ТЕХНИКО-ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ СЕРВИСА

ISSN 2074-1146

№4(42),2017

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ, издается с 2007 года

Учредитель:

Санкт-Петербургский Государственный Экономический Университет

Адрес редакции:

Санкт-Петербург, Прогонный пер., д.7, лит.А, офис 111
Для писем: 191023, Санкт-Петербург, Садовая ул., 21, офис. 215.
Электронная версия журнала:
http://unecon.ru/zhurnal-ttps;http://elibrary.ru/
Подписной индекс в каталоге «Журналы России» –95008;
тел./факс (812) 3604413; тел**.:** (812) 3684289; +7 921 7512829;
E-mail: *gregoryl@yandex.ru.*
Оригинал макет журнала подготовлен в редакции

Санкт-Петербург – 2017

СОДЕРЖАНИЕ

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

ЭКОНОМИКА ЦИФРОВАЯ И РЕАЛЬНАЯ

"Говорят, что числа правят миром. Нет, они только показывают, как правят миром."[1]

Впервые термин "цифровая экономика" был введен в употребление в 1995-ом году известным американским информатиком Николасом Негропонте. Сегодня этот термин используется по отношению к некому общему направлению развитии экономики в противовес, так называемой "аналоговой экономике", как хозяйственной деятельности общества, а также совокупности отношений, складывающихся в системе производства, распределения, обмена и потребления. Особенно безальтернативно этот термин употребляют политики[2], многие предприниматели и журналисты. В большинстве случаев под термином "цифровая экономика" выражают некое размытое понятие, подразумевающее использование в любых экономических отношениях компьютера, интернета, сотовой связи, т.е. – информационно-коммуникационных технологий.

Однако применяются и более конкретные определения, например: "Цифровая экономика – это виртуальная среда, дополняющая нашу реальность" [3]. Т.е. "Цифровая экономика – часть реальной экономики, которая появилась с созданием компьютера, с появлением и использованием компьютерных технологий, компьютерных сетей, банков и баз данных, содержащих используемую на производстве и в различных производственных отношениях информацию, и имеющих как материальное, так и денежное выражение. До изобретения компьютера виртуальная реальность существовала в виде информации, хранившейся на бумажных и иных носителях (включая книги, картины, денежные знаки и др.), а также в мыслительных процессах и образах. С изобретением компьютера удалось "оцифровать" данную реальность и перевести ее в электронные товары и услуги. В данном смысле, цифровая экономика – это деятельность, непосредственно связанная с электронной коммерцией, в которую входят: сервисы по предоставлению онлайн услуг, интернет-магазины, информационные сайты, зарабатывающие на рекламе и прочие виды деятельности. В итоге можно сказать, что к цифровой экономике можно причислить практически любые способы заработка в сети Интернет. Идея о цифровой экономике начала появляться в последние годы 20-го века. Причиной этому послужило развитие технологий, позволивших осуществлять все больше и больше коммерческих операций в онлайн режиме. Сегодня эта концепция широко применяется к компаниям, предлагающим электронные или цифровые продукты в Интернете. Включая покупку, обработку и доставку этих товаров и услуг, посредством загрузки или предоставления доступа к услугам, размещенным на удаленном сервере.

В последние годы концепция цифровой экономики начала выходить за рамки коммерческого аспекта покупки и продажи электронных продуктов в Интернете. Сегодня эта идея также включает использование виртуальных процессов в рамках текущей деятельности крупных компаний и корпораций. Также данная концепция внедряется во внутреннюю работу правительств для эффективного выполнения транзакций между предприятиями и ведомствами. По мере того, как технологии продолжают развиваться, цифровая экономика продолжит расширяться, поскольку спектр товаров и услуг, предлагаемых в электронном виде, постоянно растет.

