиться в том, что никто не сделает из вашей сети Smurf-усилитель, в этом могут помочь сторонние ресурсы для проверки сети. Например, сайт Powertech. Если обнаружено, что сеть все-таки подвержена уязвимостям, то необходимо останавливать пакеты направленной трансляции в пограничном маршрутизаторе или брандмауэре. Существует возможность предотвратить усиление эффекта и возможно это с помощью запрета операций прямой широковещательной рассылки на всех граничных маршрутизаторах. Также дополнительно имеет смысл установить в ОС режим «тихого» отбрасывания широковещательных эхо-пакетов ICMP. Например, на языке Cisco существует простая команда «no ip directed-broadcast», которая во внешнем маршрутизаторе предохранит открытую сеть от принятия пакетов, посланных на адрес сетевой трансляции, а также помешает маршрутизатору преобразовывать пакеты, которые были отправлены на адрес IP-трансляции сети, в трансляцию MAC- уровня, тем самым сбрасывая все подобные запросы на входе в сеть и не давая использовать сеть как Smurf-усилитель. Такая конфигурация принята по стандарту в межсетевой операционной системе IOS 12.0 и выше, однако на маршрутизаторах Cisco с более ранними операционными системами и маршрутизаторах других изготовителей следует явно отключать направленную трансляцию для каждого интерфейса на маршрутизаторе.

DNS-атака с усилением (DNS Amplification)

Данный вид DDoS-атаки использует специфику работы DNS служб в сети Интернет. Его сущность заключается в том, чтобы запросить у публичного DNS-сервера данные о домене и направить его ответ на атакуемый сервер. При реализации данного вида атаки злоумышленник формирует запрос, в ответ на который DNS-сервер возвращает как можно больше данных. Например, запрос списка всех DNS-записей в определенной зоне. Так как в протоколе UDP не выполняется проверка IP-адресов источника, злоумышленник генерирует запросы от имени сервера-жертвы, указывая его IP-адрес в поле исходящего адреса. Таким образом, злоумышленник добивается заполнения канала сервера-жертвы объемными ответами от публичных DNS-серверов. Так, используя всего несколько ботов для генерации запросов к публичным DNS-серверам, злоумышленник может увеличить поток генерируемого “мусорного” трафика до 100 раз. При этом вычисление злоумышленника или хотя бы его IP-адреса генераторов запросов практически не представляется возможным, потому что реальный исходящий IP-адрес всегда заменяется на иной.

Методами защиты и противодействия является отключение рекурсивных запросов и проверка актуальности версии DNS-сервера, а также добавление в black-лист адресов отправителей трафика и закрытие 53 порта (DNS) являются максимально эффективными методами защиты и противодействия, в довесок можно выполнить ряд процедур, которые поспособствуют уменьшению использования сети как усилителя. Например, фильтровка пакетов по содержимому DNS-запросов с последующим отсеиванием содержащих запросы атакующих и использование модуля recent на Linux-сервере с целью создания динамических таблиц IP-

адресов в зависимости от определенных условий, а затем с намерением устанавливать разрешающие и запрещающие правила для этих таблиц с помощью изменения периодичности запросов определенного вида на внешний интерфейс.

TCP Reset

TCP Reset выполняется с помощью манипуляций с RST-пакетами при TCP-соединении. RST-пакет является заголовком, который сигнализирует о том, что необходимо переподключение. Как правило, это используется в том случае, если была выявлена какая-либо ошибка, или, когда появляется необходимость в том, чтобы остановить загрузку данных. Злоумышленник может прерывать TCP-соединение, неизменно пересылая RST-пакет с валидными значениями, что сводит возможность на установление соединения между источником и приемником к нулю.

Чтобы предотвратить данный тип атаки необходимо отслеживать каждый передаваемый пакет и следить за тем, что последовательность цифр поступает в нужном порядке. За это отвечаю системы глубокого анализа трафика, которые широко используются системными администраторами и специалистами по информационной безопасности. В настоящее время целью взлома устройств является организация DDoS-атак или причинение ущерба путем ограничения доступа пользователей к сайту в сети Интернет. Нередко операторы связи, интернет-провайдеры и прочие компании предлагают и организуют решения по защите от DDoS – мониторинг трафика в реальном времени для отслеживания отклонений и всплесков загруженности полосы, а также функцию Carrier Grade NAT, которая позволяет «спрятать» устройство абонента от злоумышленников, закрыв к нему доступ из интернета, а также другие интеллектуальные и даже самообучающиеся системы.

Вывод

Нами были рассмотрены наиболее распространенные типы DDoS-атак, а также меры противодействия им. Таким образом, с развитием средств защиты от DDoS происходит и развитие методов атак. Злоумышленники не стоят на месте, и сегодня провести мощную DDoS-атаку не составляет труда, а сама услуга из года в год становится лишь дешевле. Стоимость варьируется от 5 долларов до нескольких сотен за час, в зависимости от типа атаки и уровня защищенности цели. За последние несколько лет DDoS из самостоятельного метода атаки превратился во вспомогательный. Теперь его целью служит не столько нарушение работы IT-инфраструктуры, сколько отвлечение сотрудников компании от более важных событий безопасности и заметание следов взлома. Это неизбежно приведет к необходимости увеличения уровня автоматизации работы систем предупреждения и предотвращения атак, чтобы дать возможность специалистам по информационной безопасности максимально эффективно выполнять свои обязанности.

Библиографический список

1. Лукацкий А. Обнаружение атак. – Спб.: Изд-во БХВ, 2014. – 624 с.

Интернет-ресурсы:

2. Операции BGP и безопасность. [Электронный ресурс] – Режим доступа: https://tools.ietf.org/html/rfc7454

3. Современные тенденции развития DDoS-атак и защита от них с помощью DefencePro Radware. [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/muk/blog/217695/

4. Лямин, А. Лучшие практики противодействия DDoS-атакам. [Электронный ресурс] – Режим доступа: https://lib.itsec.ru/articles2/cyberwar/luchshie-praktiki-protivodeystviya-ddos-atakam

5. DNS амплификация (DNS Amplification Attack). [Электронный ресурс] – Режим доступа: https://ddos-guard.net/ru/terminology/attack_type/dns-amplifikaciya-dns-amplification-attack

6. Атака широковещательными ICMP ECHO пакетами (Smurf Attack). [Электронный ресурс] – Режим доступа: https://ddos-guard.net/ru/terminology/attack_type/ataka-shirokoveshatelnymi-icmp-echo.

7. Как закрывают ботнеты / Блог компании Журнал Хакер / Хабрахабр. [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/xakep/blog/130792/

8. SYN_cookies. Википедия. [Электронный ресурс] – Режим доступа https://ru.wikipedia.org/wiki/SYN_cookies

9. SYN-флуд. Википедия. [Эл. ресурс] – URL: https://ru.wikipedia.org/wiki/SYN-флуд

10. TCP SYN Flooding атаки и общие меры по смягчению последствий. [Электронный ресурс] – Режим доступа: https://tools.ietf.org/html/rfc4987

11. Атака_TCP_Reset. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki /Атака_TCP_Reset

12. Исаканов, В. Что есть что и кто есть кто на рынке защиты от DDoS. [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/southbridge/blog/450092/

13. Ботнет — Википедия. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Ботнет

14. [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/vasexperts/blog/313562/

15. Немного о типах DDoS-атак и методах защиты / VAS Experts corporate blog / Habr. [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/51574/

16. DoS-атака. Распределённая_DoS-атака. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/DoS-атака#Распределённая_DoS-атака.

17. Проблемы DDOS-атак в современной IT-индустрии и методы защиты от … http://elibrary.ru.

18. Скудис, Эд: пер. с англ. Зацепин, В.Б. Хакерские атаки и защита от них в Unix и Windows. [Электронный ресурс] – Режим доступа: http://dlib.rsl.ru.

СПЕЦИАЛЬНАЯ ОЦЕНКА УСЛОВИЙ ТРУДА МЕДИЦИНСКОЙ СЕСТРЫ СТОМАТОЛОГИЧЕСКОГО КАБИНЕТА

Букловская Е.В., студент
Научный руководитель: Богатова И.Б. к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Трудовая занятость является необходимой и неотъемлемой частью жизни человека, при этом в ходе трудовой деятельности, каждый работник подвергается воздействию вредных и опасных факторов, которые могут снижать работоспособность, негативно отражаться на уровне здоровья, а так же приводить к развитию хронических заболеваний, инвалидности и, даже, смерти.

На каждом рабочем месте такие факторы не одинаковы и имеют разную степень воздействия.

С целью поддержания достойного качества жизни и здоровья населения, а также продления его трудоспособности государственная политика должна стимулировать работодателей проводить мероприятия по улучшению условий труда, снижению уровня вредных и опасных факторов и степени риска производственного травматизма. Для достижения этой цели осуществляется государственное регулирование условий труда.

С 1 января 2014 года введён в действие Федеральный Закон №426-ФЗ «О специальной оценке условий труда», заменяющий процедуру проведения аттестации рабочих мест.

Специальная оценка условий труда - единый комплекс последовательно выполняемых процедур по идентификации вредностей (опасностей) и оценке уровня воздействия выявленных вредных и опасных факторов производственной среды и трудового процесса на организм работника с учетом эффективности средств индивидуальной защиты.

Специальная оценка условий труда проводится в соответствии с Методикой проведения, утверждаемой Приказом Минтруда России от 24.01.2014 N 33н, для предотвращения негативного воздействия условий труда на здоровье работников и определения суммы компенсационных выплат и отчислений в Фонд социального страхования и Пенсионный фонд. Эта процедура требует привлечения квалифицированных и аккредитованных специалистов, обладающих необходимым измерительным оборудованием и лабораторной базой.

Процедура СОУТ предполагает оценку фактических условий труда для каждого работника, что должно позволить объективно оценить и классифицировать каждое рабочее место. По результатам специальной оценки условий труда устанавливается класс труда, в соответствии с которым работник имеет право на:

- установления льготных выплат;
- определения продолжительности отпуска;
- определения продолжительности рабочей недели в часах;
- установления частоты медицинских осмотров;
- принятия мер для обеспечения условий безопасного труда.

Целью исследовательской работы является проведение специальной оценки условий труда медицинской сестры в стоматологической клинике ООО «Инсаюр Медикал Дента».

В соответствии с целью в работе поставлены следующие задачи:

1. Изучение методики проведения специальной оценки условий труда, утвержденной Приказом Минтруда России от 24.01.2014 N 33н. и иных необходимых нормативно-правовых документов.

2. Изучение должностных обязанностей медсестры, технических особенностей помещения и оборудования, а также материалов, используемых в работе.

3. Проведение наблюдения за ходом работы медицинской сестры в стоматологическом кабинете с целью идентификации вредных и (или) опасных производственных факторов, воздействующих на неё.

4. Проведение измерения идентифицированных факторов, воздействующих на медсестру в процессе работы.

5. Определение класса условий труда медицинской сестры в стоматологическом кабинете в соответствии с полученными результатами.

Стоматологическая клиника ООО «Инсаюр Медикал Дента» расположена в жилом доме, по адресу Самарская область, г. Тольятти, ул. Ленинградская, д. 45, занимает один этаж.

Клиника оказывает стоматологические услуги по лечению, профессиональной гигиене зубов ультразвуковым методом, услуги по ортопедии, хирургии, ортодонтии. Она оснащена следующим оборудованием:

1. Стоматологические установки, с водяной системой охлаждения, снижающие концентрацию зубной пыли в воздухе.
2. Ультрафиолетовые шкафы для хранения стерильного инструмента.
3. Бактерицидные облучатели Дезар.
4. Установка ультразвуковая механическая для дезинфекции мелких стоматологических инструментов.
5. Гласперленовый стерилизатор для мелких инструментов.
6. Стерилизаторы паровые.

Используемые материалы в процессе работы:

- дезинфицирующие и антисептические средства;
- пломбировочные материалы.

Рабочее место медицинской сестры – терапевтический кабинет, имеет следующие характеристики:

- площадь кабинета – 20 кв.м., наличие окна;
- наличие приточно-вытяжной вентиляции;
- наличие бытового кондиционера;
- наличие батареи центрального отопления.

Идентифицированы следующие факторы, воздействующие на медицинскую сестру в стоматологическом кабинете:

1. Химические факторы – химические вещества и смеси в воздухе рабочей зоны и на коже работников, образующиеся при применении дезинфицирующих средств, приготовлении стоматологический смесей, использовании антисептических лекарственных растворов.

2. Биологические факторы - воздействие патогенных и условно-патогенных микроорганизмов во время контакта с пациентами и биологическим материалом; вероятность повреждения кожи инструментом, загрязненным кровью или слюной пациента, наличие в воздухе зубной пыли.

3. Физические факторы - воздействие шума при работе стоматологической установки, загрязнение воздуха частицами порошка, применяемого при профессиональной гигиене и опилом пломбировочного материала.

4. Факторы трудового процесса - вынужденная или неудобная рабочая поза во время приема, статические нагрузки, высокая интенсивность трудового процесса, психоэмоциональное напряжение.

Оценка условий труда по каждому фактору, а также общая оценка и класс труда на рабочем месте по степени вредности и опасности представлена в таблице 1.

По результатам таблицы следует, что условия труда медицинской сестры соответствуют 2 допустимому классу.

Исходя из проделанной работы сформулированы предложения по улучшению условий труда медицинской сестры стоматологического кабинета ООО Инсаюр Медикал Дента:

Таблица 1 - Итоговая оценка условий труда

Наименование фактора	Класс (подкласс) условий труда
Химический	2
Биологический	-
Аэрозоли преимущественно фиброгенного действия	2
Шум	2
Вибрация общая	-
Вибрация локальная	-
Инфразвук	-
Ультразвук воздушный	-
Неионизирующие излучения	-
Ионизирующие излучения	-
Параметры микроклимата	-
Световая среда	-
Тяжесть трудового процесса	2
Напряженность трудового процесса	1
Итоговый класс (подкласс)	2

1. В стоматологическом кабинете проводить постоянный контроль состояния воздушной среды и микроклиматических параметров.

2. С целью уменьшения нервно - эмоционального перенапряжения предусмотреть формирование смен для оказания лечебно-диагностических манипуляций и малых операций пациентам с учетом психологической совместимости.

3. С целью профилактики утомления периодически (через 3-3,5 часа работы) проводить физкультурные паузы.

4. Для профилактики и снижения нервно - эмоционального перенапряжения создать комнаты психологической разгрузки с использованием методов аутогенной тренировки и психотерапевтических сеансов.

Библиографический список

1. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 24.04.2020).

2. Федеральный закон «О специальной оценке условий труда» от 28.12.2013 N 426-ФЗ.

3. Приказ Минтруда России от 24.01.2014 N 33н «Об утверждении Методики проведения специальной оценки условий труда, классификатора вредных и (или) опасных производственных факторов, формы отчета о проведении специальной оценки условий труда и инструкции по ее заполнению».

ВИЗУАЛЬНОЕ ЗАГРЯЗНЕНИЕ СРЕДЫ

Лбова А.Е., студент
Научный руководитель: Романова Е.П., к. б. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Ландшафты современного города относятся к преобразованным ландшафтам, в котором элементы, созданные человеком, доминируют над естественными. Такой ландшафт называют урбанизированным, что подчеркивает его искусственность и величину преобразования [4]. Главной особенностью такого ландшафта является его *дискретность, что подчеркивается искусственно созданной планировкой города.* Основными элементами городского ландшафта является сеть дорог и инженерные коммуникаций [9].

Современная жилая застройка с доминированием геометрических элементов, насыщенная большим количеством однообразных поверхностей зданий с бедной цветовой гаммой, гомогенна и однообразна по своему составу. В ней преобладают агрессивные поля, содержащие множество одинаковых, равномерно распределённых видимых элементов. Это нарушает основу зрительного восприятия, не соответствует нормам зрения, приводит к визуальному загрязнению. Сознательно и неосознанно воспринимаемый человеком видеоряд оказывает влияние на его здоровье и жизнедеятельность в такой же степени, как температура, свет, влажность и другие экологические факторы [8].

Большое число прямых линий, прямых углов нарушает основу зрительного восприятия, что может привести к нарушениям физического и психического здоровья жителей. Противоестественная визуальная обстановка может вызвать у человека целый букет серьёзных заболеваний: от близорукости до эпилепсии и прочих психических недугов. Установлено, что жизнь и работа в среде, бедной зрительными элементами, а также в затемненных помещениях, таких, как фотоателье, полиграфическое предприятие, вызывает у людей невротические состояния, депрессии, галлюцинации, расстройство сна [6]. В гомогенной сфере не могут полноценно работать системы включения и выключения рецепторов (on- и off-системы) [1]. Воздействие агрессивной визуальной среды вызывает у человека снижение времени ясного видения; увеличение числа ошибок, рассеянность, усталость, утомление; раздражительность и агрессивность, что сказывается на эффективности выполняемой работы [3].

Агрессивный визуальный фон порождает целый ряд социальных последствий. В такой обстановке человек чаще пребывает в состоянии беспричинного озлобления, регистрируется больше правонарушений, наблюдается рост числа психических заболеваний. Энцефалограммы людей, созерцающих современную типовую застройку, близка к энцефалограмме переживающего припадок эпилептика [1].

Для г. Тольятти, в котором практически все основные жилые массивы застроены типовыми зданиями 60 – 80 - хх годов прошлого века, тема визуального загрязнения чрезвычайно актуальна.

Цель нашей работы – оценить визуальное загрязнение на примере г.о. Тольятти.

Задачи:

1. Изучить степень гомогенности городской среды районов города.
2. Предложить способы и методы изменения визуальной среды города (применение элементов стрит-арт, граффити, архитектурного освещения).

В составе территории города специалисты Института экологии Волжского бассейна РАН выделяют 27 видов геокомплексов, или индивидуальных территориальных единиц, каждый из которых обладает определенной степенью однородности природных или антропогенных ландшафтов. В городской среде в них входит застройка, зеленые насаждения естественного или искусственного происхождения.

По функциональному использованию территория города делится на 4 зоны:

- жилая (селитебная);
- промышленная;
- зоны отдыха;
- стыковая зона (между селитебной и промышленной застройкой).

Селитебные территории города Тольятти разделены на три района, каждый их них отличается не только своей историей, но и характером застройки.

Наиболее крупным по величине является Автозаводский район, расположен на западе города. Район разделен на кварталы параллельными и перпендикулярными, широкими улицами и проспектами; улицы расположены в меридиональном и широтном направлениях. Построен в 70 – 80-е годы прошлого века, строительство продолжается и сейчас. Планировка района квартальная. Сами кварталы имеют, в среднем, равную площадь и, как правило, являются квадратными по своей геометрической форме. По периметру кварталы застроены многоэтажными жилыми зданиями, в основном девяти-, шестнадцатиэтажными. Внутри каждого квартала находится образовательные учреждения, детские и спортивные площадки, здания жилищно-коммунальных и коммерческих структур, а также рекреационные зоны района: скверы, бульвары, парки.

В этом районе наиболее полно (практически 90%) представлена так называемая гомогенная среда, характеризующая ритмичным чередование однообразных плоскостных поверхностей зданий, как правило, серого, темно-серого или кирпичного цвета, в то время как с точки зрения благоприятного воздействия на человека допустимая концентрация гомогенных и агрессивных факторов на фасадах зданий не должна превышать 50%.