Таким образом, под термином "цифровая экономика" сегодня сосуществуют два понятия. Расширенное – цифровая экономика – это экономическое производство с использованием цифровых технологий и классическое – цифровая экономика – это экономика, основанная на цифровых технологиях и относящаяся исключительно к области электронных товаров и услуг. Примерами классического определения являются – дистанционное обучение, цифровое телевидение, интернет и т.п. Примерами расширенного определения являются – производство компью-

[1]Иоганн Вольфганг фон Гёте – немецкий поэт и государственный деятель[2]

[2] Максим Акимов – первый заместитель руководителя аппарата Правительства: «Цифровизация изменит абсолютно все…"

[3]Владимир Иванов – доктор экономических наук, член-корреспондент РАН– РИА Новости; URL: https://ria.ru/science/20170616/1496663946.html

теров, инжиниринговые услуги, производство систем "умного дома" и пр.

В обоих терминах материализованная в виде "цифровой экономики" виртуальная среда становится производительной силой, где создаются новые товары и услуги, строятся товарно-денежные отношения.

Важную часть цифровой экономики сегодня составляют цифровые компьютерные технологии, используемые в науке, в проектировании техники и строительных объектов, в управлении технологическими процессами и производством. Здесь виртуальная реальность совмещена с естественной реальностью: можно исследовать реальные процессы, производить и апробировать реальные объекты в реальных условиях используя при этом их виртуальные модели. В образе подобных технологий, цифровая экономика имеет значительное экономическое превосходство над "аналоговой", которая связана зачастую с многократным производством полномасштабных моделей реальных объектов, их испытанием и разрушением в реальных условиях, а не в виртуальной среде.

Еще одним неоспоримым преимуществом цифровой экономики является оцифровка денежных отношений и электронная коммерция, которая значительно ускоряет реализацию услуг и продукции, а виртуальные платежные системы ускоряют товарообмен, интернет-реклама по своей эффективности превосходит все известные ранее способы оповещения о новом виде товара (услуги).

Обобщая, можно сказать, что цифровая экономика на сегодняшний день является быстро развивающейся неразрывной частью реальной экономики и в значительной степени влияет на материальное производство и качество предоставляемых услуг. Вторым аспектом этого процесса следует считать то, что уровень "цифровизации" реальной экономики в значительной мере зависит от уровня развития цифровой экономики, как отдельной отрасли хозяйства – электронной коммерции. Сегодня развитием этой отрасли хозяйства занимается правительство РФ уже на законодательном уровне, оказывая для ее быстрого развития финансовую и управленческую поддержку[4]. Ориентируясь на принятую стратегию развития информационного общества в РФ [1] в июле 2017 г. Правительством РФ утверждена программа "Цифровая экономика Российской Федерации" [2]. Настоящая Программа, исходит из того, что цифровая экономика представляет собой вид хозяйственной деятельности, направленный на развитие российских информационно-телекоммуникационных технологий, а также на формирование новой технологической основы для социальной и экономической сферы.

Цифровая экономика вошла в перечень основных направлений стратегического развития России до 2025 года[5]. В программе определено приоритетное развитие ключевых сквозных цифровых технологий, включая искусственный интеллект, распределенные реестры, робототехнику, квантовые вычисления, развитие информационно-телекоммуникационной и вычислительной инфраструктуры. Перечислены основные сквозные цифровые технологии, причем предусматривается изменение перечня таких технологий по мере их развития и появление новых технологий и определяет пять базовых направлений развития цифровой экономики в России на период до 2024 года:

- нормативное регулирование;
- кадры и образование;
- формирование исследовательских компетенций и технических заделов;
- информационная инфраструктура;
- информационная безопасность.

Наиболее активно на Программу откликнулся российский бизнес, именно он и рассматривается в качестве основного потребителя продукта информационной экономики, приводящего к полной трансформации процессов внутри компании. Так, благодаря только интернету, даже новые и небольшие из бизнес-компаний могут реализовать собственную продукцию по всему миру. С помощью информационных технологий есть возможность снижать издержки и при этом повышать эффективность и производительность труда во многих отраслях экономики.

Сегодня почти 80% представителей российского бизнеса считают свою компанию цифровой. Хотя понимание цифровизации, как автоматизированного сбора и управления данными, есть только у их малой части. Однако положение компаний на рынке с учетом цифровой экономики становится все более сложным. Увеличиваются риски и уровень неопределенности во время принятия стратегических решений. Чтобы выживать и при этом развиваться в новых условиях, компаниям приходиться повышать собственную компетентность в сфере цифровых информационных технологий. Многие также считают, что в России недостаточно развит отечественный ИТ-

[4] В.В. Путин – "… без цифровой экономики у страны нет будущего."//Москва, 15 июня – РИА Новости.

[5] Опубликован в разделах: Поручения Президента, Комиссии и Советы, Совет по стратегическому развитию и приоритетным направлениям. Дата публикации: 19 июля 2017 года, 17:00

сектор и связывают с этим проблему обеспечения информационной безопасности.

Принятая программа "Цифровая экономика Российской Федерации" [2] своей основной целью ставит выход России на лидерские позиции в данной сфере. «Сегодня уже недостаточно заниматься автоматизацией и цифровизацией отдельных операций или производственных процессов. Качественный скачек эффективности бизнеса предполагает создание моделей управления другого уровня – киберфизических систем. Когда в единое целое соединяются цифровые технологии, оборудование и конечный продукт. Киберфизические системы начинают обмениваться информацией и анализировать ее на этапе производства, и продолжают делать это на протяжении всего жизненного цикла продукта. Вот к чему нам надо готовиться», – считает президент «Ростелекома» Михаил Осеевский [3].

Согласно поручения Правительства РФ, Минкомсвязь, Минэкономразвития (совместно с заинтересованными федеральными органами исполнительной власти, АНО «Цифровая экономика» и АНО «Аналитический центр при правительстве Российской Федерации») должны до 15 февраля 2018 года подготовить и представить в правительство предложения по включению в программу новых направлений, «предусматривающих цифровую трансформацию отдельных отраслей экономики и социальной сферы».

Срок окончания реализации масштабного проекта назначен на 2025 год. К этому времени Минкомсвязи рассчитывает создать широкополосное покрытие сети Интернет даже в самых отдаленных уголках РФ, причем стоимость услуг интернет планируется значительно снизить. "Будут созданы интегрированные цифровые платформы для управления ресурсами (водными, энергетическими, топливными), что позволит объединить всех участников рынка, снизить транзакционные издержки и изменить систему разделения труда" [2]. Для комфортных условий функционирования бизнеса планируется создание «умных городов».

Целями образования в Программе [2] являются решение задач, связанных с подготовкой кадров для цифровой экономики. В том числе: "выпускников образовательных организаций высшего образования по направлениям подготовки, связанным с информационно- телекоммуникационными технологиями, – 120 тыс. человек в год; количество выпускников высшего и среднего профессионального образования, обладающих компетенциями в области информационных технологий на среднемировом уровне, – 800 тыс. человек в год; доля населения, обладающего цифровыми навыками, – 40 процентов". Так, уже 2018 году должны быть разработаны образовательные и профессиональные нормативные документы, требования к описанию компетенций цифровой экономики, запущена их пилотная реализация и апробация. В 2020 г. в интересах цифровой экономики, должны быть обеспечены ресурсами и согласовано работать структуры и механизмы общего, профессионального, дополнительного образования. А в 2024 г. будет обеспечен постоянно обновляемый кадровый потенциал цифровой экономики и соответствующая компетентность граждан.

Для успешного решения стоящих перед образованием целей в первом квартале 2018 г. будут определены целевые показатели международных рейтингов, указывающих на решение задачи, а в IV квартале 2018 г. будет обеспечен в необходимом объеме государственный заказ по перечню специальностей и направлениям подготовки в системе высшего образования, критически важным для развития цифровой экономики. При этом в формировании стратегий развития организаций профессионального образования будут привлекаться высокотехнологичные отечественные компании цифровой экономики. Окончательно система подготовки кадров и переподготовки преподавателей с учетом требований цифровой экономики будет сформирована в IV квартале 2019 г. Тогда же будут созданы комфортные условия для привлечения действующих работников ИТ-индустрии для преподавания в системе профессионального образования по информационным технологиям. К IV кварталу 2020 г. будет создана система "элитного" среднего профессионального образования в области цифровой экономики, обладающая новой нормативной базой, правами независимой аттестации (оценки) обучаемых в отношении уровня сформированности базовых компетенций цифровой экономики как одного из результатов своей деятельности.

Список использованных источников

1.Указ Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” от 11 мая 2017 [электронный ресурс]: http://www.garant.ru/products/ ipo/prime /doc/71570570/#ixzz579uSdUPL (дата обращения 05.10.2017).