В Центральном районе находится исторический центр города. Это средний по величине селитебный район, включающий целый комплекс частных малоэтажных (1-2 этажа) коттеджных строений, частично скрытых от центральных улиц многоэтажными жилыми домами. Основная часть застройки района – стандартные 5-этажные постройки 60-х годов, так называемые «хрущевки». Многоэтажные строения сосредоточены на юго-востоке района, это наиболее «молодые» здания, в основном девяти – шестнадцатиэтажные, расположены вдоль улиц, между ними находятся малоэтажные образовательные и коммерческие учреждения.

Гомогенность среды этого района, согласно карте-схеме города, оценивается в среднем немного выше 50%. Благоприятным является то, что в районе присутствует много зеленых насаждений, также он имеет большую границу с лесным массивом. Однако внутри кварталов и вдоль проезжей части очень много старых, находящихся в аварийном состоянии малоценных пород деревьев: тополь, карагач, клен ясенелистный, часть которых регулярно удаляется.

Рекреационными зонами являются площадь Свободы перед администрацией и Центральная площадь, а также Парк отдыха, расположенный неподалеку. В нем в настоящее время удалены практически все крупные тополя, зеленый покров восстановлен лишь частично. Парк находится в состоянии реконструкции.

Комсомольский район имеет неровный рельеф, что придает ему разнообразные визуально-видовые преимущества. Район небольшой, территория холмистая, лесные массивы и Волга находятся в непосредственной близости с трех сторон района. Шесть основных улиц района пересекаются под прямым углом, разделяя территорию на несколько микрорайонов, приблизительно одинаковых по площади. Застроен район современными 5–9 и 16-и этажными зданиями. Наряду с селитебными территориями, район включает в себя крупное промышленно-коммерческое предприятие - речной порт. Поскольку он примыкает непосредственно к Волге, в настоящее время практически вся набережная представляет собой прогулочно-рекреационную территорию.

Район не имеет разделяющей зеленой зоны в силу небольшой площади. Парк представляет собой участок природного леса, в котором половина сосен засохла и удалена, остальные находятся в угнетенном состоянии. Проходит реконструкция зеленых насаждений, не всегда удачная. Визуальное загрязнение ниже 50%.

*Шлюзовой поселок ф*ункционально является частью Комсомольского района, но территориально отделен автострадой. На своей территории имеет крупные промышленные предприятия, поэтому не является полностью селитебным районом. Особенностью поселка является наличие железнодорожного узла, расположенного непосредственно рядом с жилыми зданиями. Шлюзовой, также как Комсомольский район, выходит к Волге и не имеет защитных зеленых полос. Регистрируется много несанкционированных свалок, неблагоустроенных участков. Визуальное загрязнение 70% и выше.

*Портпоселок р*асположен зоне отдыха, не является самостоятельным районом города, административно относится к Центральному району. По типу застройки малоэтажная абсолютно преобладает, имеются частные коттеджные строения, но они не являются доминантными. Микрорайон отделен от других селитебных комплексов лесными массивами, наиболее благоприятный с визуальной точки зрения, а также для проживания.

Облик промышленных зон насыщен контурными очертаниями оборудования и специальных установок под открытым небом, является более контрастным по отношению к облику жилых районов. В нашем индустриальном городе промышленные районы занимают значительную территорию, являясь основным градообразующим ядром.

В зависимости от производственной вредности предприятий на основании Санитарно-эпидемиологических правил и норм (СанПиН 2.2.1/2.1.1.1200-03 от 25.09.2007) установлены следующие градостроительные категории промышленных районов:

– 1 категория – промышленные районы, в состав которых входят предприятия, имеющие значительную производственную вредность и размещенные на расстоянии 500-1500м и более от селитебной территории;

– 2 категория – промышленные районы, в состав которых входят предприятия, имеющие незначительную производственную вредность, но связанные с большим грузооборотом и размещаемые в периферийной части города на расстоянии 100-500м от селитебной территории;

К предприятиям 1 категории следует отнести «Куйбышевазот», «Тольяттифосфор», «ТольяттиСинтез» («Сибур», бывший «Синтезкаучук»), «ТоАЗ». Кроме последнего, они сосредоточенные на северо-востоке Центрального района, составляя так называемый Северный промузел. Для предприятий данного класса вредности характерны самые различные по величине здания, в зависимости от их принадлежности к определенному виду производства. Занимаемая площадь зданий варьируется от 1,2 тыс. м² до 7,5 тыс. м². Разнообразной данная промышленная застройка является по этажности (3-9 этажей).

Промышленная зона Центрального района не имеет санитарно-защитной полосы или стыковой зоны, отделяющей ее от селитебной территории. Жилая территория, учебные, образовательные, коммерческие учреждения подходят практически вплотную к химическим предприятиям. Связано это с тем, что район находится в окружении лесных массивов, находящихся в федеральном подчинении, и новой территории для застройки практически не имеет.

ВАЗ относится ко 2 категории промышленных предприятий. Площадь завода 524 га. Специфика производственных зданий машиностроительной промышленности – преобладание горизонтальной протяженности сборочных цехов, которые имеют соотношение высоты здания к его длине 1:80 и более.

При линейной схеме промышленная зона АвтоВАЗа с более или менее одинаковой санитарной характеристикой размещена параллельно селитебной зоне Автозаводского района, тем самым обеспечивается в процессе развития города и их устойчивое пространственное взаимодействие. В условиях застройки Тольятти вопросы композиционного взаимодействия промышленных и селитебных зон были решающими уже на первых порах формирования облика этой новостройки.

Таким образом, анализ территории г.о. Тольятти выявил достаточно высокую степень видеозагрязнения. Гомогенные и агрессивные поля преобладают в тех районах города, где много типовой застройки 60 - 70 – 80-х годов. Целые микрорайоны состоят из унылых блочных коробок.

Что касается общественных зданий, то следует отметить, что именно они являются ярким примером агрессивных полей. Увлечённость современной архитектуры большими стеклянными поверхностями, как правило, тёмного цвета, не делает среду обитания горожан комфортной и безопасной, наоборот, порождает чувство подавленности.

При невозможности значительно изменить архитектурный облик города, комфортность среды обитания можно создать и цветовым решением. Цвет в архитектуре города призван выполнять ряд важнейших функций: он ориентирует человека в пространстве и во времени, придаёт значение отдельным компонентам среды, создаёт психофизиологический комфорт, формирует содержательное и эмоционально насыщенное городское пространство. Моноцветие застройки также можно рассматривать как пример гомогенности в условиях города.

Современное строительство жилых домов сопровождается разнообразием цветовой гаммы и геометрических форм, однако невысокая степень озеленения новой точечной застройки подчёркивает однообразие окружающих серых домов, понижает визуальную благоприятность нового строительства, не дает в полной степени гармонизировать окружающее пространство города.

Проведённый социальный опрос жителей города подтвердил наши выводы о влиянии гомогенных и агрессивных полей на человека.

Чтобы уменьшить видеозагрязнение в городе, с нашей точки зрении, необходимо провести ряд мероприятий:

1. Там, где уже есть гомогенная среда, необходимо избавиться от неё с помощью эколого-колористического оформления (путём озеленения города, сочетания зеленых насаждений и граффити), изменения цветовой гаммы уже имеющихся построек с применением элементов арт-сити, граффити и других элементов дизайна.
2. Для цветового насыщение городской среды необходимо шире использовать разнообразие приемов ландшафтного дизайна: вертикальное озеленение, озеленение крыш гаражей в гаражных кооперативах, «цветочную архитектуру» и прочее.
3. Как можно шире использовать архитектурное освещение, придающее совершенно новый вид ночному городу.

Цветовая гамма города может гармонично объединить достаточно большое количество разноплановых по архитектуре зданий. Однако для того, чтобы разработать общий подход, объединяющий разноплановые факторы, такие как природный компонент, историческое наследие, социально-культурные предпочтения граждан, грамотное мнение специалистов и т.д., нужны соответствующие нормативно-правовые акты городского уровня. Для ряда городов (Москва, Санкт-Петербург, такие нормативы уже разработаны. Например, Постановление Правительства Москвы № 114-ПП от 28 марта 2012 года «О колористических решениях фасадов зданий, строений, сооружений в городе Москве», на основании которого для каждого здания должен быть разработан **колористический паспорт здания** - документ, устанавливающий цветовое решение фасада здания.

В настоящий момент разработаны методы количественной оценки агрессивности визуальной городской среды [2], предложено программное средство для подбора наиболее целесообразного мероприятия по снижению визуальной агрессивности изучаемого объекта до нейтрального уровня, основанную на оценочные представления [5].

Полученные результаты предлагаем использовать для внедрения в нормативную документацию при разработке архитектурных проектов города.

Библиографический список

1. Волков, М.А. Визуальная среда обитания / М.А. Волков, Ю. Калачева, О. Кожевникова // SCI-ARTICLE. - Электронный периодический научный журнал. – 2013. - № 3. – с. 30-42.
2. Голубничий, А.А. Количественный метод оценки агрессивности городской визуальной среды / А.А. Голубничий // Изв. Самарского научн. центра Российской академии наук. – 2012. - том 14, №1(9). - с. 2409–414.
3. Кинева, Д.Г. Методики оценки влияния агрессивной визуальной среды на работоспособность человека / Д.Г. Кинева, Г.А. Сулкарнаева, Г.В. Шарухо // Медицина труда и экология человека. – 2015. - №4. - с. 136–139.
4. Литвенкова, И.А. Экология городской среды: урбоэкология: Курс лекций / И.А. Литвенкова. – Витебск: Изд-во УО «ВГУ им. П.М. Машерова». 2005. - 163 с.
5. Неделина, Д.О. Разработка программного средства для выбора наиболее оптимального мероприятия по снижению визуальной агрессивности объектов архитектурной среды / Д.О. Неделина // Молодой учёный. Международный научный журнал. - Казань: ООО «Молодой ученый». - 2017. - № 3 (137). - с. 40–43.
6. Филин, В.А. Видимая среда в городских условиях как экологический фактор / В.А. Филин. - М.: Наука; 1990.
7. Филин, В.А. Автоматия саккад. Монография – М.: МГУ, 2002. - 240 с.
8. Филин, В.А. Видеоэкология. Что для глаза хорошо, а что – плохо. Монография. – М.: Видеоэкология, 2006. - 512 с.
9. Филин, В.А. Визуальная среда города. Вестник Международной академии наук (русская секция) / В.А. Филин, 2006. - №2. – с. 43–50.

СОВРЕМЕННЫЕ МЕТОДЫ БОРЬБЫ С БИОЛОГИЧЕСКИМ ЗАГРЯЗНЕНИЕМ

Малов Д.Н., студент
Научный руководитель: Беспалова К.В., к. х. н.
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Состояние источников водоснабжения в настоящее время вызывает тревогу, что связано с бактериологическим загрязнением, в особенности поверхностных водоёмов. Современные методы очистки ориентированы на удаление вредных бактерий, однако полной деконтаминации не происходит, и водопроводная вода содержит живые микроорганизмы. Бактерии могут служить источником проблем как непосредственно, так и через продукты своей жизнедеятельности - пирогены, нуклеазы или щелочную фосфатазу. Питьевая вода должна быть безопасной в эпидемиологическом отношении, безвредной по химическому составу и иметь хорошие органолептические свойства. Для осуществления этих требований необходимо изучить влияние водных микроорганизмов и продуктов их жизнедеятельности на обработку воды и разработать оптимальные решения по её очистке.

С целью снятия биогенной нагрузки на источники водоснабжения и улучшения качества питьевой воды была проведена разработка оптимальных решений по усовершенствованию очистки природных вод от микроорганизмов и продуктов их жизнедеятельности.

Вода из естественных водоисточников должна подвергаться предварительной водоподготовке (очистке и обеззараживанию). Основными методами очистки воды для хозяйственно-питьевого водоснабжения являются:

– улучшение органолептических свойств: (осветление, обесцвечивание, дезодорация);

– обеспечение эпидемиологической безопасности (хлорирование, озонирование, ультрафиолетовая радиация, ультразвуковое обеззараживание);

– кондиционирование минерального состава (фторирование, обезжелезивание, умягчение и обессоливание).

Современные технологические схемы водоподготовки традиционно представляют собой совокупность двух основных процессов: удаление взвесей (осветление) и обеззараживание.

Осветление воды представляет собой удаление из нее взвешенных веществ, что может быть достигнуто отстаиванием воды в отстойниках, центрифугированием в гидроциклонах, пропусканием ее через слой ранее образованного взвешенного осадка в оборудовании, называемом осветлителями, фильтрованием воды через слой зернистого или порошкообразного фильтрующего материала в фильтрах или фильтрованием через сетки и ткани.

Обеззараживание воды - процесс, производимый для уничтожения содержащихся в ней болезнетворных бактерий и вирусов. Наиболее часто применяют хлорирование, но возможны и другие способы – ультрафиолетовое облучение, ультразвуковая обработка и др.

Выбор метода обработки воды основан на предварительном изучении состава и свойств источника, планируемого к использованию, и их сопоставления с требованиями нормативных документов, и самих потребителей.

Хлорирование воды зарекомендовало себя как надежное средство, обеспечивающее микробиологическую безопасность обрабатываемой воды, и предотвращающее распространение большинства патогенных бактерий (бациллы брюшного тифа, туберкулеза и дизентерии, вибрионы холеры, вирусы полиомиелита и энцефалита).

Бактериологический эффект при хлорировании зависит от дозы вводимого хлора и продолжительности контакта его с водой. Поэтому хлоропоглощаемость одной и той же воды, равная суммарному расходу хлора на окисление микроорганизмов, органических и неорганических примесей, и является переменной величиной, зависящей от внедрённой дозы, продолжительности контакта, величины pH, температуры воды и прочего. Очевидно, что доза вводимого хлора должна быть больше величины хлоропоглощаемости на величину оста-

точного хлора, присутствие которого является гарантией того, что окисление бактерий и органических веществ в воде практически завершено.

Эффективность хлорирования зависит от:

1. Активности применяемых веществ. Наибольшей активностью обладает хлор, слабее действует хлорная известь, причем ее эффективность зависит от содержания в ней активного хлора (25-35 %), прочие соединения оказывают ещё более слабое воздействие;
2. Качества (чистоты) хлорируемой воды. Взвешенные в воде частицы препятствуют бактерицидному действию хлора, хлор тратится на окисление органических веществ воды. Чем чище вода, тем эффективнее хлорирование;
3. Дозы хлора и времени его действия. От дозы хлора (и величины хлорпоглощаемости) зависит количество остаточного хлора, с помощью которого и обеспечивается обеззараживающее воздействие;
4. Свойств самих микроорганизмов.

Основными недостатками хлорирования является следующее:

1. Хлор изменяет органолептические свойства воды (запах, вкус, прозрачность);
2. Имеются хлоррезистентные микробы (например, спорообразующие).

Наряду с хлорированием одним из наиболее распространенных методов обеззараживания воды считается **ультрафиолетовое (УФ) обеззараживание воды**.

Основное применение данный способ нашёл на начальной стадии водоочистки от болезнетворных микроорганизмов. УФ-обработка может быть применена в сочетании с обеззараживанием воды хлором и гипохлоритом, причем хлорирование обязательно производится после обработки воды ультрафиолетом.

Столь широкому распространению ультрафиолетовое облучение обязано своей безреагентной основе, такая технология не только не приводит к образованию в процессе обеззараживания токсичных соединений (как в случаях с применением хлора), но и одновременно почти полностью уничтожает патогенную микрофлору. Ультрафиолетовое обеззараживание воды происходит при помощи способности УФ излучения проникать сквозь стенки клетки, добираясь до ее информационного центра — нуклеиновых кислот ДНК и РНК. В ДНК живой клетки хранится вся информация, которая контролирует процесс развития и нормального функционирования в клетке. **Ультрафиолетовое обеззараживание воды заключается в поглощении лучей излучения нуклеиновыми кислотами.** При поглощении излучения ДНК и РНК теряют способность делиться, вследствие чего теряется способность клетки к размножению, так как именно в разделении нуклеиновых кислот заключается репродукция клетки.

Важным фактором является размер и вид организма. Теоретически, ультрафиолетовая радиация способна убить вирусы, бактерии, грибки и простейших. Но на практике большие организмы, такие как простейшие, могут потребовать большей дозы облучения. Так же многое зависит от вида организма: некоторые бактерии более устойчивы к облучению, чем другие.

Третьим рассматриваемым способом обеззараживания воды в процессе водоочистки является **ультразвуковая обработка**. Данный метод основан на использовании кавитации вызванной ультразвуком. Суть его воздействия заключается в следующем: при протекании кавитации образовываются высокие давления, что приводит к разрыву оболочек клеток микроорганизмов и дальнейшей их гибели. Важной особенностью ультразвукового обеззараживания является чрезвычайно сильная зависимость итоговой эффективности от интенсивности колебаний.

Основным минусами данного метода являются:

– Отсутствие точной локализации. Чтобы уничтожение вредных отложений происходило быстро, приходится увеличивать мощность излучения, что оказывает разрушительное влияние на сварные соединения, пайку, окрасочные, защитные и декоративные слои;

– Невозможность точного контроля, ввиду отсутствия визуального доступа. Невозможность проверки хода рабочих процессов ведет за собой невозможность оптимизации длительность, интенсивность обработки и иных параметров.

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 [Электронный ресурс]. – Введ. 2002-01-01 - Режим доступа: http://mhts.artinfo.ru/BIBLIO/SNIPS/Sanpiny/2.1.4.1074-01/2.1.4.1074-01.htm

2. Ведяпина, В.О., Селезнев, В.А. Оценка влияния водных микроорганизмов на обработку природной воды.

3. Degremont – Технический справочник по обработке воды СПб.: Новый журнал, 2007. – 920 с.

4. Кульский, Л.А., Строкач, П.П. Технология очистки природных вод. 2-е изд., перераб. и доп. – К: Вища шк. Головное изд-во, 1986. –352с.

5. ООО «Издательство ВСТ», журнал «Водоснабжение и санитарная техника». 1999-2013 гг.

6. Водоподготовка: Справочник. /Под ред. д.т.н., действительного члена Академии промышленной экологии С.Е. Беликова. М.: Аква-Терм, 2007. – 240 с.

7. Журавлевич, Н.Е. Обеззараживание питьевой воды: метод. рекомендации / Н. Е. Журавлевич. – Минск: БГМУ, 2017 г. – 26 с.

ОЦЕНКА КАЧЕСТВА ВОЗДУШНОЙ СРЕДЫ Г.О.ТОЛЬЯТТИ В ЛЕТНИЙ ПЕРИОД 2020 ГОДА ПО ДАННЫМ МОНИТОРИНГА НА СТАЦИОНАРНЫХ ПОСТАХ

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

Атмосферный воздух – это важнейшая составляющая окружающей среды, необходимая для существования живых организмов на планете, в том числе и человека, любое его загрязнение оказывает негативное воздействие на их жизнедеятельность. Именно этим обусловлена важность оценки качества атмосферного воздуха путем организации его мониторинга. Таким образом, тема исследования является актуальной.

Целью данной работы является анализ данных мониторинга атмосферного воздуха на стационарных постах в г.о. Тольятти в летний период 2020 года.

Мониторинг атмосферного воздуха — комплексная система наблюдений за состоянием атмосферного воздуха, включающая в себя определение наличия и концентрации в нем загрязняющих веществ, а также прогноз его состояния. Наблюдения за уровнем загрязнения атмосферы осуществляют на постах. Постом наблюдения является выбранное место, на котором размещают павильон, оборудованный необходимыми приборами.