2. Программа "Цифровая экономика Российской Федерации" /Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р [электронный ресурс] http://static.government. ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 05.10.2017).

3. Цифровая экономика. Михаил Осиевский. [Интернет рессурс] URL: http://www.comnews.ru/digital-economy/content/111781/quote/2018-02-12/mihail-oseevskiy-prezident-pao-rostelekom

УДК 614.84

РАЗРАБОТКА ПЕЧИ ДЛЯ ИСПЫТАНИЯ НА ОГНЕСТОЙКОСТЬ КАБЕЛЬНЫХ ЛИНИЙ

А.А. Пономарёв[1], М.А. Никитина[2], И.Н. Бутко[3]

Санкт-Петербургский политехнический университет (*СПбПУ*) *Петра Великого,* 195251, *Санкт-Петербург*, *Политехническая*, 29.

Разработка печи для определения огнестойкости кабельных линий принесет удешевление конструкции самой печи и расходы на испытание образцов.

Ключевые слова: Печь, огнестойкость, кабельные линии

DEVELOPMENT OF A FURNACE FOR TESTING THE FIRE RESISTANCE OF CABLE LINES

A.A. Ponomarev, M.A. Nikitina, I.N. Butko

St. Petersburg Polytechnic University, 195251, *St. Petersburg*, *Polytechnical*, 29.

The development of a furnace to determine the fire resistance of cable lines will reduce the cost of constructing the furnace itself and the cost of testing the samples.

Keywords: Bake, firebrick, cable lines

Огнестойкие кабельные линии (ОКЛ) начали применяться относительно недавно. Раньше изоляции кабелей изготавливались на основе слюды, стеклоткани, базальтовой нити и пр. Такой огнестойкий кабель был сложен как по конструкции, так и по технологии изготовления, и поэтому был достаточно дорогой. Как правило, огнестойкий кабель применялся на особо опасных ответственных объектах, например, атомных электростанциях, метро, объекта\х оборонной промышленности и т.п. Кабельные линии применяются для систем противопожарной защиты, где важно сохранять работоспособность в условиях пожара в течение времени, необходимого для своевременной эвакуации людей в безопасную зону. Огнестойкие кабельные линии используется для систем обнаружения, оповещения и управления эвакуацией людей и обеспечения деятельности подразделений пожарной охраны при пожаре. Кроме того, огнестойкие кабельные линии широко применяются для обеспечения аварийного освещения на путях эвакуации, аварийной вентиляции и противодымной защиты, автоматического пожаротушения, внутреннего противопожарного водопровода и лифтов. Дальнейшее развитие техники, появление высокотехнологичных энергоемких производств и объектов развитой инфраструктуры с массовым пребыванием людей выдвинуло на первый план повышение надежности функционирования систем, обеспечивающих безопасность людей, в том числе в условиях пожара. Работа таких систем могла быть обеспечена только стойким к огню кабелем. К этому подталкивало и появление новой нормативной базы. Так в 2003 году был введен в действие ГОСТ Р МЭК 60331-21-2003 «Испытания электрических и оптических кабелей в условиях воздействия пламени», приняты МЧС нормы пожарной безопасности «Проектирование систем оповещения людей о пожаре в зданиях и сооружениях» (НПБ 104-03). НПБ 104-03 обязывали проектировщиков СОУЭ организовывать систему эвакуации людей так, чтобы она могла функционировать в течение времени, необходимого для завершения эвакуации людей из здания во время пожара. В 2005 году вышло постановление правительства Москвы об утверждении региональных нормативов градостроительного проектирования «Нормы и правила проектирования многофункциональных высотных зданий зданий-комплексов в городе Москве МГСН 4.19-2005». В нем были введены требования по обеспечению предела огнестойкости кабелей в зависимости от места прокладки кабелей от 1 часа до 3 часов.

[1]*Пономарёв Александр Алексеевич – магистрант* 1 *курса, СПбПУ, тел.:* +7 960 009 09 33, *email: alexander_ponomarev@outlook.com*

[2]*Никитина Мария Андреевна – магистрант* 1 *курса, СПбПУ, тел.:* +7 981 164 90 73, *email: angrymari@gmail.com*

[3]*Бутко Игорь Николаевич – магистрант* 1 *курса, СПбПУ, тел.:* +7 921 845 85 62, *email: igorbutik@mail.ru*

Основным регламентирующим документом на сегодняшнее время является Федеральный закон №123 «Технический регламент о требованиях пожарной безопасности», а именно статья 82 «Кабельные линии и электропроводка систем противопожарной защиты, средств обеспечения деятельности подразделений пожарной охраны, систем обнаружения пожара, оповещения и управления эвакуацией людей при пожаре, аварийного освещения на путях эвакуации, аварийной вентиляции и противодымной защиты, автоматического пожаротушения, внутреннего противопожарного водопровода, лифтов для транспортировки подразделений пожарной охраны в зданиях и сооружениях должны сохранять работоспособность в условиях пожара в течение времени, необходимого для выполнения их функций и эвакуации людей в безопасную зону.» [1]. Кроме того, требования к кабельным линиям предъявляются согласно ГОСТ Р 53316-2009 «Кабельные линии. Сохранение работоспособности в условиях пожара».

В соответствии с ГОСТ Р 53316-2009 кабельная линия состоит из:

- одного или нескольких параллельных кабелей (проводов, токопроводов), проложенных в коробах, гибких трубах, на лотках, роликах, тросах, изоляторах, свободным подвешиванием, а также непосредственно по поверхности стен и потолков, в пустотах строительных конструкций или другим способом;
- коробок монтажных огнестойких;
- соединительных, стопорных и конечных муфт (уплотнений);
- крепежных деталей.

Согласно вышесказанным документам к кабельным линиям предъявляются требования, для выполнения этих требований кабельным линиям нужно пройти испытания в печи, при температурном режиме которой соответствует температурному режиму пожара. Выход установки на рабочую температуру устанавливается с малыми погрешностями, график представлен на рисунке (рисунок 1).

Одна из разновидностей печей, гидравлическая опрокидывающаяся печь FTT (Рисунок 2) для испытания на огнестойкость вертикальных и горизонтальных образцов – прибор для определения огнеупорности горизонтальных и вертикальных сборных конструкций, колонн либо опор, также служит для определения способности такой продукции, как двери и заслонки, а также строительные материалы, противостоять воздействию высоких температур. Измерение производится при помощи оценки определенных показателей: удельной нагрузки, способности к локализации пожара и теплопроводности материалов и систем

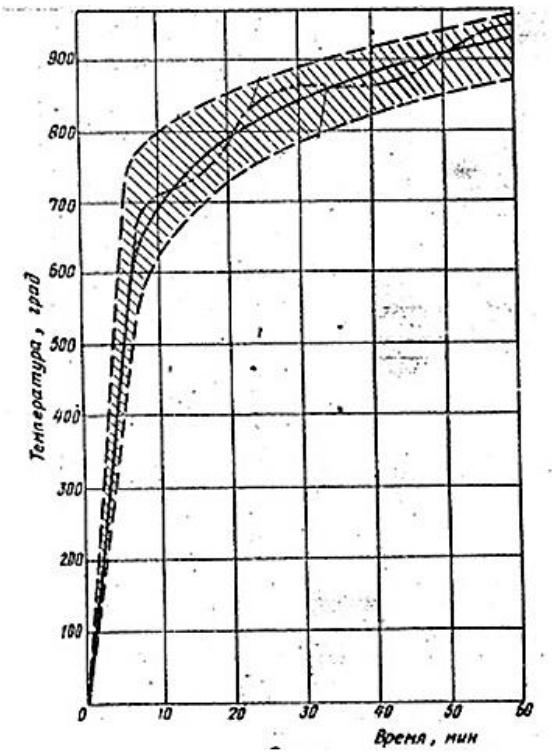


Рисунок 1 – **Стандартный режим пожара**

Рассмотрим основные характеристики системы FTT. Размеры печи для испытания на огнестойкость: 3000 мм (ширина) х 4000 мм (высота) х 1000 мм (глубина).