Стационарный пост предназначен для обеспечения непрерывной регистрации содержания загрязняющих веществ и регулярного отбора проб воздуха для последующего анализа.

Посты размещаются на открытой, проветриваемой со всех сторон площадке с непылящим покрытием: на асфальте, твердом грунте, газоне. Если пост разместить на закрытом участке (вблизи высоких зданий, на узкой улице, под кронами деревьев или вблизи низкого источника выбросов), то он будет характеризовать уровень загрязнения, создаваемый в конкретном месте, и будет или занижать реальный уровень загрязнения из-за поглощения газов густой растительностью, или завышать из-за застоя воздуха и скопления вредных веществ вблизи строений.

Число стационарных постов определяется в зависимости от численности населения в городе, площади населенного пункта, рельефа местности и степени индустриализации,

расположения мест отдыха. Зависимость количества стационарных постов от численности населения представлена в таблице 1. Мониторинг атмосферного воздуха на стационарных постах осуществляется по одной из четырех программ. Одновременно с отбором проб воздуха на постах определяют следующие метеорологические параметры: направление и скорость ветра, температуру и влажность воздуха.

Таблица 1 - Зависимость количества
стационарных постов от численности населения

Численность населения тыс. чел	Количество стационарных постов
< 50	1
50 - 100	2
100 - 200	3
200 - 500	3 - 5
500 - 1000	5 - 10
1000 - 2000	10 - 15
>2000	15 - 20

В работе была изучена система организации мониторинга на стационарных постах г. о. Тольятти. Систематическое наблюдение за содержанием в атмосферном воздухе города Тольятти вредных веществ осуществляет Тольяттинская специализированная гидрометеорологическая обсерватория. Наблюдения проводятся на 8 стационарных постах наблюдения за качеством атмосферного воздуха (ПНЗ) с периодичностью отбора 5 дней в неделю, 3 раза в сутки. ПНЗ расположены почти во всех административных районах города.

Места расположения стационарных постов в городе Тольятти представлены на рис. 1.

На ПНЗ осуществляется наблюдение за содержанием в атмосферном воздухе основных и специфических загрязнителей. Для нашего города к специфическим загрязняющим веществам, за которыми ведется мониторинг, относятся аммиак, формальдегид, оксид азота, гидрофторид, углеводороды, толуол, бензол, этилбензол, ксилол и ряд тяжелых металлов, в том числе свинец и бензапирен. Были изучены воздействия загрязнителей атмосферного воздуха города Тольятти на окружающую среду и здоровье населения (таблица 2).

Рисунок 1 - Места расположения стационарных постов

В процессе исследования изучены методы отбора проб атмосферного воздуха, применяемые на стационарных постах города Тольятти. Отбор проб осуществляется путем аспирации. Для этого используются электроаспираторы. После отбора пробы воздуха доставляют в лабораторию, где осуществляется их химический анализ. Методы химического анализа проб

воздуха также были изучены в процессе работы. В городе Тольятти химический анализ проб воздуха осуществляет Тольяттинская специализированная гидрометеорологическая обсерватория.

Таблица 2 - Воздействия загрязнителей атмосферного воздуха города Тольятти на окружающую среду и здоровье населения

Вещество	Воздействие
Диоксид азота	- Вызывает болезни дыхательных путей: катар верхних дыхательных путей, бронхиты, круп и воспаление легких. - Вызывает обесцвечивание листьев, увядание цветков, прекращение плодоношения и роста у растений.
Оксид углерода	- Вызывает острый недостаток кислорода, нарушение клеточного дыхания, удушье
Диоксид серы	- Вызывает болезненные явления в лёгких и дыхательных путях, иногда возникают отёк лёгких, глотки и паралич дыхания, нервные расстройства, нарушением умственной деятельности - Вызывает у растений деформации и некрозы ассимиляционных органов, ингибирование фотосинтеза, изменение метаболизма, увеличение восприимчивости к болезням и вредителям, ускорение старения
Пыль	- Повышается частота заболеваний раком. - Вызывает хронические заболевания дыхательных путей, астмой, бронхитом, эмфиземой легких. - Нарушение системы кровообращения.
Аммиак	- При высокой концентрации паров вызывает возбуждение и бред. - При контакте с кожей вызывает жгучую боль, отек, ожег с пузырями. - При хронических отравлениях наблюдаются расстройство пищеварения, катар верхних дыхательных путей, ослабление слуха. - Вызывает сильный кашель и удушье
Формальдегид	Постоянное воздействие высококонцентрированного вещества может привести к мутации органов. - Оказывает побочное действие на ЦНС, вызывая головные боли, утомление и подавленность, бледность, депрессия, затрудненное дыхание, нередко судороги по ночам - Потенциально может вызывать астму и астматические приступы

Был проведен анализ данных мониторинга загрязнения атмосферного воздуха на стационарных постах, с учетом данных о метеорологической обстановке, в городе Тольятти. Все данные были взяты с сайта Приволжского управления по гидрометеорологии и мониторингу окружающей среды. Сбор данных проводился в период летней практики, с понедельника по пятницу. Целью их анализа является выявление превышений ПДКм.р. и ПДКс.с. загрязняющих веществ в атмосферном воздухе и влияния на его загрязнение погодных условий. Поскольку на сайте фактические концентрации загрязняющих веществ сравниваются только с ПДКм.р., для более полного анализа данных были дополнительно использованы нормативы среднесуточных предельно допустимых концентраций ПДКс.с. для веществ, по которым проводился мониторинг, чтобы оценить не только опасность химического загрязнения воздуха, но и вредность его воздействия.

В результате анализа данных мониторинга атмосферного воздуха на стационарных постах, на территории города Тольятти, в летний период, были выявлены превышения ПДКс.с. у пыли, диоксида азота, аммиака, формальдегида и гидрофторида. Превышения были зафиксированы почти на всех ПНЗ. Далее выполнялся графический анализ полученных данных, они были представлены в виде диаграмм, позволяющих оценить наиболее частые и сильные

превышения ПДКс.с., и дату, когда они произошли. Превышений ПДКм.р. обнаружено не было.

Были проанализированы данные по погодным условиям в рассмотренный период. Из-за однородности метеорологических параметров, закономерностей между ними и изменениями концентраций загрязняющих веществ в атмосферном воздухе выявлено не было.

На ПНЗ 3 ПДКс.с. пыли была превышена на 0,05 мг/м³.

На ПНЗ 9 ПДКс.с. пыли была превышена на 0,15 мг/м³ (в два раза).

На ПНЗ 7 ПДКс.с. пыли была превышена на 0,05 мг/м³.

На ПНЗ 8 ПДКс.с. пыли была превышена на 0,05 мг/м³.

На ПНЗ 9 ПДКс.с. диоксида азота была превышена на 0,037 мг/м³ (почти в два раза).

На ПНЗ 8 ПДКс.с. диоксида азота была превышена на 0,013 мг/м³,

На ПНЗ 4 ПДКс.с. диоксида азота была превышена на 0,038 мг/м³ (почти в два раза)

На ПНЗ 9 ПДКс.с. формальдегида была превышена на 0,019 мг/м³ (почти в три раза).

На ПНЗ 7 ПДКс.с. формальдегида была превышена на 0,013 мг/м³ (более чем в два раза).

На ПНЗ 4 ПДКс.с. формальдегида была превышена на 0,018 мг/м³ (почти в три раза).

На ПНЗ 2 ПДКс.с. аммиака была превышена на 0,03 мг/м³.

На ПНЗ 3 ПДКс.с. аммиака была превышена на 0,08 мг/м³ (в три раза).

На ПНЗ 7 ПДКс.с. аммиака была превышена 28.06.2017 на 0,07 мг/м³ (почти в три раза).

На ПНЗ 10 ПДКс.с. аммиака была превышена 28.06.2017 на 0,05 мг/м³ (более чем в два раза).

На ПНЗ 11 ПДКс.с. гидрофторида была превышена на 0,007 (более чем в два раза) мг/м³.

По результатам выполненной работы можно сделать следующие выводы:

1. Были изучены теоретические основы мониторинга атмосферного воздуха на стационарных постах;
2. Была изучена система мониторинга атмосферного воздуха на стационарных постах в городе Тольятти;
3. Изучены воздействия загрязнителей атмосферного воздуха города Тольятти на окружающую среду и здоровье населения;
4. Были изучены методы отбора проб атмосферного воздуха, применяемые на стационарных постах, в г. Тольятти и методы их химического анализа, применяемые в Тольяттинской специализированной гидрометеорологической обсерватории;
5. В результате анализа данных мониторинга атмосферного воздуха на стационарных постах, и метеорологических условий на территории города Тольятти в летний период 2020 года, были выявлены частые превышения ПДКс.с. у пыли, диоксида азота, аммиака, формальдегида и гидрофторида;
6. Превышений ПДКм.р. за рассмотренный период обнаружено не было.
7. Были проанализированы данные по погодным условиям в летний период 2020года. Из-за однородности метеорологических параметров, закономерностей между ними и изменениями концентраций загрязняющих веществ в атмосферном воздухе выявлено не было.

Библиографический список

1. Афанасьев, Ю.А., Фомин, С.А. Мониторинг и методы контроля окружающей среды / Учебн. пособие. - М.: Изд-во МНЭПУ, 2018. – 468 с.

2. Мониторинг загрязнения атмосферного воздуха — г. о. Тольятти. [Электронный ресурс] – Режим доступа: http://pogoda -sv.ru/monitoring/ecology_aero/sam/tol.php

ОРГАНИЗАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Абросимова А.Е., студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Одним из важных аспектов деятельности производственной системы является обеспечение информационной безопасности на рабочих местах пользователей. Под информационной безопасностью на рабочих местах понимается, в первую очередь, наличие актуальной информации, ее сохранность, защита доступа к ней, снижение рисков потери информации. Поэтому проектирование информационной системы является на наш взгляд необходимым условием эффективной работы с информацией.

Целью публикации является обзор существующей организационной системы по защите информации на примере конкретного подразделения виртуального предприятия. Показана организационно-управленческая модель защиты информации на рабочих местах и описан функционал служб, которые обеспечивают деятельность этой модели.

Как известно, из источников литературы [1], под информационной безопасностью подразумевают процесс обеспечения конфиденциальности, целостности и доступности информации.

Информационную безопасность можно разбить на три важных аспекта:

- доступность
- целостность
- конфиденциальность

Нарушение аспектов может быть вызвано различного рода опасного воздействия сторонних лиц на информационную безопасность. При нарушении хотя бы одного из аспектов информационная безопасность перестаёт существовать.

Анализ существующих подходов к построению информационной безопасности [2] показал, что доктрина информационной безопасности решение вопросов информационной безопасности дает возможность устойчивого развития предприятия в условиях неблагоприятной внешней среды. А использование стандартов позволяет определить виды возможных рисков, свойственных той или иной производственной системе [3].

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть: ошибки в работе персонала; сбои в технологической среде; непредсказуемые жизненные обстоятельства и стихийные бедствия; некорректная работа в линиях связи из-за воздействия внешней среды.

Для анализа существующей организационной системы по обеспечению защиты информации было выбрано подразделение промышленного предприятия. Подразделение занимается управлением различного рода машин (с двигателем мощностью более 110,3 кВт), а также обслуживанием и ремонтом их двигателей.

На рисунке 1 показана обобщенная организационная структура управления информационной безопасностью.

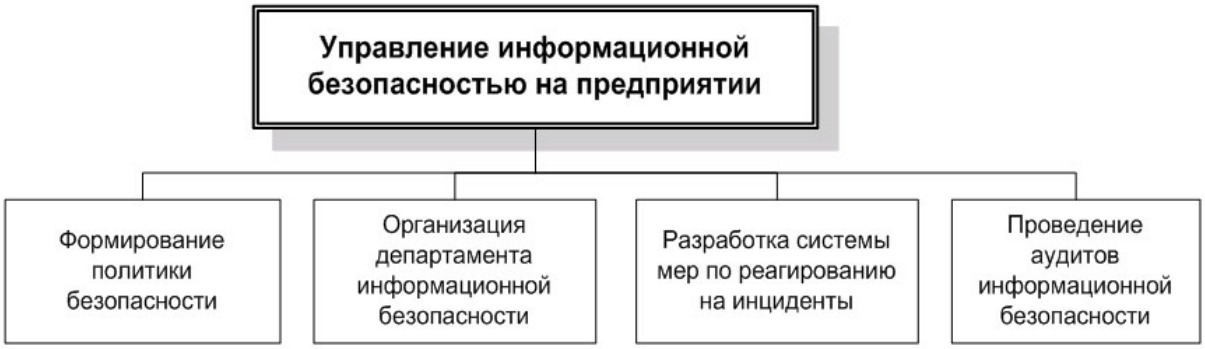

Рисунок 1 - Структура управления информационной безопасностью в подразделении

Обеспечение информационной безопасности можно подразделить на пять уровней:

1. Законодательный уровень. (Определяет порядок защиты информации, находится в различного рода нормативных актах, законах).
2. Административный уровень. (Действия общего характера, предпринимаемые руководством подразделения).
3. Морально-этический уровень. (Различного рода нормы поведения, обязательные к соблюдению).
4. Информационный уровень. (Электронные устройства и специальные программы защиты информации).
5. Физический (Препятствия механического, электронного и механически-электронного рода на возможных путях проникновения потенциальных нарушителей).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Аудит информационной безопасности, проведенный автором в октябре 2020 года на примере виртуального предприятия показал, что в основном, имеются ошибки персонала по невнимательности (рис. 2).

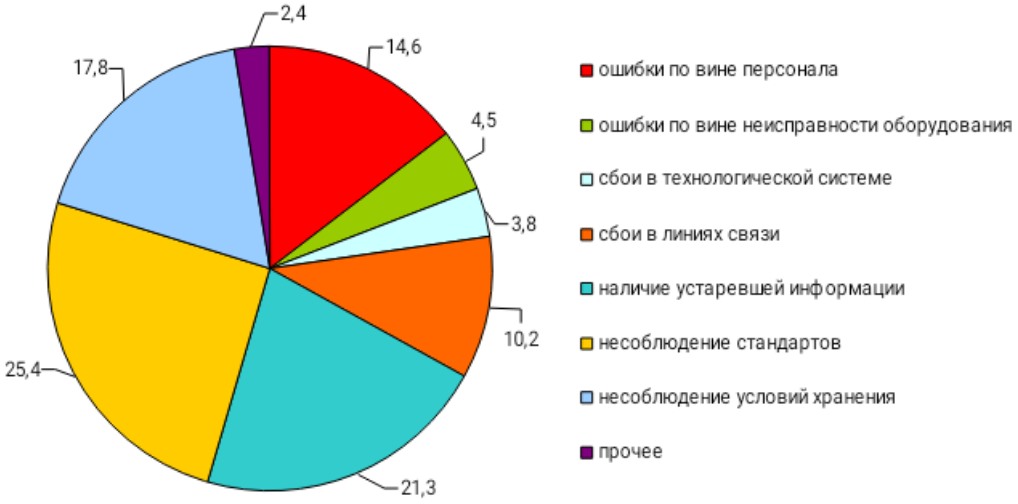

Рисунок 2 - Аудит нарушений деятельности персонала подразделения

Анализ работы [2] показал, что нужны специалисты, имеющие навыки обнаружения и локализации угроз. Они должны полностью представлять себе принципы функционирования информационной безопасности и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Для этого можно рекомендовать к изучению стандарт [4], в котором описаны требования к компетенциям специалистов, которые занимаются защитой информации.

Выводы. Благодаря обзору существующей организационной системы по защите информации на примере виртуального машиностроительного производства мы можем сделать вывод о том, что обеспечение безопасности информационной системы необходимо для полноценной работы подразделения предприятия.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 № Пр-1895) и Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
2. Глухова, Л.В. Губанова, С.Е. Некоторые аспекты менеджмента информационной безопасности промышленных комплексов. // Вестник Волжского университета им. В.Н. Татищева, 2015, № 3 (34). С. 135-144.
3. Информационная безопасность и защита информации. Учебное пособие – М.: 2004 – 82 с. http://bezopasnik.org›article/book/23.pdf.
4. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

УДК 517.9

СМЕШАННАЯ КРАЕВАЯ ЗАДАЧА ДЛЯ УРАВНЕНИЯ КОЛЕБАНИЙ СТРУНЫ

Виноградов В., магистрант
Научные руководители: Казиев В.М., к. ф.-м. н., доцент
Кабардино-Балкарский госуниверситет им. Х.М. Бербекова
г. Нальчик, Россия
Глухова Л.В., д. э. н., профессор
Волжский университет им. В.Н. Татищева
г. Тольятти, Россия

Введение

К нагруженным относят уравнения класса $Lu + Tu = f$, где L – оператор (произвольного типа, например, дифференциальный), рассматриваемые в соответствующих задачам областях $\Omega \subset R_n(x_1, x_2, ..., x_n)$, T – оператор, задающий «след» искомого решения на некотором многообразии Ω. Такие уравнения практически-ориентированные, например, описывают процессы регулирования уровня влаго- и солесодержания в почвогрунте.

Исследовали описываемые нагруженными уравнениями задачи ряд авторов, например, к данной работе близки теоретические работы АМ. Нахушева [1], А.Х. Аттаева [2], Казиева В.М., Кудаевой Ф.Х. и Кайгермазова А.А. [3], практически значимые работы Л.И. Сербиной [4], Полубариновой-Кочиной П.Я. [5], а также спектральные исследования Е.И. Моисеева [6].

Рассматриваемая задача актуальна и теоретически, и практически, «нагрузка» в уравнении отражает дискретное воздействие (в точках «нагружения») на процесс, например, на инновационный процесс управления предприятиями [7].

Постановка и исследование задачи

Рассмотрим смешанную задачу нахождения регулярного решения нагруженного уравнения колебания струны в области $\Omega \subset R_2(x, y), \quad 0 < x < l, t \geq 0$:

$$u_{tt} - u_{xx} - \lambda_0 u(x, t_0) = 0,$$

удовлетворяющее условиям:

$$u(x,0) = f(x), \;\; u_t(x,0) = g(x), \;\; u(0,t) = u(l,t) = 0.$$

Исследуем эту задачу для функций: $g(x) \in C(\overline{\Omega})$, $f(x) \in C'(\Omega)$. Будем искать методом Фурье [8] частные нетривиальные решения уравнения вида $u(x,t) = X(x)T(t)$. Подставляя в уравнение и учитывая граничные условия, получим:

$$X \cdot T'' - X'' \cdot T + \lambda_0 \cdot X \cdot T(t_0) = 0$$

или, разделяя переменные,

$$\frac{X''}{X} = \frac{T'' + \lambda_0 \cdot T(t_0)}{T} = \mu.$$

Как и для ненагруженных уравнений, постоянная $\mu < 0$. Действительно, допуская $\mu \geq 0$, получаем, что есть нетривиальные функции искомой формы:

$$X(x) = C_1 e^{\sqrt{\mu} \cdot x} + C_2 e^{-\sqrt{\mu} \cdot x}.$$

Это невозможно, вводим обоснованное обозначение $\mu = -\lambda^2$. Тогда

$$X(x) = C_1 \cos \lambda x + C_2 \sin \lambda x$$

и для уравнения

$$T'' + \lambda^2 (T + \frac{\lambda_0}{\lambda_2} T(t_0)) = 0$$

и по стандартной схеме метода Фурье [7] получаем:

$$T(t) = C_3 \cos \lambda t + C_4 \sin \lambda t - \frac{\lambda_0}{\lambda^2} T(t_0).$$

Пусть $t = t_0$. Тогда получим:

$$T(t_0) = \frac{(C_3 \cos \lambda t_0 + C_4 \sin \lambda t_0)\lambda^2}{\lambda_0 + \lambda^2},$$

при условии, что $\lambda_0 + \lambda^2 \neq 0$.

Следовательно,

$$T(t) = C_3 \left[\cos \lambda t - \frac{\lambda_0 \cos \lambda t_0}{\lambda_0 + \lambda^2} \right] + C_4 \left[\sin \lambda t - \frac{\lambda_0 \sin \lambda t_0}{\lambda_0 + \lambda^2} \right].$$

Из условий задачи следует, что при

$$\lambda_0 + \frac{\pi^2 \cdot n^2}{l^2} \neq 0,$$

можно записать:

$$u(x,t) = \sum_{n=1}^{\infty} \sin \frac{\pi n x}{l} \cdot \left\{ \left[\cos \frac{\pi n t}{l} - \frac{\lambda_0 l^2 \cos \frac{\pi n}{l} t_0}{\lambda_0 l^2 + \pi^2 n^2} \right] C_{3n} + \left[\sin \frac{\pi n t}{l} - \frac{\lambda_0 l^2 \sin \frac{\pi n}{l} t_0}{\lambda_0 l^2 + \pi^2 n^2} \right] C_{4n} \right\}$$

Функция *u*, определенная данным равенством, удовлетворяет условиям (по способу построения $u_n(x,t)$). Она будет из класса $C^2(t > 0,\ 0 \leq x \leq l)$, если ряд можно дифференцировать дважды и после этого он будет равномерно сходящимся.

Соответствующее утверждение доказано путем поиска коэффициентов (множителей). Окончательно, решение задачи записывается в виде:

$$u(x,t) = \sum_{n=1}^{\infty} \sin \frac{\pi n x}{l} A_n \left\{ \left[\cos \frac{\pi n t}{l} - \frac{\lambda_0 l^2 \cos \frac{\pi n t_0}{l}}{\lambda_0 l^2 + \pi^2 n^2} \right] + B_n \left[\sin \frac{\pi n t}{l} - \frac{\lambda_0 l^2 \sin \frac{\pi n t_0}{l}}{\lambda_0 l + \pi^2 n^2} \right] \right\}.$$

Пример. Рассматривается вышеприведенная задача для уравнения вида:

$$u_t - u_{xx} - \lambda u(x_0, t_0) = 0.$$

Аналогично, как и выше, решение находим в виде:

$$u(x,t) = \frac{4l^2}{\pi^3} \sum_{i=1}^{\infty} \left(\frac{1}{(2i-1)^3} \sin \frac{\pi(2i-1)x}{l} - \frac{1}{(2i-1)^3} \sin \frac{\pi(2i-1)x}{l} \exp\left(-\frac{\pi^2 (2i-1)^2 t}{l^2} \right) \right).$$

Условие сходимости и «непопадания в спектр» обеспечивается тем, что ряд

$$\sum_{i=1}^{\infty} \left(\frac{1}{(2i-1)^3} \sin \frac{\pi(2i-1)x}{l} \right)$$

сходится, как мажорируемый рядом с членами вида:

$$\left| \frac{1}{(2i-1)^3} \sin \frac{\pi(2i-1)x}{l} \right| \le \frac{1}{(2i-1)^3}.$$

Заключение

Рассмотренная задача – «демонстратор» применения метода Фурье к нагруженным уравнениям, не относящихся к классическим уравнениям в частных производных. Но результат применим и на практике – для прогноза, идентификации «нагружения», в системах управления процессами.

Библиографический список

1. Нахушев, А.М. Нагруженные уравнения и их приложения. – М.: Наука, 2012. -232 с.
2. Аттаев, А.Х. Характеристическая задача для нагруженного вдоль одной из своих характеристик гиперболического уравнения второго порядка // Вестник КРАУНЦ. Физ.-мат. науки, 2018, № 3(23), с. 14–18.
3. Казиев, В.М., Кудаева, Ф.Х., Кайгермазов, А.А. Задача Коши для нагруженного вырождающегося гиперболического уравнения. Вестник Бурятского государственного университета. Серия «Математика, информатика», 2018, №1. –с.95-99.
4. Сербина, Л.И. Нелокальные математические модели переноса в однородных системах. – М.: Наука, 2007. - 167 с.
5. Полубаринова-Кочина, П.Я. Теория движения грунтовых вод. - М.: Наука, 1977. - 664 с.
6. Моисеев, Е.И. Уравнения смешанного типа со спектральным параметром. – М.: МГУ, 1988. – 150 с.
7. Глухова, Л.В. Концептуальные основы управления инновационным потенциалом предприятия // Вестник волжского университета им. В.Н. Татищева, 2017, т. 2, №1. - с. 117-121.
8. Демченко, В.В. Уравнения и системы уравнений с частными производными первого порядка: учеб. пос. по направлению «Прикладные математика и физика». - 2-е изд. - М.: МФТИ, 2004. - 116 с.

ВЕБ-МОНИТОРИНГ И МОДЕЛИРОВАНИЕ ВЛИЯНИЯ ОКРУЖАЮЩЕЙ СРЕДЫ НА ЗОЖ

Науржанов А., магистрант
Научные руководители: Казиев В.М., к. ф.-м. н., доцент
Кабардино-Балкарский госуниверситет им. Х.М. Бербекова
г. Нальчик, Россия
Глухова Л.В., д. э. н., профессор
Волжский университет им. В.Н. Татищева
г. Тольятти, Россия

Введение

Информационные, антропогенные и природные риски в современном обществе растут, снижается устойчивость взаимодействующих с окружением систем, нарастают угрозы. Тре-

буется релевантная методология учета, оценки и анализа рисков, базирующаяся на основах системного анализа [1], самоорганизационных инновационных процессов [2]. Обычно используют подход риск-оценок по многофакторным статистико-математическим моделям с региональной привязкой [3]. Получаемые модели также «регионально привязанные».

Веб-мониторинг ЗОЖ

Здоровье – следствие ЗОЖ, а также экологии и наследственности. Только 12% определяет сама медицина, медицинское обслуживание. Усугубляет ситуацию также отсутствие ЗОЖ-мониторинга выборки населения, оценок здоровья каждого индивида или группы индивидов в заданной системе региональных и национальных норм. В ЗОЖ-мониторинг включено оценивание адаптационных возможностей, перенесенных (текущих) болезней, психофизиологическое состояние организма, особенно, нервной системы.

Особенно необходимо «мониторить» ЗОЖ школьников (студентов), оно имеет тенденцию ухудшаться. До 78% завершивших обучение имеют заболевания, почти половина употребляет психотропные активаторы. Новые ФГОС дополнены нормативами и требованиями по оценке не только успеваемости, но и условий самого образования (например, САНПиН работы за ПК).

Веб-системы поддержки решений в ЛПУ необходимы для перехода от эвристической, опытной медицины (больше на жалобах и «сказаниях» пациентов) к медицине доказательной (на клинических исследованиях, данных биохимии).

Путь лечения – применение интеллектуального анализа, DataMinning, BigData и других передовых инструментов. Это дает понять клинику заболевания, лучшую ситуационную картину. Персонифицируя данные ЗОЖ, можно решать задачи мониторинга и профилактики ЗОЖ, перехода от терапевтической (преимущественно) медицины к медицине профилактической, диагностической, с веб-возможностью высвобождения до 40% рабочего времени электронным документооборотом (сравнительно с «бумажными карточками»). Результат – быстрое выздоровление.

Влияния информационного воздействия на ЗОЖ

Главным учитываемым фактором чаще является загрязнение воздуха, а основными учитываемыми характеристиками популяции, организма – время (возраст), генетика, социальные, здравоохранительные и др. К основным рискам смертности по результатам ряда исследований (см., например, [4]) относятся инфаркты, инсульты, болезни легких и др.

Основанными загрязнителями стали диоксид азота, формальдегид и др. Основной идентифицируемой моделью – регрессионная зависимость смертности от загрязнения атмосферного воздуха:

$$\ln y = \alpha_0 + \sum_{i=1}^{k} \alpha_i x_{i,t-\tau},$$

где $\alpha_0, \alpha_1, \dots, \alpha_k$ – идентифицируемые параметры модели, t – время, τ – временной лаг воздействия загрязнителя, $x_{i,t-\tau}$ – факторы (параметры), y – прогнозируемый фактор.

Результаты моделирования реальных ситуаций показывают:

1) наибольшим вкладом в смертность отличается загрязнение воздуха;
2) наименьшим вкладом болезней в смертность – инсульты;
3) наибольшему влиянию факторов среды подвержены женщины, как и наибольшему лагу;
4) наибольшие коэффициенты корреляции – у болезней органов дыхания.

Риск-мониторинг можно реализовать процедурой матричной оценки степеней риска (матрицы рисков *R*, в которой строки – категории, а столбцы – факторы рисков):

$$R = ||r_1 ij\ ||, i = 1, \dots, m; j = 1, \dots, n.$$

Тяжесть риска ЗОЖ (заболевания) может оцениваться, например, зависимостью

$$g_i = 1 - e^{\frac{\ln(1-g]_m)}{T_m} T_i},$$

g_m, T_m – усредненная тяжесть и длительность воздействия, *i*-го заболевания.

Заключение

Результаты ЗОЖ-мониторинга и прогнозирование ущерба, рисков реально необходимы, чтобы скорректировать показатели ЗОЖ обучаемых, например, по этим данным рекомендуется посещать психолога, физиотерапевта и других специалистов. В работе осуществлен веб-мониторинг данных по ЗОЖ, апробированы ряд различных моделей, в частности, приведенная выше регрессионная модель.

Библиографический список

1. Глухова, Л.В., Казиев, В.М., Казиева, Б.В. Системные правила финансового контроля и управления инновационными бизнес-процессами предприятия // Вестник Волжского университета имени В.Н. Татищева, 2018, т. 2, № 1. - с. 118-126.
2. Глухова, Л.В., Казиева, Б.В., Казиев, К.В., Казиев, В.М., Шерстобитова, А.А. Управление деятельностью инновационных систем в условиях неопределенности и риска // Вестник Волжского университета имени В.Н. Татищева, 2020, т. 2, № 3(46). - с. 50-59.
3. Черных, Д.А., Тасейко, О.В., Иванова, У.С. Анализ влияния факторов окружающей среды на смертность населения г. Красноярска. // Сборник материалов конференции «Обработка пространственных данных в задачах мониторинга природных и антропогенных процессов (SDM-2019)». – Бердск, 2019. – с. 480-484.
4. Pend, R.D., Dominici, F., Louis, T.A. Model choice in time series studies of air pollution and mortality // Journal of the Royal Statistical Society. Series A. 2006, vol. 169, pp. 179-203.

БИОЭНЕРГИЯ КАК ВАЖНЕЙШИЙ ФАКТОР ПРОИЗВОДСТВА АЛЬТЕРНАТИВНЫХ ИСТОЧНИКОВ ЭНЕРГИИ

Сараквашин Д.А., финансовый аналитик
ООО НПО «Газспецстрой»
г. Москва, Россия
Щукина А.Я., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Растущие потребности в энергии удовлетворяются в настоящий момент в основном за счет увеличения использования ископаемого углеводородного топлива, что увеличивает давление на экологию со стороны энергетики.

Особая роль в решении обозначенной задачи обеспечения эколого-ориентированной энергетической безопасности и ресурсосбережения принадлежит нетрадиционной возобновляемой энергетике, одно из центральных мест в которой занимает биоэнергетика, основанная на преобразовании энергии биомассы и биоотходов. В последние годы в мире наблюдается стремительное развитие инновационных технологий, использующих биоресурсы для производства топлива и энергии. Однако не все реализуемые биоэнергетические проекты, направленные на замещение традиционных энергоносителей, оказываются успешными с коммерческой и экономической точки зрения, что связано, в первую очередь, с отсутствием универсального методического и информационного обеспечения выработки и принятия эффективных управленческих решений по выбору технологий биоэнергетики.

Современная биоэнергетика – это интенсивно развивающаяся отрасль мировой экономики, основанная на инновационных технологиях преобразования энергии биомассы, представляющей собой совокупную массу живых организмов и относящейся к возобновляемым природным ресурсам. Из биомассы и биоотходов можно производить тепло, электричество, а также экологически чистое, биоразлагаемое моторное биотопливо (биодизель, биоэтанол, биометанол, биобутанол).

Одно из главных преимуществ биоэнергетики заключается в том, что она создает предпосылки для обеспечения экономического роста и связанного с ним увеличения энергопотребления (на 1-2% ежегодно) без разрушения окружающей среды. Выбросы углекислого

газа, образующиеся при сжигании любого биотоплива, т.е. топлива, полученного из сырья или отходов биогенного происхождения, минимальны, Биотопливо относится к CO_2 - нейтральным видам энергоресурсов и не считается загрязнителем атмосферы.

Глобальная энергетическая безопасность определяется, в первую очередь, обеспеченностью топливными и иными ресурсами для производства энергии. Валовый энергетический потенциал биомассы на Земле составляет 10^{14} Вт и в 10 раз превосходит мощность современной энергетики. Для РФ валовый потенциал энергии биомассы достигает сейчас 470 млн т у.т./год, технический – 130 млн т у.т./год, экономический – 70 млн т у.т./год. Потребление энергоресурсов в России в настоящий момент превышает 1 млрд т у.т./год (1.4 т у.т. = 1 т н.э.). Поэтому биомасса уже сейчас может обеспечить более 10% потребляемой в стране энергии. Доля энергии, получаемой из биоресурсов, составляет в РФ около 2%, в мире – примерно 10%. В ближайшие десятилетия прогнозируется увеличение вклада биомассы в мировое производство топлива и энергии.

В результате этого, проведен анализ причин, ускоряющих и замедляющих замещение традиционных углеводородных энергоносителей биотопливом.

Рассматриваем возможности биоэнергетики в решении проблем ресурсосбережения и охраны окружающей природной среды проанализируем достоинства и недостатки различных способов преобразования энергии биомассы, которая используется в энергетике в виде древесных отходов; быстрорастущих деревьев и кустов, специально выращиваемых для энергетических целей; бытовых, сельскохозяйственных и некоторых промышленных отходов биоорганического происхождения, а так же в виде ряда сельскохозяйственных и водных растений, которые в основном служат сырьем для производства моторного биотоплива.

Биоэнергетика является инновационной эколого-ориентированной отраслью экономики, способствующей не только решению проблем, связанных с ростом энергопотребления, но и развитию технологий утилизации отходов, что улучшает экологическую обстановку в различных регионах мира.

Для энергетических целей биомасса используется в основном в виде твердого топлива (дров, опилок, щепы (измельченного древесного сырья), соломы, прессованных древесных и сельскохозяйственных отходов – брикетов и топливных гранул (пеллет), которое замещает в котлах, каминах, печках, котельных, теплоцентралях и на электростанциях ископаемые углеводородные энергоресурсы. При этом не требуется серьезных модификаций оборудования для сжигания топлива, а выбросы углекислого газа, оксидов серы и других загрязнителей резко снижаются. Минимальное количество отходов и наибольшая теплоотдача, сопоставимая с традиционными энергоносителями, достигаются при сжигании размельченной, гранулированной и спрессованной древесины.

В биогазовых и газогенераторных установках из биомассы и биоотходов получают газообразные виды биотоплива – биометан или биоводород, являющиеся полными аналогами метана и водорода за исключением их происхождения. Для производства биогаза, основной компонентой которого является метан, активно используются сельскохозяйственные, бытовые и некоторые промышленные отходы (навоз, птичий помет, зерновые отходы и отходы спиртового производства из сахара, отходы рыбной и мясной промышленности, сточные воды, трава, молочная сыворотка, технический глицерин от производства биодизеля из рапса, отходы производства соков и переработки картофеля и т.д.).

К перспективным видам сырья для получения путем пиролиза одного из главных видов газообразного биотоплива - биосинтез -газа (биосингаза, синтез-газа, сингаза), состоящего в основном из водорода, относятся древесина, солома, стебли кукурузы, отходы растениеводства, а также твердые бытовые отходы (ТБО). Использование малогабаритных установок мощностью 10 МВт и выше, сжигающих газообразное биотопливо, позволяет обеспечивать тепловой и электрической энергией отдельные населенные пункты и производства, а также создает предпосылки для выработки энергии в промышленных масштабах. Для сжигания газообразного биотоплива подходят обычные газовые котлы ТЭС, ТЭЦ и котельных. Газообразное биогорючее используется также в автотранспортных средствах.

Интенсивное развитие получили в последние годы технологии производства жидкого моторного биотоплива. Сырьем для производства биодизеля служат в основном эфирные масла рапса, сои, кокоса, пальмы или касторовое масло. Перспективными являются те технологии производства биодизеля, которые не используют пресную воду и сельскохозяйственные растения – например, получение биодизеля из богатых маслом водорослей или из отработанного растительного масла. Для производства биоэтанола, биометанола и биобутанола осуществляют сбраживание углеводов. Указанные виды топлива обычно получают из сахарного тростника, кукурузы, пшеницы, картофеля, морского фитопланктона, некоторых пород быстрорастущих деревьев или из соломы.

Отходы производства жидкого биотоплива из кормовых культур используются для выработки комбикормов для скота и птицы. В автотранспортных средствах жидкое биотопливо можно использовать как в чистом виде, так и в смеси с бензином. Затраты на модернизацию бензинового ДВС под биотопливо минимальны.

Современные автомобильные компании производят двигатели, способные работать как на бензине, так и на горючем из биомассы. По своим энергетическим характеристикам жидкое топливо из биомассы незначительно отличается от бензина, но выбросы углекислого газа и других загрязнителей окружающей среды (окиси углерода CO, твердых частиц и т.д.) при сжигании бензина выше. Как следует из отчетов Международного энергетического агентства (МЭА), увеличение использования биотоплива на транспорте в настоящее время обеспечивает около 6% сокращения выбросов CO_2. Из биосинтез-газа можно вырабатывать целый ряд экологически безопасных биосинтетических видов жидкого топлива, которые проще и дешевле транспортировать, хранить и применять в качестве исходного источника энергии на ТЭС, а также котельного и моторного горючего. Указанное топливо названо бионефтью.

На мировом рынке биотоплива основными современными видами топлива, получаемого из биомассы, по количеству вырабатываемой из них энергии являются биоэтанол, биогаз и измельченное древесное сырье – гранулы и щепа. Сейчас в мире ежегодно производится около 15 млн т топливных гранул и примерно 80 млн т щепы. Прогноз предполагает рост производства пеллет до 80 млн т/год к 2021 г. Производство жидкого биотоплива в мире к 2021 г. может превысить 1 трлн. л/год, что сопоставимо с нынешним мировым потреблением бензина.

По данным МЭА и Renewableglobal status report (2009-2014), для мировой биоэнергетики в последние годы характерны достаточно высокие темпы роста как видно по данным таблицы 2, а конкурентоспособность энергии и топлива, выработанных из биомассы, способствует росту инвестиционной привлекательности данной отрасли экономики.

Таблица 2 - Основные показатели развития мировой биоэнергетики

Виды объекта энергетики или технологии	2005	2009	2011	2014	Среднегодовой темп роста, % / год
Электростанции использующие биотоплив,ГВт	44	52	54	~58	5,7
Теплоцентрали и котельные, использующие биотопливо, ГВт	220	250	270	~280	5
Производство биоэтанола, млрд.л	32	67	76	86	21,5
Производства биодизеля, млрд.л	4	12	17	19	38

В таблице 3 представлены данные о среднемировых капиталовложениях в сооружение электростанций на угле, газе и биотопливе, а также о себестоимости производства электроэнергии из указанных ресурсов.