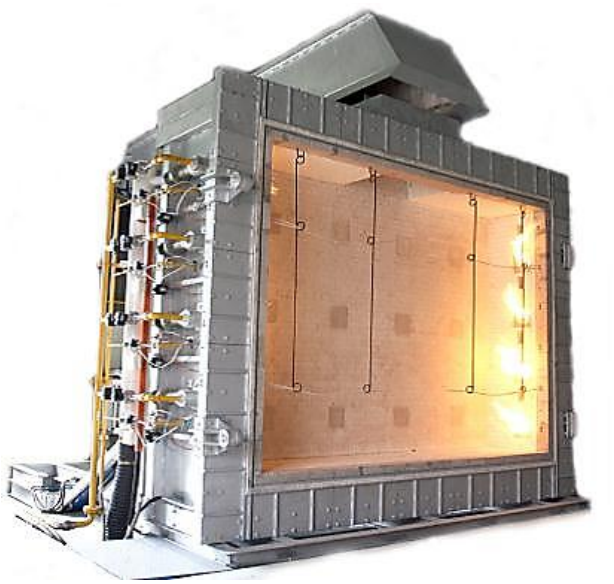


Рисунок 2 – **Печь FTT**

Целью настоящего исследования является разработка малогабаритной лабораторной установки для огневых испытаний кабельных линий. Необходимость такой установки определяется невозможностью постройки крупногабаритной установки, регламентируемой ГОСТ 30247.0-94. Испытание образцов достаточно дорогое мероприятие и печь настоящей разработки будет альтернативой дорогим испытаниям в стандартной печи. Печь такого размера (3х3х3 метра) громоздка и требует много топлива для прогрева в нужном температурном режиме. Разработка должна заменить эту печь и выйти на температурный режим пожара. В ГОСТ 30247.0-94 (ИСО 834-75) Конструкции строительные установлены следующие главные критерии для печи:

- Возможность испытания образцов при требуемых условиях температуры.
- Температура в печи и ее отклонения должны соответствовать температурному режиму пожара. Температурный режим должен обеспечиваться за счет сжигания топлива при этом должен соблюдаться температурный режим пожара, ±10℃ от номинального.
- Пламя не должно касаться образца.

В соответствии с этими требованиями разработана испытательная установка для испытаний кабельных линий, размеры которой не должны превышать значений 800×800×800 см. Эскиз предлагаемой установки представлен на рис. 3.

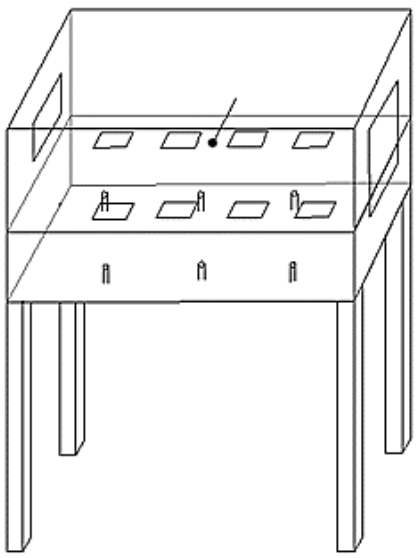


Рисунок 3 – **Эскиз печи**

Печь планируется изготовить из листовой стали, толщина которой будет достаточной для проведения большого числа долговременных огневых испытаний без разрушения или нарушения геометрических размеров конструкции. Внутри печь будет обложена углеродными блоками, которые будут выполнять функцию теплоизолятора. Такое решение будет более экономично, так как топлива для выхода на рабочую температуру потребуется значительно меньше. Крепление образца будет осуществлено за счет термостойкой пластины, которая выдерживает 1200 °С, в которой есть прорези 5×5 см на расстоянии 10 см друг от друга, для воздухообмена и за счет этих прорезей не будет контакта образца с пламенем. Пластина должна быть установлена на высоте 20 см.