Таблица 3 - Конкурентоспособность электроэнергии, выработанной из биотоплива

Виды электростанции	Капитальные вложения $/кВт		Себестоимость производства электроэнергии, цент $/кВт-ч	
	2005 г.	2030 г.	2005 г.	2030 г.
Электростанции на биотопливе	1000-2500	950-1900	3,1-10,3	3,0-9,6
ТЭС на угле	1000-1200	1000-1250	2,2-5,9	3,5-4,0
ТЭС на газе	450-600	400-500	3,0-3,5	3,5-4,5

Следует отметить, что сравнение экономической эффективности биоэнергетики и традиционной энергетики следует проводить не только на основе данных о себестоимости производства энергии и капитальных вложениях в сооружаемые объекты, но и с учетом будущих рисков, обусловленных возрастанием цен на традиционное топливо и затратами на охрану окружающей среды и сохранение здоровья населения в условиях возрастающей эмиссии загрязнителей, выбрасываемых ТЭС на угле, мазуте и газе. Принимая во внимание указанные риски, можно сделать вывод о том, что технологии биоэнергетики в ближайшие десятилетия смогут конкурировать с традиционными энергетическими технологиями на рынке производства электроэнергии. Современные технологии позволяют производить электричество из биомассы с КПД 30-45%, который сопоставим со средними значениями КПД ТЭС на угле и газе (около 40%).

Исходя из вышеизложенного, биоэнергетику можно считать инновационной эколого-ориентированной отраслью экономики в большинстве регионов мира.

Так как биотопливо является одним из наиболее дешевых и доступных возобновляемых источников энергии, в ближайшей перспективе, вероятнее всего, сохранятся достаточно высокие темпы роста его использования, что создает предпосылки для ускорения темпов замещения традиционной углеводородной энергетики эколого-ориентированной биоэнергетикой.

В таблице 4 приведены собранные сведения о ценах на некоторые виды биогорючего.

В 2014 году, по оценкам экспертов информационно-аналитического агентства «Ифобио», в РФ было произведено около 1 млн тонн топливных гранул из древесины и лузги подсолнечника, что составляет 7,8% от общемировой выработки этого вида энергоресурсов. Большая часть производимых в России топливных гранул и брикетов экспортируется. По данным Росстата, в 2014 году экспорт отечественного биотоплива растительного происхождения (солома, жмых, древесина и т.д.) достиг 3,2 млн тонн, увеличившись за последние 3 года на 10%. Проведенный анализ показывает, что отечественная биоэнергетика является относительно молодой, но быстро развивающейся и перспективной отраслью экономики.

Целесообразность развития эколого-ориентированных биоэнергетических технологий в РФ следует обосновывать, в первую очередь, исходя из запасов, качества и ассортимента имеющегося в стране сырья для указанных технологических процессов, мощности действующих и перспективных производств по преобразованию энергии биомассы, наличия возможности эффективного решения проблем энергосбережения и улучшения экологической обстановки в результате реализации перспективных проектов в сфере биоэнергетики, а также с учетом имеющихся в стране инновационных разработок в области производства биотоплива и биоэнергии. По оценкам экспертов, Россия является мировым лидером по запасам биомассы, которую можно использовать в энергетике и топливной промышленности.

Основным биотопливным ресурсом в РФ является древесина, общие запасы которой составляют 23% от общемировых запасов и превышают 82 млрд $м^3$, что эквивалентно 41 млрд тонн. В таблице 5 представлены обобщенные данные об энергетическом потенциале биомассы и биоотходов в РФ.

Таблица 4 - Цены на различные виды биотоплива

Вид биотоплива	Цена
Биоэтанол	0,4-0,6 евро/л (ЕЭС); 0,3 $/л. (США); 0,2 $/л (Бразилия)
Биогаз	0,5 евро/л (ЕЭС)
Пеллеты	200 евро/т (ЕЭС)
Биодизель	0,4-0,8 $/л
Биобутанол	1 $/л (США)
Газообразно и жидкое биотопливо 2-го поколения, получаемое путем пиролиза	<1 евро/л (ЕЭС)
Биотопливо 3-го поколения из водорослей	0,75 $/л (США)

Таблица 5 – Энергетический потенциал биомассы и биоотходов в РФ

Наименование показателя	Отходы АПК	Бытовой мусор	Древесные отходы	Лес	Топливные культуры резервных сельскохозяйственных земель
Накопление, млн. т/год	~ 773	~ 50	~ 50	>400	~225
Энергосодержание, млн. т у.т.	~ 100	~ 15	~ 25	>140	~60

Анализ эколого-ориентированных энергетических характеристик различного отечественного сырья биогенного происхождения, показывает, что в российской биоэнергетике к наиболее перспективным видам биомассы относятся: быстрорастущие многолетние деревья – энергетические леса; опилки, а также отходы рубки и переработки древесины; солома и другие отходы АПК; бытовой мусор; сельскохозяйственные культуры низких сортов.

В настоящее время в России имеются передовые высокорентабельные технологии производства биодизеля и биоэтанола, газификации биомассы с КПД 75-85%, получения биотоплива второго поколения.

Таким образом, для развития инновационных технологий эколого-ориентированной биоэнергетики в РФ имеются 3 главные составляющие: передовые промышленные технологии, производства топлива и энергии из биомассы; надежное оборудование для выработки биотоплива и биоэнергии; масштабная сырьевая база.

Библиографический список

1. Анализ эффективности технологий переработки типовых отходов, создающих одинаковые проблемы во всех регионах, и рекомендаций по их внедрению. [Электронный ресурс] - Режим доступа: http://www.waste.ru/uploads/library/tech_waste.pdf, свободный.

2. Биогаз - новый путь в будущее. [Электронный ресурс] - Режим доступа: http://www.rosbiogas.ru/, свободный.

3. Конец «мусорной цивилизации»: пути решения проблемы отходов. [Электронный ресурс] - Режим доступа: http://libed.ru/knigi-nauka/1168057-1-sapozhnikova-konec-musornoy-civilizacii-puti-resheniya-problemi-othodov-izdanie-podgotovleno-pri-podderzhke-pre.php, свободный.

4. Ефремова, Т.В., Щукина, А.Я. Смена вектора развития эколого-ориентированной направленности: Монография. - Тольятти: Изд-во Волжского ун-та имени В.Н. Татищева, 2015. - 293 с.

5. Современные тенденции развития биоэнергетики 2019 год. [Электронный ресурс] - Режим доступа: https://www.c-o-k.ru/articles/ sovremennye-tendencii-razvitiya-bioenergetiki

ПРОБЛЕМА ПОВОРОТА ВЕКТОРА СОВРЕМЕННОЙ ЭКОНОМИКИ В СТОРОНУ ЭКОЛОГООРИЕНТИРОВАННОЙ НАПРАВЛЕННОСТИ

Сараквашин Д.А., финансовый аналитик
ООО НПО «Газспецстрой»
г. Москва, Россия
Щукина А.Я., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Процесс глобализации, развертывающийся по инициативе постиндустриальных государств, транснациональных корпораций и всемирных организаций должен способствовать переходу мирового сообщества не к постиндустриальному, а к устойчивому будущему всей цивилизации.

В переходе к устойчивому развитию Россия имеет ряд особенностей (в первую очередь имеются в виду высокий интеллектуальный потенциал и наличие мало затронутых хозяйственной деятельностью территорий, составляющих более 60 % всей территории страны), благодаря которым она может сыграть роль лидера в переходе к новой цивилизационной модели развития. В настоящее время важно выйти из системного кризиса, обрести относительно стабильное и безопасное состояние, из которого можно наименее болезненно начать переход на траекторию устойчивого развития.

Мировой системный кризис, оказывает сильное негативное влияние на инновационное развитие России и ставит под сомнение возможность реализации инновационной стратегии развития ее экономики, так как она требует огромных капиталовложений. Положение усугубляется продолжающимся кризисом, связанным с развитием событий на Украине, Сирии. Есть три слоя в этом кризисе. Мы из кризиса не можем выйти в прежнюю модель, поскольку прежняя модель — сырьевая. Возврат в неё спровоцировал замедление инвестиционного процесса, итогом которого стало падение темпов роста. Это произошло ещё до марта 2014 года.

Второй слой — колебания на мировом рынке, связанные с падением цен на нефть, что снизило предложение, отсюда уменьшение ее потребления. Это спровоцировало конкурентную войну саудитов за передел нефтяного рынка — против инновационной американской экономики в этой области. Причиной падения спроса является замедление темпов экономического развития Китая и рецессия в Еврозоне. Однако спрос снижался меньшими темпами, чем нарастало предложение.

Все эти процессы усиливают санкции — третий слой кризиса. Возникла проблема в необходимости рефинансировать корпоративные долги, что составляет около 130 миллиардов долларов дополнительно, которые страна платит и которые бы не платила, если бы компании могли привлечь средства с зарубежных рынков. Это треть валютного запаса национального банка. В современных условиях эти процессы осложняются пандемией, что способствует более глубокому протеканию системного кризиса в России.

В связи с этим в сфере инноваций возникают проблемы. В условиях кризиса государство должно тратить средства и на свое развитие, т.е. на нейтрализацию негативных воздействий кризисных явлений. В настоящее время инновационная деятельность в России базируется в основном на внедрении микро- и псевдоинноваций (модификация разработанных ранее продуктов и технологий). Оценка современного состояния инновационного развития Российской Федерации представлена в таблице 1.

Россия заняла 14-е место в Bloomberg s Global Innovation Index – рейтинге по степени развития инноваций среди самых развитых стран мира, составленном агентством Bloomberg. Аналитики изучили более 200 стран, из которых был впоследствии сформирован Топ-50. Лидером стали США, за ними следуют Южная Корея и Германия, в первую десятку попали сразу шесть стран Евросоюза. Однако в силу объективных причин интерес вызывает скорее не результат (он, по мнению большинства специалистов, более чем спорен), а структура

рэнкинга, которая позволяет сделать вывод о недостатках проводимой инновационной политики и приоритетах дальнейшего развития конкурентоспособности.

Таблица 1 - Основные проблемы развития научной и научно-инновационной активности российской экономик

Состояние инновационной сферы	**Человеческий потенциал**	**Бизнес**	**Наука**
Сформирована частично	Снижение качества образования на всех уровнях - от базового, начального и среднего профессионального	Низкий уровень восприимчивости бизнеса к инновациям технологического характера	Сокращение численности исследователей
Низкая инновационная активность и эффективность работы компаний	Дефицит управленческих кадров в сфере науки, образования, технологий и инноваций	Низкий уровень абсорбционной способности и отдача от реализации технологических	Разрыв поколений
Низкий уровень развития конкурентной среды, стимулирующей использование инноваций	Ограниченный доступ к внешнему финансированию в совокупности с отсутствием собственных		Низкий удельные показатели научной результативности
Низкий уровень взаимодействия науки и бизнеса, коммерциализации научных разработок	Низкий уровень восприимчивости населения к инновациям		Низкий уровень востребованности работ мировым научным сообществом
Низкий уровень эффективности государственных средств, выделяемые на НИОКР.			
Старение научных кадров			
Низкий спрос на инновации в			

В таблице 1 обобщены основные проблемы развития научной и научно-инновационной активности российской экономики. По итогам анализа можно сделать ряд основных выводов о проблемах и противоречиях современной политики России в сфере применения интеллектуального капитала:

- политика государства, направленная на стимулирование частных агентов научной и инновационной сферы, пока себя не оправдала. Так, согласно опросу, проведенному специалистами Института анализа предприятий и рынков ГУ-ВШЭ, большинство предприятий считают свою деятельность «невысоко эффективной»;

- к недостаткам делового и инвестиционного климата по-прежнему можно отнести «отсутствие внятной политики стимулирования иностранных инвестиций», ясной и целенаправленной политики приоритетной направленности иностранных инвестиций в сферы, позволяющие использовать влияние мультипликативного эффекта инвестиций в соответствующие точки роста на развитие определенных сфер народного хозяйства;

- основным барьером для инновационной активности российских предприятий является ограниченный доступ к внешнему финансированию в совокупности с отсутствием собственных средств. Большинство региональных инвестиционных фондов или не финансируют НИОКР или объемы финансирования неприемлемо малы.

Данные таблицы позволяют выделить ряд факторов, определяющих текущее состояние и проблемы развития инновационной сферы экономики России:

1. Слабый спрос со стороны государства и коммерческих структур на результаты научных исследований и, как следствие, снижение инновационной и инвестиционной активности;

2. Низкий уровень ассигнований на академическую науку в целом, и на фундаментальные исследования в частности;

3.Неэффективность финансовых механизмов реализации инновационной политики;

4. Недостаточная правовая поддержка инновационной политики;

5. Недопонимание отдельными представителями законодательной и исполнительной власти, а также руководителями предприятий роли науки и инновационной сферы для развития экономики страны;

6. Низкая конкурентоспособность российских предприятий;

7. Решение проблем по ускорению инновационного развития в значительной мере препятствуют трудности, связанные с принятием обоснованных управленческих решений на долгосрочный период;

8. Большая часть инноваций на российских предприятиях связана с организационно-управленческими, маркетинговыми, инфраструктурными сторонами их деятельности и только незначительная часть предприятий осуществляет нововведения непосредственно в производственной сфере.

Анализ отмеченных выше факторов свидетельствует, что в современных условиях основным звеном инновационной активности могут быть предприятия, которые объективно в наибольшей степени заинтересованы в том, чтобы добиваться определенных конкурентных преимуществ. Как показывает мировая практика, к таким предприятиям относятся, в первую очередь, транснациональные корпорации (ТНК), как российские, так и зарубежные, действующие на территории нашей страны. Осуществление инновационной деятельности предполагает периодическое обновление (модернизацию) продукции определяющей основу хозяйственных результатов данного предприятия и расширение видов его хозяйственной деятельности. В условиях кризиса это могут делать только ТНК.

Учитывая особую важность рассматриваемой проблемы, можно обозначить основные целевые установки перспективного инновационного развития России на 2014-2020гг., к числу которых относятся следующие:

- рост инвестиций в базисную структуру и инновационное обновление основных фондов страны в целом;

- освоение новых рыночных ниш, ускорение темпов экономического роста, концентрация ресурсов бизнеса и государства на прорывных инновационных технологиях, обеспечивающих повышение конкурентоспособности отечественной продукции;

- повышение эффективности использования интеллектуальной собственности, возрождение и реструктуризация научно-технологического потенциала страны, реализация научно-технических достижений и изобретений;

- обеспечение стратегической направленности создаваемых национальной и региональных инновационных систем.

Целевые установки долгосрочного инновационного развития возможно будет реализовать при помощи государственной инновационной политики России, которая сводится к реализации следующих задач:

1. Создание законодательной базы, стимулирующей и поддерживающей инновации и инновационную деятельность, к которой в первую очередь относятся законы: об общих принципах организации инновационной деятельности и проведения исследований и разработок; о защите интеллектуальных прав на объекты научных исследований и разработок; о льготном налогообложении и налоговом стимулировании субъектов инновационной деятельности; о создании особых экономических зон и ином стимулировании субъектов инновационной деятельности;

2. Создание в РФ развитой и эффективной инновационной инфраструктуры, которая нуждается: в государственном финансировании фундаментальных и прикладных исследований, осуществляемых высшими учебными заведениями, исследовательскими институтами и прочими субъектами инновационной деятельности, имеющих стратегическое национальное значение; создание и поддержка технопарков, инновационных инкубаторов,

центров трансферта технологий, инновационно-технологических центров, наукоградов, венчурных фондов и т.д.; финансовая поддержка высшего и профессионального образования для подготовки специалистов по управлению инновационной деятельностью.

3. Прямое финансирование отдельных стратегических национальных программ НИОКР, в том числе с привлечением частного инвестиционного капитала.

Современную национальную инновационную систему можно охарактеризовать как совокупность взаимодействующих элементов государственных и негосударственных секторов экономики, которые обеспечивают оперативное преобразование научных знаний в современные технологии, новые материалы и иную конкурентоспособную продукцию, и представлена на рисунке 1

Рисунок 1 – Схема национальной инновационной системы

Сформированная таким образом государственная инновационная политика и инновационная система России вполне может содействовать трансформации современной экономики в сторону экологоориентированной направленности, а, следовательно, обеспечению безопасности в рамках новой модели, то есть модели устойчивого развития.

Библиографический список

1. Долгосрочная целевая инвестиционная программа обращения с твердыми бытовыми и промышленными отходами в Санкт-Петербурге на 2012-2020 годы. [Электронный ресурс]. Режим доступа: http://www.greenpeace.org/russia/Global/russia/report/toxics/recycle/LIP-part2.pdf., свободный.

2. Урсул, А.Д., Романович, А.Л., Концепция устойчивого развития и проблема безопасности. 2010 г.

3. Васильев, А.Н., Щукина, А.Я. Устойчивое развитие как основа формирования экономики новейшего типа: Монография. - Тольятти: Издательство Волжского университета имени В.Н. Татищева, 2018. – 281 с.

РОЛЬ ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ В ОРГАНИЗАЦИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Труфанова Н., студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

В последние годы Российская Федерация вступила в период собственного бурного становления, связанного с происходящими переменами во всех сферах жизни страны и общества. Впрочем, осуществляемое в РФ реформирование, имеющее целью составление рыноч-

ной домашней системы и правового демократического государства, проходит сложно, иногда очень противоречиво и в том числе и негативно [1]. Одной из ведущих причин, тормозящих старания властей по укреплению государственности, созданию крепкой, разносторонней экономики, направленной на обеспечение размеренного финансового становления страны и общества, их безопасности от финансовых опасностей, считается непостоянность экономической системы РФ. Стремительные темпы смены рубежей рыночной реформы не дозволили экономической системе принять размеренную форму и оформить ее главные институты, это касается и правовых [2].

Все это определило необходимость создания рабочего муниципального механизма обеспечения экономической защищенности РФ, и определило актуальность выбранной темы исследования.

Экономические информационные системы сегодня являются инструментом снижения неопределенности и риска принимаемых управленческих решений. Это возможно за счет информатизации и цифровизации потоков информации, поддержки ее полноты и достоверности, сокращения затрат на поиск, обработку и хранение информации. То есть. применение информационных экономических систем сегодня можно рассматривать как пример финансовой защищенности организации, как "залог независимости государства, условие прочности и действенной жизнедеятельности общества, достижение поставленных целей" [3].

Отметим следующие особенности оценки экономической безопасности в мировом масштабе [4].

1. В условиях пандемии, агентство S&P сменило прогноз для мировой экономики с роста на падение из-за вируса. Агентство S&P Global Ratings сменило прогноз развития мировой экономики в 2020 году с роста на 0,4% до падения на 2,4%, отмечая, что в 2021 году страны мира ожидает восстановительный рост.

2. Мировая экономика из-за пандемии коронавируса SARS-CoV-2 по итогам 2020 года не только не покажет рост, но уйдет в минус на 2,4%. К такому выводу пришли эксперты рейтингового агентства S&P Global Ratings, которые пересмотрели свой недавний прогноз.

3. «Влияние COVID-2019 на экономику оказалось более длительным и сильным, чем ожидалось ранее, поэтому "наши макропрогнозы ухудшились". "Теперь ожидается, что мировой ВВП в 2021 году снизится на 2,4%", — говорится в специальном сообщении агентства, посвященном коронавирусу. Еще 31 марта S&P предсказывало, что ограничительные меры из-за пандемии коронавируса приведут к снижению роста мирового ВВП с ожидавшихся 3,3% до 0,4% [5].

Обобщая выше сказанное, можно сказать, что экономическая безопасность представляет собой совокупность внутренних и внешних условий, благоприятствующих эффективному динамическому росту национальной экономики, её способности удовлетворять потребности общества, государства, индивида, обеспечивать конкурентоспособность на внешних и внутренних рынках, гарантирующую от различного рода угроз и потерь.

Из этого можно сделать два вывода:

Первый. Экономическая безопасность страны должна обеспечиваться, прежде всего, эффективностью самой экономики, то есть, наряду с защитными мерами, осуществляемыми государством, она должна защищать сама себя на основе высокой производительности труда, качества продукции и т. д.

Второй. Обеспечение экономической безопасности страны не является прерогативой какого-либо одного государственного ведомства, службы. Она должна поддерживаться всей системой государственных органов, всеми звеньями и структурами экономики.

Продолжая обсуждение особенностей экономической безопасности и возможностей снижения неопределенности и риской за счет применения экономических информационных систем, приведем пример использования одной из них.

Обучаясь на специальности "Экономическая безопасность" мы формируем навыки управления рисками при принятии определенных экономических решений. Например, для обеспечения эффективного бизнес-планирования и снижения рисков прогнозирования эф-

фективности функционирования конкретной организации, можно предложить применять такую аналитическую экономическую информационную системы как Project Expert.

Она уникальна тем, что позволяет проводить обоснование затрат на продукт, выводимый на рынок в условиях жесткой конкуренции. Моделировать деятельность предприятия виртуально и рассчитывать риски от того, насколько будут меняться окружающие базовые экономические показатели (как внутренние, так и внешние): объемы продаж, цена изделия, налоги, стратегические прерогативы поставщиков и прочее.

Сформированные в процессе обучения компетенции ее практического применения позволят обеспечить поддержку полученных выше двух выводов. Для будущих рабочих мест экономистов по экономической безопасности это будет практический инструмент, позволяющий оценивать возможные потери, несмотря на то, в каком отделе будет работать будущий выпускник.

Алгоритм работы с экономической системой можно представить на рисунке 1.

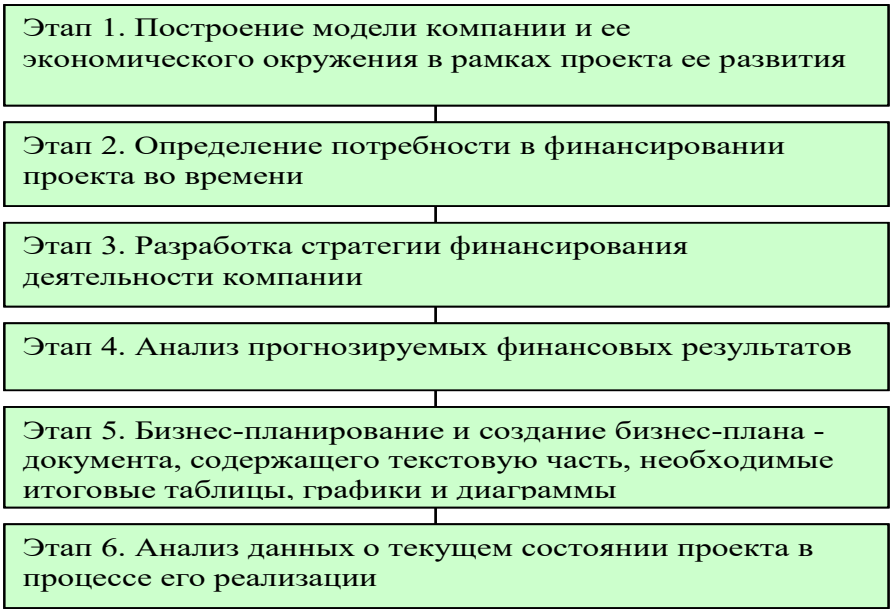

Рисунок 1 - Обобщенный алгоритм моделирования деятельности компании в Project Expert

Сделаем выводы: экономическая информационная система Project Expert является не только аналитической, но и информационно-решающей, советующей системой. Она также относится к интеллектуальной системе обработки данных. Создаваемый в этой системе бизнес-план учитывает специфику российской экономики и соответствует международным требованиям: методике UNIDO по оценке инвестиционных проектов и методике финансового анализа, определенными международными стандартами IAS [6].

Применение экономических информационный систем позволит сформировать навыки обоснованного принятия различных управленческих решений в условиях неопределенности и рисков, что является важным условием формирования основ экономической защиты информации на рабочих местах [7].

Библиографический список

1. Указ Президента РФ от 29 апреля 1996 г. №608 О государственной стратегии экономической безопасности РФ (Основные положения) // Справочная правовая система «КонсультантПлюс».

2. Сафина, И.И., Мухамадиева, Э.Ф. Об угрозах экономической безопасности России во внешнем аспекте // В сборнике научных статей II Международной научно-практической конференции. 2018. С. 146-149.

3. Федеральная служба государственной статистики. Официальный сайт. [Электронный ресурс]. Источник доступа: www.gks.ru – официальный сайт ФСГС.

4. Сайт Министерства финансов РФ. [Электронный ресурс]. Источник: http://www.minfin.ru/ru/

5. Экономическая безопасность хозяйственных систем. Учебник. Под общей редакцией доктора экономических наук, проф. А. В. Колосова. М.: Изд-во РАГС. 2018. - 326 с.
6. Project Expert. Описание [Электронный ресурс]. Источник: https://www.expert-systems.com/financial/pe/
7. Глухова, Л.В., Губанова, С.Е. Инструменты и методы менеджмента для повышения конкурентоспособности промышленных предприятий: синергетический подход // Вестник Волжского университета им. В.Н. Татищева. 2016. Т. 2. № 3. С. 100-104.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ: ОСНОВНЫЕ ПОНЯТИЯ И ВОЗМОЖНЫЕ ПРИЛОЖЕНИЯ В ПРАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Устинова Я.А., студент
Научный руководитель: Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти, Россия

Обучаясь по специальности "экономическая безопасность", начинаешь задумываться, в чем особенности будущей профессиональной деятельности в этом направлении. Поэтому, целью статьи является обзор существующих понятий и нормативной базы, которые позволят сформировать представление о будущих практических приложениях и приобретенных в процессе учебы знаний и навыков в получаемой профессии.

Я вижу перспективу своей профессиональной деятельности экономиста в конкретной организации, поэтому и выполнила анализ специализированных источников с целью определения понятия «экономическая безопасность организации». Дадим характеристику терминам «безопасность», «экономическая безопасность» и определим в чем их суть.

На государственном уровне разработана стратегия экономической безопасности Российской Федерации (Указ Президента РФ от 29 апреля 1996 г.) с учетом национальных интересов в области экономики.Государственная стратегия включает внешние и внутренние угрозы безопасности РФ как совокупность факторов, создающих опасность для важных экономических интересов личности, общества и государства. Реализация государственной стратегии производится через систему мер, осуществляемых на основе качественных индикаторов и количественных показателей: макроэкономических, демографических, внешнеэкономических, экологических, технологических и др. Здесь, в широком смысле термин "экономическая безопасность"— область научного знания, в рамках которой изучают состояние экономики, при котором обеспечивается высокий и устойчивый рост экономических показателей; эффективное удовлетворение экономических потребностей [1].

Сегодня толкование категории экономической безопасности многолико и неоднозначно. Например, в работах [2, 3] отмечено, что это есть определенная совокупность условий и факторов, обеспечивающих стабильность и устойчивость национальной экономики и, способность ее к постоянному обновлению и самосовершенствованию.

В работах [4, 5, 6] экономическая безопасность рассматривается как важнейшая характеристика существующей экономической системы, определяющая ее способность поддерживать нормальные условия жизнедеятельности населения. В этом случае, критерием экономической безопасности является минимум совокупного ущерба, наносимого всему обществу и конкретному отдельному человеку [7].

Конкретизацией такого подхода выступает обоснованное объединение понятия экономической безопасности с понятием риска [8, 9].

Под экономической безопасностью предприятия подразумевается состояние корпоративных ресурсов и их эффективное использование для предотвращения угроз и обеспечения стабильного функционирования. Оценка уровня экономической безопасности производится с помощью системы функциональных критериев, рассчитываемых по наиболее важным направлениям (составляющим): финансовому, интеллектуально-кадровому, технико-технологическому, политико-правовому, экономическому, информационному, силовому.

Например, на всех крупных промышленных предприятиях существуют специальные отделы по экономической безопасности, и входящие в их структуры отделы по информационной безопасности, в которых реализуется защиты циркулирующей в производственной системе информации от несанкционированного доступа к ней и сознательного искажения ее или утраты.

На рисунке 1 показан пример такой структуры (составленный автором в процессе анализа деятельности промышленного предприятия).

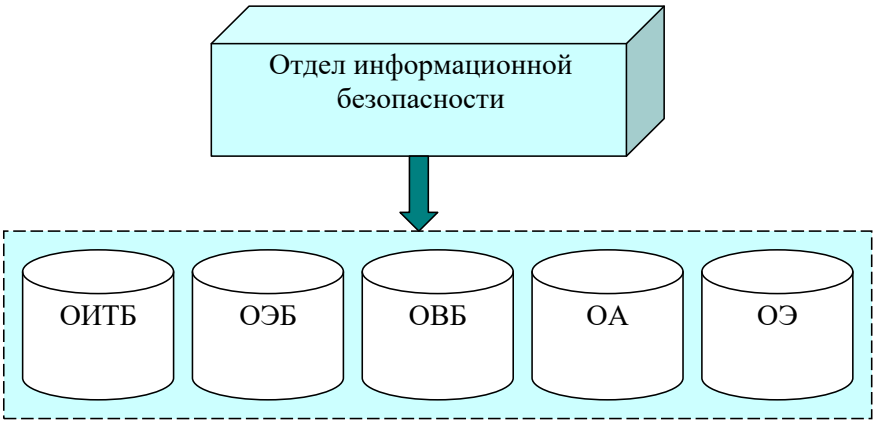

Рисунок 1 - Примерная структура отдела информационной безопасности предприятия
ОИТБ - отдел инженерно-технической безопасности; ОЭБ - отдел экономической безопасности; ОВБ - отдел внутренней безопасности; ОА - отдел аналитики; ОЭ - отдел экспертизы.

Каждая из структурных единиц выполняет свои должностные обязательства, в которых много внимания уделяется функциям анализа и контроля.

В процессе обучения мы также формируем навыки контроля, прогнозирования, управления рисками. Например, при составлении бизнес-планов с целью обеспечения экономической безопасности для виртуальных предприятий малого бизнеса, мы применяем автоматизированную экономическую систему Project Expert.

Используя ее возможности, мы получаем точку безубыточности проекта для нашего бизнес-плана (рис. 2) и оцениваем возможности будущей хозяйственной деятельности.

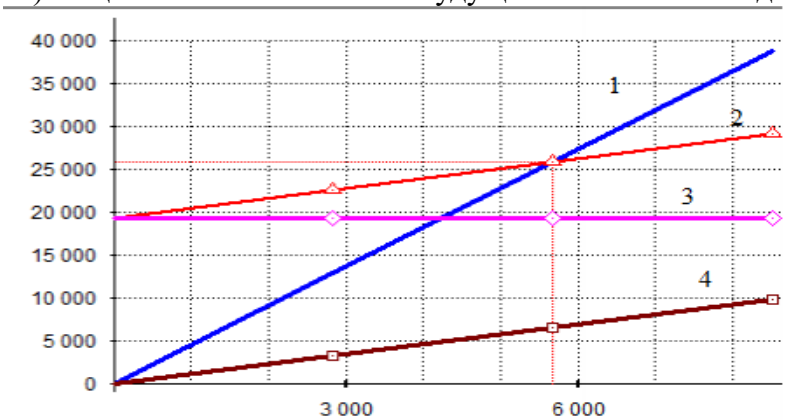

Рисунок 2 - Примерный вариант полученных расчетов
1 - поступления от продаж за анализируемый период (месяц); 2 - график суммарных издержек за анализируемый период; 3 - график постоянных издержек; 4 - график прямых издержек

Имея возможности изменения исходных параметров, с помощью Prolect Expert можно прогнозировать менее безопасную с экономической точки зрения ситуацию на рынке для функционирования предприятия.

Однако, рассматривая такие показатели, как объемы продаж, цена за единицу продукции, суммы налогов, издержки, мы можем рассматривать их как случайные факторы. В этому случае, применяя метод Монте Карло, заложенный в Project Expert (режим статистиче-

ский анализ), мы можем оценить уровень неопределенности (риск) изучаемых показателей и выбрать те значения, которые наименее рискованны.

Можно сделать следующий вывод: будущему экономисту, который обучается на специальности "экономическая безопасность" необходимо владеть навыками управления различными видами экономических рисков и умениями оценки возможности их идентификации и снижения негативного воздействия за счет выявления причин возникновения и методов управления. В этом нам видится один из основных аспектов приложения инструментов экономической безопасности в будущую профессиональную сферу деятельности.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 № Пр-1895) и Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»

2. Холчева, И.А., Кисова, А.Е. Основные подходы к исследованию понятий "экономическая безопасность" и "экономическая безопасность государства" // Дневник науки. 2019. № 5 (29). С. 96.

3. Глухова, Л.В. Губанова, С.Е. Некоторые аспекты менеджмента информационной безопасности промышленных комплексов // Вестник Волжского университета им. В.Н. Татищева, 2015, № 3 (34). С. 135-144.

4. Глухова, Л.В. Информационно-аналитическая деятельность по обеспечению экономической безопасности // Наука - промышленности и сервису. Тольятти: 2013, № 8-1 С.154-157

5. Губанова, С.Е. Особенности гармонизации промышленной и торговой политики предприятия с учетом экономической безопасности //Вестник Поволжского государственного университета сервиса. Серия: Экономика. 2013. № 5 (31). С. 108-112.

6. Губанова, С.Е. Атрибутный подход к обеспечению защиты информации при организации экономически безопасной политики предприятия // Вестник Волжского университета им. В.Н. Татищева. 2016. Т. 2. № 1. С. 126-131.

7. Губанова, С.Е. Экономическая безопасность: особенности электронных коммуникаций и защиты информации в деятельности предприятий //Информационные системы и технологии: управление и безопасность. 2016. № 4. С. 39-43.

8. Сафина, И.И., Мухамадиева, Э.Ф. Об угрозах экономической безопасности России во внешнем аспекте / В сборнике: сборник научных статей II Международной научно-практической конференции. 2018. С. 146-149.

9. Глухова, Л.В., Казиева, Б.В., Казиев, К.В., Казиев, В.М., Шерстобитова, А.А. Управление деятельностью инновационных систем в условиях неопределенности и риска // Вестник Волжского университета им В.Н. Татищева, 2020, т.2, №3(46). С. 50-59.

БЕЗОПАСНОСТЬ В СМИ

ПРОБЛЕМА ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В ЖУРНАЛИСТИКЕ

Агеева Ю.К., студент
Волжский университет имени В.Н. Татищева
Соловов Л.В., студент
Поволжский государственный университет сервиса
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
Поволжский государственный университет сервиса
г. Тольятти

Один из главных аспектов информационной безопасности аудитории — достоверность сообщений СМИ. Достоверность журналистских текстов обеспечивает целый ряд логических практик. Журналистика относится к разряду профессий, этические основы которых закрепляются особыми документами государственного уровня. Само собой, ни один из этих документов не будет требовать от журналиста лжи, все они будут настаивать на его обязанности поставлять обществу достоверную информацию. Так, статья 49 Закона РФ «О средствах массовой информации» требует от журналиста проверять достоверность сообщаемой им информации.

Надежность данных, с которыми работает журналист, зачастую подвергается сомнению на всех этапах подготовки материала. Так, не теряет своей актуальности проблема представления интересов источников сообщений через СМИ. Несмотря на разграничение понятий «пропаганда» и «средства массовой информации», объединенных при СССР, большинство ньюсмейкеров по-прежнему воспринимают издания как своеобразную трибуну, позволяющую не только оповещать о достигнутых результатах и поставленных задачах, но и навязывать свою позицию [2, с. 17].

Существенное влияние на достоверность информации на стадии ее получения оказало развитие новых медиа, не требующих временных затрат на обработку и публикацию сообщения и не снабженных органом редактуры. Традиционные издания прибегают к помощи социальных медиа в ситуациях, требующих наиболее оперативной передачи данных читателю или зрителю. Однако вероятность получения диффамации или дезинформации в данном случае увеличивается в связи с уменьшением времени проверки текстов, открытостью аккаунтов для хакерских атак и слабой правовой защищенностью от недостоверности постов, публикуемых в блогах и соцсетях.

Основными требованиями, предъявляемыми к журналисту, следует отметить достоверность информации, неподкупность, объективность и законопослушность. Исходя из этого, можно выделить следующие нормы:

Журналист распространяет и комментирует только ту информацию, в достоверности которой он убежден и источник которой ему хорошо известен. Он прилагает все силы к тому, чтобы избежать нанесения ущерба кому бы то ни было ее неполнотой или неточностью, намеренным сокрытием общественно значимой информации или распространением заведомо ложных сведений.

При выполнении своих профессиональных обязанностей журналист не прибегает к незаконным и недостойным способам получения информации.

Журналист рассматривает как тяжкие профессиональные преступления злонамеренное искажение фактов, клевету, получение при любых обстоятельствах платы за распространение ложной или сокрытие истинной информации; журналист вообще не должен принимать ни прямо, ни косвенно никаких вознаграждений или гонораров от третьих лиц за публикации материалов и мнений любого характера.

Журналист отвечает собственным именем и репутацией за достоверность всякого сообщения и справедливость всякого суждения, распространенных за его подписью, под его псевдонимом или анонимно, но с его ведома и согласия.

В соответствии со ст. 49 Закона о СМИ журналист имеет право проверять достоверность сообщаемой им информации. Эта норма является подспорьем для репортера в его стремлении к правдивости и объективности [1, с. 78].

В современном демократическом обществе роль и влияние на общество СМИ огромно. В руках СМИ такие рычаги давления и воздействия, как пресса, радио, телевидение, Интернет, реклама. Та роль, которую играют СМИ в информирующемся обществе делает возможным называть их «четвертой властью», что символически ставит СМИ в один ряд с законодательной, исполнительной и судебной. Это приводит к неправильному представлению о том, что управляемые закулисными магнатами СМИ могут при желании управлять правительством и даже отправлять его в отставку.

С целью более эффективной работы российских СМИ с точки зрения пользы обществу стоило бы создать общественную структуру, своего рода рейтинговое агентство по СМИ, в которую могут войти ведущие общественные, научные деятели, деятели культуры, представители основных религиозных организаций России, представители силовых структур. Агентство должно составлять ежегодный топ-лист российских СМИ на предмет правдивости информации и доверия граждан, а точнее, фиксировать факты лжи в российских СМИ. Российские СМИ, сильно злоупотребляющие свободой слова, дискредитирующие понятие демократия, найдут «достойное» место в этом рейтинге.

Создание рейтингового агентства по СМИ явится еще одним достижением на пути строительства институтов гражданского общества в России, позволит установить гармонию между свободой слова и правом граждан на правду.