Для измерения температуры внутри печи будем применять термопару. Термопара используется для измерения температуры различных объектов, а также в автоматизированных системах управления и контроля. Измерение температур с помощью термопар получило широкое распространение из-за надежной конструкции датчика, возможности работать в широком диапазоне температур и дешевизны. Широкому применению термопары обязаны в первую очередь своей простоте, удобству монтажа, возможности измерения локальной температуры. Они гораздо более линейны, чем многие другие датчики, а их нелинейность на сегодняшний день хорошо изучена и описана в специальной литературе. К числу достоинств термопар относятся также малая инерционность, возможность измерения малых разностей температур. Термопары незаменимы при измерении высоких температур (вплоть до 1300°С). Термопары могут обеспечивать высокую точность измерения температуры на уровне ±0,01°С. Они вырабатывают на выходе термоЭДС в диапазоне от микровольт до милливольт, однако требуют стабильного усиления для последующей обработки. Термопары, в отличие от других датчиков, не нуждаются в источнике тока, но для обработки сигнала термопар требуются прецезионные усилители, например терморегуляторы с цифровой индикацией. Термопара встроена внутри печи и будет измерять температуру воздуха на уровне образца.

Материал термоэлектродов термопары:

а) положительного – сплав хромель (90,5% Ni +9,5% Cr)

б) отрицательного – сплав алюмель (94,5% Ni + 5,5% Al, Si, Mn, Co).

Коэффициент термоЭДС, мкв/°С (в диапазоне температур, °С): 35 – 42 (0 – 1300).

Диапазон рабочих температур, °С: от -200 до +1200.

Предельная температура при кратковременном применении, 1300°С.

Наблюдение за состоянием испытываемого образца будет осуществляться через специальное окно. Окно размером 15×15 см из жаропрочного стекла. Аналогичное окно, размещенное на стенке печи, будет использоваться для видео-фиксации объекта во время огневых испытаний. Окна для печи будут изготовлены из кварцевого песка, выбор такого стекла обусловлен его высокой температурой плавления более 1500°С.

Печь будет использовать сжиженный газ (пропан). Причина выбора пропана как топлива обусловлена его относительно высокой теплотой сгорания. Подача газа в печь будет осуществляться по рампе, которая расположена вне печи для избегания нагрева. Через форсунки (количество которых будет определено опытным путем по результатам испытаний) будет подаваться газ подобно конструкции в форсунки горелки Бунзена (рисунок 4), в форсунке смешивается газ с воздухом, который находится в печи, за счет этого происходит устойчивое горение.

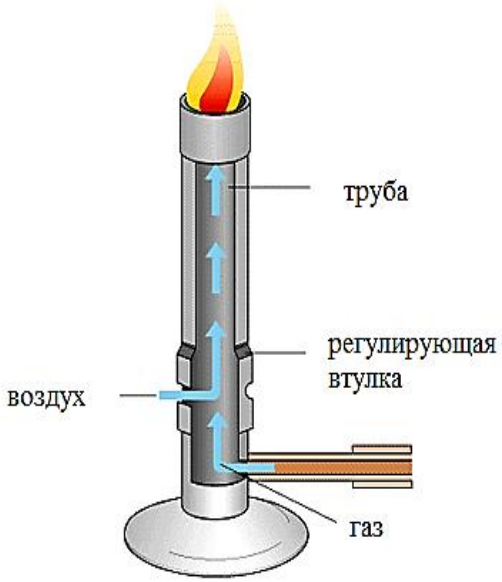


Рисунок 4 – **Форсунка в горелке Бунзена**

Выбор такой конструкции и вида топлива обусловлен его простотой и доступностью. Сжиженный газ легче подать в зону горения, он находится под давлением в баллоне. Если выбирать жидкое топливо, то нужен насос (повыситесь давления), который будет нагнетать топливо в рампу и форсунки. Управление такой системой требует дополнительных электронных блоков. Электронные блоки нужно будет создавать под установку, а это ведет к сильному удорожанию конструкции. Выбор газа под давлением обусловлен тем, что так будет проще регулировать температурный диапазон, регулятор будет стоять на баллоне.

На форсунке можно регулировать топливовоздушную смесь. Тем самым будет регулироваться высота пламени. Оптимальная высота пламени и смесь воздуха/газа будет определена опытным путем.

Разработка этой печи даст нам более выгодный и экономичный вариант установки по определению степени огнестойкости кабельных линий.

Литература

1. Федеральный закон от 22.07.2008 N 123-ФЗ (ред. от 29.07.2017) "Технический регламент о требованиях пожарной безопасности"

2. СП3.13130.2009. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности.