Библиографический список

1. Кастельс, М. Информационная эпоха: экономика, общество и культура [Текст] / М. Кастельс / пер. с англ.: под науч. ред. О.И. Шкаратана. — М.: ГУ ВШЭ, 2000. — 608 с.

2. Кравцов, В.В. Инновационные изменения в медиапространстве современной России [Текст] / В.В. Кравцов // Журналист. Социальные коммуникации. – М., 2015. - № 3-4 (19-20). – С. 18 – 26.

«ГРУППЫ СМЕРТИ» ИЛИ ОПАСНЫЕ ГРУППЫ В СОЦИАЛЬНЫХ СЕТЯХ

Алещенко А.В., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

В современном обществе представить свою жизнь без средств массовой информации практически невозможно. Мы постоянно следим за новостями по телевизору, читаем интересные статьи в прессе, общаемся с друзьями в интернете. Так как большинство населения - это молодежь, и она является ярым потребителем СМИ, а СМИ в свое время имеет влияние на молодежную аудиторию. Конечно же, частый выбор среди молодого поколения падает на интернет.

В последние годы в России широко обсуждали «группы смерти» в интернете, где подросткам раздают «задания», которые могут довести их до самоубийства. Специалисты неоднократно заверяли, что опасность таких групп преувеличена: так, по данным МВД, лишь 1% подростковых суицидов связан с закрытыми группами в соцсетях. Главные причины, на которые приходится по 30% всех случаев, – неразделенная любовь или конфликты в семье.

Но все же эти группы в социальных сетях вызывали у молодежи огромные психологические проблемы. «Группы смерти» и их вариации — современное проявление подростковой романтизации смерти. Обычно дети попадают в такие группы в тот момент, когда им плохо:

страшно, одиноко, они страдают от непонимания или находятся в состоянии конфликта. Попадая в закрытую группу, ребенок подвергается информационной интоксикации: он смотрит видео и читает тексты, якобы полные скрытых важных смыслов. Кроме того, он начинает ощущать угрозу: сделаешь что-то не так — вылетишь, а значит, перестанешь быть избранным, лишишься поддержки группы и оснований чувствовать свое превосходство. Философия таких групп строится на том, что мир жесток и несправедлив; при этом подростку внушают, что в группе его любят и ценят. Чем больше он выполняет абсурдных или опасных заданий, тем более высокое положение занимает в группе.

Многие подростки приходят в такие группы, потому что им просто интересно, но постепенно группа начинает удовлетворять их потребность в признании. Вначале возникает привязанность, а потом и зависимость от лидеров группы. Таким образом, подросток попадает в замкнутую систему, подвергается постоянному информационному воздействию и постепенно перестает замечать вокруг себя другие точки зрения, другую информацию.

Обычно подросток, который участвует в смертельном квесте, подписан и на множество других пабликов. Если проанализировать содержание подписок, можно заметить, что основные его интересы сконцентрированы на депрессивных группах. У подростка, находящегося в подавленном эмоциональном состоянии, ослабевают механизмы психологической защиты. Выполненные задания вызывают у него искреннюю радость и эмоциональную разрядку, он получает похвалу от куратора и становится еще более зависимым от игры. Из такой группы ребенок может выбраться только с помощью других людей.

ПРОБЛЕМЫ МАСС-МЕДИА В ПРЕДЕЛАХ МЕЖКУЛЬТУРНОЙ КОММУНИКАЦИИ

Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
Поволжский государственный университет сервиса
г. Тольятти

В сфере рассмотрения проблем масс-медиа, а также их проблем в межкультурной коммуникации можно сказать, что в современном мире они приобрели значительную роль, и заняли огромное место в диалоге между культурами. Здесь необходимо рассмотреть следующие аспекты:

1. Национальные и культурные особенности средств массовой информации в каждой стране, потому что они могут противоположно отличаться друг от друга.
2. Речевой этикет масс-медиа в каждой стране.
3. Язык культуры средств массовой информации.

В последнее время масс-медиа стали доминирующим фактором в межкультурной коммуникации современного мира, который определяет в большинстве случаев не только политические взгляды всех стран, но и культуру каждой страны, потому что они призваны определять картину мира современного общества с вытекающими отсюда последствиями: человеческие ценности, стереотипы людей, представление людей о межкультурной коммуникации, процессы политического взаимодействия различных стран мира [1, с. 60]. Средства массовой информации обязаны освещать все происходящее в мире как можно более правдиво. Рассмотрим, какие же проблемы существуют у современных средств массовой информации:

1. Проблема первая. Одной из актуальнейших проблем современных средств массовой информации является установление диалога между ними и властью, то есть политическими системами и народом, потому что, как известно, люди первые реагируют на публикации статей в мировой жизни народа, политические телепередачи в межкультурной коммуникации. Какой должна быть информация, предоставляемая масс-медиа: позитивной или негативной? Так что же происходит с людьми, когда им с утра до вечера средства

массовой информации представляют негативную политическую информацию в межкультурной коммуникации? А происходит следующее. У людей начинает накапливаться негатив к политической жизни страны, он может в любой момент взорваться, то есть можно сказать, что это эффект «бомбы замедленного действия».

Общественное мнение – это важнейший фактор для средств массовой информации, который они должны каждую минуту контролировать и регулировать, особенно в межкультурной коммуникации.

2. Проблема вторая. У средств массовой информации есть еще одна важная актуальная проблема – это этнический, национальный, религиозный аспект, потому что в современном мире нет ни одной моноэтнической, мононациональной, монорелигиозной страны. Не стоит забывать, что Россия испокон веков всегда была страной, где живет множество национальностей, людей с разными религиями, поэтому в России исторически сложилось так, что на почве разных религий в ней никогда не бывает конфликтов, чего нельзя сказать о странах Европы, где всегда доминирует только одна национальность, одна религия.

Однако в последнее время ситуация в странах Европы кардинально поменялась, поскольку в связи с политической ситуацией в мире в страны Европы приехало очень много беженцев и эмигрантов, и коренное население этих стран вынуждено считаться с новым фактором в их жизни, потому что, как правило, беженцы – это мусульмане, то есть с абсолютно другой религией, кардинально отличающейся от христианства. В этой непростой ситуации средства массовой информации должны первыми реагировать на этот фактор, потому что этот контингент достаточно взрывоопасный. Масс-медиа вынуждены маневрировать между двумя абсолютно противоположными религиями, что непременно сказывается на их деятельности в межкультурной коммуникации.

3. Проблема третья. Есть еще одна проблема в современном обществе, а значит и у средств массовой информации – это правдивость, адекватность предлагаемой информации обществу. Уже ни для кого не секрет, что американские и европейские масс-медиа регулярно искажают политическую информацию, якобы в пользу Америки и стран Европы. Но, если посмотреть внимательнее, они только вредят их странам в межкультурной коммуникации, потому что правда всегда «выплывает на свет божий». К сожалению, политика и политики в современном мире всегда вмешиваются в деятельность и работу средств массовой информации, хотя по–хорошему этого происходить не должно, потому что масс-медиа должны быть независимыми ни от политики, ни от экономики в межкультурной политической коммуникации.

Что же происходит в российских и западных средствах массовой информации и чем они отличаются при подаче информации обществу? Российские масс-медиа дают конкретную, реальную информацию, а только потом журналисты могут высказать свое мнение, комментарии по поводу происходящих событий, при этом никому не навязывая его, как бы вскользь, иногда обыгрывая. Американские средства массовой информации, давая информацию людям, постоянно навязывают свою точку зрения, после каждой произнесенной ими фразы, комментируют ее, таким образом, их мнение выглядит как догма, перекрывая и затмевая всю правдивую информацию. Нужно сказать, что американцы больше воспринимают комментарии журналистов, а не суть вопроса, поэтому их средства массовой информации работают на публику.

4. Четвертая проблема. Язык, культура и речевой этикет – это особо болезненная область в средствах массовой коммуникации, потому что, как мы видим в последнее время, они часто начали забывать, что есть такое понятие, как «культура языка». Когда мы включаем телевизор, начинаем читать газеты, то сталкиваемся с тем, что на каждом шагу происходит нарушение этикетных норм. С недавних пор журналисты при освещении политических тем начали переходить на просторечный, разговорный язык, забывая о том, что в их профессиональной деятельности необходимо использовать деловой язык журналистов. Это самая большая, на наш взгляд, проблема, потому что, когда люди слышат с экрана телевизоров или читают в газетах такую лексику, они начинают воспринимать ее как

норму языка. Языковая культура журналистов должна быть на высочайшем уровне, на которую люди должны ориентироваться [2].

Разумеется, проблем в средствах массовой информации множество, и их благоразумно необходимо решать без перегибов в одну или в другую сторону.

Библиографический список

1. Гаранина, С.Н., Гаранин, В.М. Лингвокультурологические особенности в межкультурной коммуникации при обучении студентов – иностранцев деловому русскому языку на начальном этапе. [Текст] / С.Н.. Гаранина, В. М. Гаранин / Предвузовское обучение иностранных студентов: современное состояние, проблематика. / Сборник статей по материалам межвузовской науч. – практической конференции. – М., РУДН, 2015. – С. 60–64.

2. Гаранина, С.Н., Гаранин, В.М. Адаптационные процессы у иностранных учащихся на довузовском этапе обучения в культурном пространстве России / Сборник статей I международного конгресса преподавателей и руководителей подготовительных факультетов в двух частях. [Электронный ресурс] / С.Н.. Гаранина, В. М. Гаранин / Довузовский этап обучения в России и мире: язык, адаптация, социум, специальность. / 19 – 21 октября 2017 г., Часть I., URL: http://dporudn.ru/news/postreliz–o–i–rukovoditeley–podgotovitelnykh–f/

СМИ И АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Буторова А.А., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

С точки зрения Доктрины информационной безопасности, чрезвычайно важно сохранять и развивать информационное пространство России в целях обеспечения единства нашей страны. А то сегодня это пространство, как мы видим, распадается и дробится. Местная пресса занята исключительно местными интересами, на нее большое влияние оказывают местные власти. Но когда «за деревьями не видно леса», когда за местными интересами не видно общероссийских, это создает реальную угрозу для всех нас. Поэтому сейчас, когда восстанавливается вертикаль власти, следует подумать о воссоздании вертикали прессы (речь, конечно же, идет не о той модели управления СМИ, которая существовала в советские времена). Это необходимо сделать, потому что пресса, отстаивающая национальные интересы, может сыграть важную роль в достижении информационного единства государства, что, в свою очередь, повысит управляемость огромной страной, то есть укрепит ту самую вертикаль власти. Доктрина указывает реальные пути к тому, как преодолеть информационный раскол и обеспечить доступ к информации техническими, структурными и другими средствами. Информационное единство – первый важный момент информационной безопасности с точки зрения средств массовой информации.

Второй состоит в том, что в последние десять лет в обществе существует известная конфронтационная стилистика – противопоставление точек зрения разных групп. С одной стороны, для демократического государства это естественно. Но, с другой стороны, во многих случаях отсутствует желательный консенсус, а средства массовой информации порой азартно нагнетают этот конфронтационный стиль. Справедливо подчеркивается, что печать, радио и телевидение в своей политической деятельности являются оппонентом власти, они контролируют власть, от имени общества указывая на ее недостатки, помогают гражданам корректировать действия властных структур. Это все верно, но нужно помнить и о конечной цели – выработке консенсуса для решения обществом общих задач. Наши средства массовой информации мало делают для создания обстановки терпимости, толерантности, часто воспитывают конфронтационный дух, который ведет к развитию в массовом сознании негативных стереотипов, когда самые невинные шаги власти воспринимаются как заговоры против народа.

Словом, сама стилистика наших средств массовой информации нуждается в известной корректировке. Можно сказать, что в советское время все было проще: все средства массовой информации были государственными, ЦК КПСС принимал решения – они их выполняли. Но сегодня СМИ присущи различные формы собственности: государственная, частная, общественная, они плюралистичны и каждое издание, радиостанция или телеканал имеют право действовать в соответствии со своими интересами, задачами и идеями. Однако при всем этом главная задача всех средств массовой информации остается прежней – поддержание единства общества, основанного на едином понимании национальных интересов. Средства массовой информации обязаны играть очень важную роль в примирении государственных, частных и общественных интересов.

Доктрина информационной безопасности, подчеркивающая важность защиты Конституции и конституционных прав граждан, создает необходимую основу для единства действий любых средств массовой информации в интересах России. Кроме того, большое значение имеет взаимодействие государственного и частного секторов СМИ, работающих в них журналистов, правительства и владельцев прессы. Речь вновь идет не о единомыслии, а, если хотите, о трехстороннем подходе к проблемам – со стороны журналистов, медиа-бизнеса и представителей властных структур, – что очень важно для поддержания общественного согласия. Так делается во многих странах. В качестве примера вспомним, что интернет уже регулируется на основе согласованного взаимодействия всех заинтересованных сторон – государственных структур, провайдеров и обществ потребителей. Нечто аналогичное должно быть достигнуто в России в сфере средств массовой информации.

Общенациональная политика в области средств массовой информации, предложенная в Доктрине, может стать важным стимулом для выработки консенсуса в обществе. Особо следует обратить внимание на проблему телевидения. В свое время немецкий философ Юрген Хабермас выдвинул концепцию публичной сферы, где между гражданами и правительством действуют общественные институты, и, в частности, средства массовой информации. Сегодня эта публичная сфера занята во многом именно телевидением, которое, как уже было отмечено выше, подвергается серьезной опасности – вместо объективной информации и разных мнений оно предлагает зрителю спектакли, которые, к сожалению, часто действуют на сознание сильнее, чем логика и доводы рассудка. Речь идет о манипулировании сознанием. Для противодействия этому необходимо иметь, наряду с коммерческим телевидением, телевидение и радио, которые подставляли бы общественные интересы. Кстати, Совет Европы требует, чтобы было организовано такое общественно-правовое телевидение. В Европе оно давно существует, и, как правило, это государственное телевидение. И в России государственные телевидение и радио тоже могут стать общественно-правовыми. Вспомним, что на определенном этапе Российская телерадиокомпания (ВГТРК или второй канал) уже выполняла реальные функции этого самого общественно-правового телевидения, особенно в то время, когда ее возглавлял Олег Попцов. Конечно, государственные телевидение и радио не могут быть свободны от государства, но ведь многое зависит от того, как понимать государство. Есть концепция государства, идущая от Людовика XIV, который изрек знаменитое: «Государство – это Я!». Но есть другая концепция, где государство представляет интересы всех граждан. Если исходить из этой концепции, то государственное телевидение должно быть телевидением не правительственным, президентским, министерским, оно должно быть общенародным, принадлежать всем. Конечно, правительство должно иметь возможность отстаивать свои интересы, но на государственном телевидении слишком велика опасность административно-командного, чиновничьего вмешательства. Ее можно избежать, если создать авторитетные общественные советы, обеспечить известную автономию государственных телевидения и радио. В этом случае мы можем получить серьезные, актуальные каналы, которые будут работать не на коммерцию, а на интересы государства, граждан, гражданского общества.

Об эффективности надо говорить как о центральной профессиональной задаче сотрудников СМИ. В конечном счете, это вопрос о том, насколько оправдывают себя колоссальные

материальные и интеллектуальные затраты общества на прессу. Это и вопрос о раскрытии возможностей журналистики как инструмента саморазвития и самоуправления социальной системы. Наконец, достижение видимого эффекта приносит удовлетворение и сотрудникам редакций, и представителям аудитории. Результаты работы СМИ подразделяются на несколько видов в зависимости от объектов воздействия, формы реакции на деятельность прессы и масштаба возникающего эффекта. Для определения различий в силе воздействия прессы на соц. жизнь служит понятие масштаба действенности.

Углубление журналистского анализа, активное внедрение в практику редакций исследовательских методов работы, привлечение к сотрудничеству ученых и специалистов — все это должно вести к усилению резонанса выступлений. С «пространственной» точки зрения эффекты подразделяются на локальные и широкомасштабные. Обращаясь к локальной ситуации, добиваясь решения конкретного вопроса, печать выполняет лишь начальную задачу. При классификации по времени действия мы сталкивается с эффектами ближайшими и отдаленными. Представим себе, что от публикации, как от брошенного в воду камня, расходятся широкие круги действенности. Преобладающая часть отдаленных последствий остается неведомой журналистам. С течением времени под воздействием прессы меняются взгляды общества на события и явления, другими становятся и мировоззренческие установки. Эффекты так же подразделяются на основные и побочные. Основные последствия относительно несложно предвидеть, запланировать (поэтому их можно называть еще плановыми). Побочные же, случается, бывают для корреспондента полной неожиданностью. Нежелательные побочные эффекты нередко возникают после критических, разоблачительных публикаций. Отдельно надо сказать о ситуациях, когда журналистская деятельность приводит к результатам, которые прямо противоположны исходным целям - эффект бумеранга. В свою очередь, они тоже делятся на две группы: в итоге неумелой и непродуманной работы журналистов ущерб наносится либо тому делу, которому они стремились помочь, либо их собственной репутации (впрочем, вероятнее всего, произойдет и то и другое). Любой материал оказывает большее или меньшее влияние на аудиторию. Прогнозирование результатов своего выступления — обязательная фаза творческого процесса в журналистике. Как мы могли убедиться, это отнюдь не элементарная операция, а сложнейшая интеллектуальная работа, сопряженная с высокой гражданской и этической ответственностью. И практики, и исследователи прессы обязаны видеть как ближайшие, так и перспективные результаты деятельности СМИ, соотносить их с интересами общества и отдельного человека. С учетом множественности и разнообразия последствий журналистской деятельности ее эффективность определяется как совокупность результатов воздействия на сознание, психологию и поведение аудитории, человека, социальной группы и общественной системы. На практике сложности вызывает вопрос о содержании эффективности прессы. Тому есть несколько причин, заложенных в природе журналистского взаимодействия с социальным миром. Во-первых, каждая редакционная акция, как мы уже знаем, дает несколько эффектов одновременно. Во-вторых, большинство изменений в действительности лишь частично зависят от прессы. Как правило, печать усиливает действие комплекса факторов, как бы ускоряет созревание верного решения. В-третьих, в создании эффекта наравне с журналистом участвует читатель, зритель, слушатель, с его индивидуальным способом восприятия информации, непредсказуемой психической организацией, субъективным взглядом на жизнь, наконец — с определенным уровнем грамотности и обшей культуры, который становится фильтром на пути слова от автора к аудитории. В-четвертых, для точного определения действенности необходимо использовать научный инструментарий, заимствуя его у социологии, социальной психологии, прогностики и других наук. Под затратами надо понимать весь объем израсходованных ресурсов — человеческих, организационных, материальных. По своей ценности затраты не должны превышать результаты, иначе эффективность окажется со знаком минус. Соотношение затрат и результатов особенно выразительно показывает экономика редакции.

Другие стороны производственной жизни редакции также поддаются расчету. Например, главный редактор обязан взвешивать, насколько целесообразно командировать непод-

готовленного сотрудника в «горячую точку»: интерес читателей к репортажам с места боев вряд ли окупит возможные увечья или даже гибель корреспондента. Не чуждо прессе и моделирование, более того — для нее это один из самых органичных способов взаимодействия с органами управления. «Строительным материалом» при этом служат факты, добытые и проверенные опытом, оцененные специалистами и скрепленные между собой публицистическим анализом. Редакции, по сути дела, готовят комплексные пакеты предложений (проекты), которые могут лечь в основу решений государственных, хозяйственных, общественных служб. Элементы моделирования можно встретить как в «большой» прессе, так и в местной журналистике, которая регулярно ведет рубрики типа «Что бы я сказал на заседании мэрии», посвященные обсуждению намечаемых решений городских властей. В этом, частном, случае моделирование сближается с экспертизой.

Под экспертизой понимается публичная оценка, которую пресса дает новым явлениям, затрагивающим жизненно важные интересы граждан. Объектом экспертизы могут стать и действия властей, и реформы в банковско-финансовой сфере, и перестройка системы образования, и потребительские товары и т.д. От массового обсуждения, например, законопроектов она отличается тем, что опирается на мнение небольшого количества знатоков вопроса, даже на единичное мнение и не предполагает затяжной дискуссии. В зависимости от предмета оценки экспертиза влияет на решение и поведение либо органов управления (анализируются качество и последствия распоряжения городской администрации), либо группы людей и коллективов (рассматривается инициатива организаторов политической акции), либо массовой аудитории (оценивается качество товаров повседневного спроса). В случае с представителями власти пресса ставит перед собой задачу откорректировать не самое, может быть, взвешенное решение или добиться его отмены. По отношению к массе населения пресса выступает как консультант, влияющий на выбор бытовой покупки, жилья, услуг туристических фирм и т.п. В последние годы эта деятельность (которую не надо путать с рекламными публикациями) получила необычайно широкое распространение. Пресса способна добиваться большего — помочь обществу сделать шаг вверх, развиться, получить неосвоенные пока еще блага. Такой эффект возникает при умелой пропаганде передового опыта.

Библиографический список

1. Журналистика и публичная экспертиза [Электронный ресурс] / https://cyberleninka.ru /article/n/zhurnalistika-i-publichnaya-ekspertiza

2. Профессиональные задачи журналистской деятельности [Электронный ресурс] / https://www.academia.edu/36890196/Профессиональные_задачи_журналистской_деятельности

3. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” [Электронный ресурс] / https://www.garant.ru/products/ipo/prime/doc/71456224/

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРЕДЕЛАХ СМИ

Мартынова А.Д., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

В условиях широкой свободы деятельности плюралистической журналистики при недостаточном осмыслении и реализации требований информационного порядка при организации функционирования СМИ стала остро ощущаться совокупность ряда проблем информационной безопасности. Среди многочисленных проблем национальной безопасности существенное место занимает проблема информационной безопасности. Не случайно во Всеоб-

щей декларации прав человека указывается, что реализация прав человека, в том числе и на информацию, является «основой свободы, справедливости и всеобщего мира».

Средства массовой информации, обращенные, прежде всего, к массовой аудитории, природой своей призваны обеспечить массово-информационную безопасность за счет «доставки» потребителям необходимых для принятия решений информационных ресурсов, защиты от дезинформирующей (манипулятивной) информации, которая распространяется теми же СМИ.

Понятие «информированность» входит постепенно в законодательство. В Законе «О праве на информацию» указывается на обязанность органов и организаций сообщать для всеобщего сведения ставшую им известной при осуществлении своей деятельности информацию:

- если она может предотвратить угрозу жизни или здоровью граждан;
- если требуется пресечь сообщение недостоверной информации;
- если она имеет или может иметь общественно значимый характер [2].

Однако этот закон не касается СМИ, а, следовательно, пока на их деятельность не распространяется требование реализации принципа информированности граждан.

Чтобы сделать гражданина достаточно информированным для принятия и реализации максимально верного решения, во-первых, от СМИ надо ожидать одинаково активной работы со всеми сторонами массового сознания (мировоззрением, миросозерцанием, историческим сознанием и особенно общественным мнением); во-вторых, информирование должно протекать с учетом объективных потребностей каждой социальной группы, общественного слоя, а также различий в их представлениях, взглядах, настроениях; в-третьих, следует исходить из понятия общества как системно организованной целостности, где каждая группа функционирует лишь при наличии других и в органической связи с ними [2, с. 6].

В связи с этим государственная (национальная) политика в сфере СМИ должна прочно базироваться на идее и практике политического, идеологического, культурного плюрализма, предполагающей, что все возможные взгляды не только могут, но и должны быть предъявлены обществу, быть доступными самым различным слоям, подвергнуться всестороннему обсуждению в целях поиска общеприемлемого решения.

Однако очевидно, что не все социальные силы и их идейные представители имеют возможность создать свои СМИ, а предлагаемые в «чужие» СМИ материалы нередко отвергаются.

Одной из составляющих национальной политики в сфере СМИ должна быть толерантность - терпимость, притом благожелательная, к взглядам других, признаваемых равноправными в силу равенства социальных сил, их выражающих и защищающих.

Общегосударственная информационная политика, включает положение о необходимости активного ведения социального диалога в СМИ. Способы ведения диалога могут быть разными, «Открытый» диалог предполагает максимально полное изложение своих позиций и аргументации в надежде на встречную открытость других участников. «Закрытая» позиция сводится к монологическому изложению своей точки зрения при убежденности в ее полной правоте. «Полузакрытыми» формами диалога являются «монологический диалог» [2, с. 8].

СМИ, ведущие открытый диалог, озабочены поиском такого решения (компромисса, консенсуса), который был бы на пользу всем и не опасаются упрека в «слишком больших уступках» или даже «потере лица».

Открытый диалог, ведущийся одной стороной, в споре может наталкиваться на «закрытую» позицию других, непонимание и нежелание идти на сближение и поиск общеприемлемого решения, а порой и на стремление к односторонней выгоде.

Несмотря на увеличение числа газет, программ ТВ и радио, возможности граждан получить необходимую и достаточную информацию не только не возрастают, а сужаются. Информационное пространство страны «рвется», так как общефедеральные издания не доходят до большей части региональной, да и московской аудитории, в то же время, рост местной прессы крайне затруднен и ее информация локализирована. развитие плюрализма без четко

налаженного диалога различных сил и движения к общественному согласию по общенациональным проблемам приводит к обострению социального напряжения.

При недостаточной урегулированности деятельности СМИ и непонимании субъектами информационной деятельности необходимости коррелировать свои интересы и стремления с общенациональными и даже общечеловеческими нуждами возникает и часто реализуется желание гиперболизировать общественную роль СМИ, превратить их в «сверхвласть»

Эти опасные тенденции можно минимизировать и устранить лишь тогда, когда государственная политика в области СМИ будет содержать гарантии такого «информационного порядка», при котором демократические и гуманистические принципы функционирования журналистики реализуются полно и точно разными силами.

Библиографический список

1. Воскресенский, Ю. Понятие средства массовой информации. роль коммуникации и СМИ в политической системе общества / [Электронный ресурс] URL: http://www.lawmix.ru/comm/1121/

2. Некляев, С.Э. Участие средств массовой информации в обеспечении информационно-психологической безопасности в условиях локальных войн и международного терроризма [Текст] / С. Э. Некляев // :автореферат дис. ... кандидата филологических наук : 10.01.10/ Моск. гос. ун-т им. М.В. Ломоносова. - Москва, 2003. - 21 с.

УГРОЗЫ И АТАКИ В СМИ

Нольде Н.С., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

СМИ – это некая совокупность органов, которые служат для публичной передачи информации большому количеству людей и помогают им в этом современные технические устройства, которые есть на данный момент почти у каждого человека, например, смартфон или телевизор, находящиеся во многих семьях. Основа понимания безопасности СМИ - характеристика оптимального состояния объектов защиты (государства, общества, граждан) с указанием характера опасностей и угроз и их источников. После этого требуется определить и выяснить пути и средства обеспечения безопасности, способы устранения опасности и ликвидации угрозы и соответственно её источника. Также следует найти организации или организационные формы, функции которых - мониторинг и анализ состояния безопасности СМИ.

Информационная безопасность может быть подвержена опасности при условиях, когда большая часть технологических процессов выполняется через компьютерные системы и предполагает широкое использование телекоммуникационных технологий, которые имеют высокую вероятность выйти из строя или быть взломаны разного рода опасными группировками или мошенниками. Подобного рода действия приравниваются к нарушению закона. А если такие действия привели к нарушения прямого эфира, во время которого корреспондент озвучивал какую-то важную информацию, то это приравнивается к нарушениям свободы слова.

Также за журналистами могут вести прослушивание или слежку, что является нарушением их профессиональной деятельности, либо как факторы, создающие предпосылки к этому. Слежка и прослушивание дают способы определить источник информации, что впоследствии нарушает ее конфиденциальность.

Самыми молодыми и перспективными среди СМИ являются интернет-издания. Интернет-медиа наиболее широко из всех СМИ используют современные технологии, но, к сожалению, данные технологии не обладают достаточно хорошей защитой и чаще всего подвергаются серьезным угрозам, которые могут повлечь за собой потерю важных данных или

любой другой информации, которая хранилась в компьютерной сети или же полностью нарушить систему интернет-издания или вывести из строя дорогое оборудование.

Рассмотрим случаи атаки на интернет-издания, сайты и общественные организации. В Казахстане наблюдались серьёзные атаки на «Зона.Кз», «Гео.Кз», «Республика.Кз», причем в отдельных случаях защита не выдерживала и сайты оказывались заблокированными. Это стало поводом для обращения лидеров пяти партий Казахстана к генеральному прокурору с просьбой защитить независимые сайты, Интернет-порталы от «информационного терроризма» и привлечь виновных к ответственности. В дальнейшем в связи с подобными случаями появился термин «виртуальный терроризм». С сентября 2008 года указанные сайты стали подвергаться сетевым атакам, что вынудило многократно менять предлагающих хостинг провайдеров разных стран, а также вызвало серьезные осложнения в работе изданий. А в феврале 2009 года двухнедельные кибератаки вынудили сайты, подверженные атакам уйти в статус «недоступно» и впоследствии они были выведены из строя. Смена провайдера не дала положительного эффекта, так как провайдер отключил IP-адрес сервера. По сообщению от 7 октября 2009 года, веб-ресурсы изданий в течении года подвергались абсолютно всем видам известных сетевых атак с целью прекратить их деятельность, причем данные атаки приносили серьёзный ущерб компаниям, так как они усиливались в момент выпуска новых изданий компании. Целью таких атак является полное уничтожение и прекращение работы разных интернет - ресурсов, чтобы ни один провайдер не смог проложить их у себя. Также подобные атаки могут быть вызваны в политических целях или частных.

Таким образом, современные технологии в СМИ не обладают должной защитой и легко подвергаются кибератакам, которые наносят существенный и серьезный ущерб по компаниям и интернет-изданиям.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТРЕБОВАНИЯ К ПОДАЧЕ ИНФОРМАЦИИ В СМИ

Русяева П.И., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры [2, с. 59].

Существуют цели информационной безопасности такие, как:

– Защита национальных интересов;

– Обеспечение человека и общества достоверной и полной информацией;

– Правовая защита человека и общества при получении, распространении и использовании информации [1, с. 40].

Важнейшим аспектом информационной безопасности является обеспечение объективности и достоверности информации, получаемой населением посредством информационных передач, передаваемых теле- и радиовещательными организациями. Недостаток информации создает благоприятные условия для манипуляций, поэтому Европейская конвенция по трансграничному телевидению устанавливает, что телевещатель должен обеспечивать условия для того, чтобы в новостях факты и события представлялись справедливо и поощрялось свободное формирование мнений. Для соблюдения этого требования к содержанию программ в законодательстве ряда европейских стран вводятся соответствующие нормы. 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 плюрализма и сбалансированности в освещении жизненно важных событий политического, экономического и социального характера. Тенденциозный комментарий, представленный в авторской программе, должен быть сбалансирован освещением других существующих в обществе точек зрения по спорному вопросу путем показа другой авторской программы, круглого стола, дискуссионной программы в разумный период времени [1, с. 47]. Подобные требования к подаче информации в СМИ в той или иной форме установлены во всех демократических государствах Запада. Французское законодательство о телерадиовещании требует соблюдения правила «трех третей», согласно которому при освещении актуальных событий треть выделенного для этого времени предоставляется для выражения своей позиции парламентскому большинству, треть - оппозиции и треть - правительству Французской республики. На выступления президента Франции это правило не распространяется. Американские журналисты при освещении текущих событий строго придерживаются правила отделения факта от комментария. Законодательством о СМИ ФРГ ставятся условия обеспечения внутренним и внешним беспристрастности вещателей. В современной России остро стоит вопрос о правовом обеспечении информационной безопасности в СМИ. Следующие мероприятия и положения могут стать основой этого обеспечения. Обязательными для всех вещателей должны стать положения о необходимости информационной защиты территориальной целостности России в радио- и телепередачах. Законодательством о лицензировании телевещания, радиовещания и вещания дополнительной информации должны устанавливаться ограничения на предоставление лицензии на вещание с территории РФ нерезидентам, доля которых в уставном капитале крупных СМИ должна составлять менее 50 процентов; предусматриваться способы минимизации возможностей их влияния на российское общество. В целях защиты национальных интересов России необходимо ввести обязательные квоты национальной. медиапродукции в эфире российского телерадиовещателей. Установление квот и других подобных правил, разработанных в целях защиты национального языка и культуры - важный элемент в законодательстве многих стран.

Библиографический список

1. Ефимова, Л.Л. Зарубежный опыт правового регулирования защиты информационной безопасности при осуществлении теле- и радиовещания [Текст] / Л.Л. Ефимова // Информационная и психологическая безопасность в СМИ: В 2 т. Т. 1: Телевизионные и рекламные коммуникации. М., 2002. – 322 с.

2. Психология общения. Энциклопедический словарь [Текст] / Под общ. ред. А.А. Бодалева. М., 2011. – 2280 с.

«TELEGRAM» КАК БЕЗОПАСНАЯ ПЛАТФОРМА ДЛЯ ЧИТАТЕЛЕЙ И АВТОРОВ

Уваров А.А., студент
Научный руководитель: Благов Ю.В., к. п. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

В современном мире, интернет-СМИ – основной источник получения информации. Радио, газеты, телевидение – все эти СМИ значительно уступают интернету в популярности. Сегодня почти каждое издание имеет свой личный веб-сайт.

Для большинства информационных ресурсов очень важно качественно и оперативно подавать информацию. А также не менее важно получать обратную связь от своих читателей или слушателей. Все эти потребности удовлетворяет интернет-СМИ.

С возникновением интернет-СМИ, аудитория стала уделять больше времени посещению сайтов тех изданий, которые им интересны. Но чем большим количеством изданий интересовался читатель, тем большее количество сайтов ему приходилось посещать. В какой-то момент этот процесс мог превратиться в не один десяток открытых вкладок в браузере, что уже было не так удобно.

На помощь веб-сайтам пришли социальные сети – онлайн-платформы, которые используются для общения и знакомства. Ярким примером таких платформ могут служить «VK», «Одноклассники» и «Facebook». В социальных сетях стали создаваться «паблики» - сообщества по интересам. Пользователи могут подписываться на различные сообщества, которые в свою очередь формирую новостную ленту. Таким образом, отпадает потребность посещения десятков сайтов, ведь все они теперь умещаются в одной компактной новостной ленте.

Интернет-СМИ стали создавать свои официальные сообщества в социальных сетях. В этих сообществах публиковались либо небольшие материалы, либо аннотации и ссылки на какие-то объемные работы, которые размещались на сайте издательства.

Но удобство пользования должно распространяться не только на читателей, но и на авторов. Несмотря на все плюсы социальных сетей как платформы для публикации новостей, продвижение этих самых новостей является менее удобной задачей. Так, например, если у пользователей слишком большое количество подписок, то новостная лента становится слишком перегружена, и пользователи могут легко пропустить ту или иную новость из-за обилия и перегруза информации.

Теперь уже на помощь социальным сетям приходят мессенджеры – система мгновенного обмена сообщениями. Рассмотрим мессенджер «Telegram». До недавнего времени «Telegram» был практически обычным мессенджером, за исключением того, что в нём было встроено шифрование трафика. Благодаря этому «Telegram» начинал привлекать к себе больше внимания. Со временем в мессенджере стали появляться всё новые и новые функции. Так, последним нововведением стали комментарии к публикациям, прямо как в социальных сетях.

Для контентмейкеров «Telegram» стал буквально идеальной платформой. Если в социальных сетях публикации попадали в новостную ленту, где их легко можно было пропустить, то в мессенджере публикации попадают прямо в личные сообщения пользователя.

Как и написано выше, в «Telegram», также, как и в социальных сетях, есть свои сообщества – чаты – и интернет-СМИ не стали исключением. Они так же создали свои сообщества, но теперь уже в «Telegram».

Brand Analytics – агентство социальных исследований, называет «Telegram» самой цитируемой платформой за период лета 2020 года. 71% всех публикаций рунета цитирует новости из «Telegram» [2].

Но действительно всё ли так хорошо у «Telegram»? С одной стороны – да. Процент цитирований в СМИ может говорить сам за себя. С другой стороны - «Telegram» это в какой-то степени бесконтрольная зона. Администрации каналов мало того, что остаются анонимными, так ещё и не несут никакой ответственности за публикации.

На официальном сайте «Telegram» можно посмотреть статистику каналов по определенным предпочтениям. В разделе «Новости и СМИ» показываются каналы с наибольшим количеством подписчиков [1]. Сравним статистику с популярной социальной сетью «VK». Так, например, канал «RT на русском» в «Telegram» имеет 142 тысячи подписчиков против 1.2 миллионов в «VK», «РИА Новости» имеет 124 тысячи против 2,5 миллионов, «Дождь» 83 тысячи против 480 тысяч, «РБК» 51 тысячу против 774 тысяч и так далее. Разница между платформами огромнейшая.

Но кто же тогда занимает первые места по подписчикам в разделе «Новости и СМИ» в «Telegram»? Если не брать в расчёт каналы, посвященные ситуации в Беларуси, и несколько каналов официальных СМИ то в первой десятке лидеров остаются «Давыдов. Индекс», «Крысиное Королевство» и «Рифмы и Панчи». Первые два имеют почти по 500 тысяч подписчиков, а последний – 360 тысяч. Аудитория довольно-таки большая, но справляются ли

эти каналы со своей задачей как СМИ? На этот вопрос сложнее ответить. Несмотря на то, что эти каналы находятся в категории «Новости и СМИ», со СМИ они ничего общего практически не имеют. На этих канал превалирует субъективная точка зрения на события, а некоторые публикации не проходят фактчекинг. Так, например, «Рифмы и Панчи» несколько раз летом 2020 года публиковали непроверенную информацию о смерти северокорейского политического лидера Ким Чен Ына.

И тут возникает главный вопрос, ответ на который каждый должен дать для себя сам «Является ли «Telegram» хорошей, а главной безопасной платформой для читателей и авторов?».

Библиографический список

1. Каналы «Новости и СМИ». [Электронный ресурс] / URL: https://tlgrm.ru/channels/news

2. Топ-платформы и 100 вириальных русскоязычных медиаресурсов, ИЮНЬ 2020. [Электронный ресурс] / URL: https://br-analytics.ru/blog/top-100-june-2020/

СОДЕРЖАНИЕ

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ В СМИ

В е с т н и к
по безопасности

Выпуск тринадцатый

Компьютерная верстка и дизайн О.Ю. Федосеева

Сдано в набор 14.12.2020.
Подписано к печати 16.12.2020.
Формат 60х84/16. Бумага офсетная.
Гарнитура Times ET.
Печать офсетная. Усл. п.л. 13,75.
Тираж 500 экз. Заказ № 180.