3. СП5.13130.2009. Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования.

4. СП6.13130.2009. Электрооборудование. Требования пожарной безопасности.

5. ГОСТ 30247.0-94 Конструкции строительные. Методы испытаний на огнестойкость.

6. ГОСТ Р 53316-2009 Кабельные линии. Сохранение работоспособности в условиях пожара. Метод испытания.

УДК 661.174

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ДРЕНЧЕРНОГО РАСПЫЛИТЕЛЯ НИЗКОГО ДАВЛЕНИЯ С ТОНКОРАСПЫЛЕННОЙ ВОДОЙ

А.В. Андреев[1], С.В. Сычов[2], М.О. Лепешкин[3]

Санкт-Петербургский политехнический университет (*СПбПУ*) *Петра Великого,*
195251, *Санкт-Петербург*, *Политехническая*, 29.
ООО «Холдинг Гефест»,Санкт-Петербург, ул. Сердобольская, д. 65*, лит. «А»*

Аннотация: В данной статье рассматриваются особенности проведения испытания по ГОСТу Р 51043-2002 дренчерного распылителя низкого давления с тонкораспыленной водой. Использование тонкораспыленной воды при тушении пожаров позволяет достигнуть высокой эффективности в тушении пожара в условиях ограничения по водоснабжению и минимизации ущерба от пролива воды.

Ключевые слова: дренчерный распылитель низкого давления с тонкораспыленной водой, проведение испытаний распылителя по государственным стандартам в России, средняя интенсивность орошения, коэффициент равномерности орошения, средний расход воды.

A STUDY OF THE EFFECTIVENESS OF DELUGE LOW PRESSURE SPRAYER WITH THE WATER MIST

A.V. Andreev, S. V. Sychev, M. O. Lepeshkin

St. Petersburg Polytechnic University, 195251, *St. Petersburg*, *Polytechnical*, 29.

This article discusses the features of testing according to GOST R 51043-2002 of deluge low-pressure sprayer with water mist. The use of fine water in fire fighting allows to achieve high efficiency in fire fighting in conditions of water supply limitation and minimization of damage from water spillage.

Keywords: deluge sprays a low pressure with water mist, testing the sprays according to the state standards in Russia, the average intensity of irrigation, the coefficient of uniformity of irrigation, the average water consumption.

Высокой эффективностью при пожаротушении в небольших помещениях обладают распылители низкого давления с тонкораспыленной водой. Обладая высокой проникающей и охлаждающей способностью, тонкораспыленная вода позволяет надёжно тушить пожары при небольшом расходе огнетушащего вещества.

Недостатком традиционных установок водяного пожаротушения является низкая эффективность использования огнетушащего вещества, в результате чего проливаемое при тушении избыточное количество воды может нанести дополнительный материальный ущерб защищаемому объекту.

Рост удельной поверхности капель за счет более тонкого распыла воды обеспечивает интенсивный теплоотвод из зоны горения, что позволяет сократить время работы распылителя и существенно снизить расход воды на тушение. Уменьшение водяных капель до размеров менее 100 мкм существенно меняет механизм тушения огня. [1, с.64].

Главное достоинство тонкораспыленной воды – это объемно-поверхностный способ тушения пожаров, который позволяет быстро ликвидировать пламенное горение практически всех веществ, за исключением бурно реагирующих с водой с выделением горючих газов и тепловой энергии [2, с.52]. Тонкораспыленная вода, как никакое другое огнетушащее вещество обладает способностью к охлаждению зоны горения ниже температуры воспламенения и уменьшению концентрации реагирующих веществ парами, ниже уровня устойчивого горения.

На сегодняшний день при сертификации дренчерных распылителей проводятся испытания распылителей на равномерность, интенсивность орошения и защищаемую площадь по ГОСТу Р 51043-2002 [3].

В соответствии с по п.8.23 ГОСТ Р 51043-2002 мы провели испытания распылителя низкого давления с тонкораспыленной водой ДУОЗЗ-ЦНГо/0,067-$КУ_2$ В32. Мерные банки размером (250 ± 1) х (250 ±1) мм и высотой не менее 150 мм устанавливались в шахматном порядке (рис. 1), интервал между осями банок составлял (0,50 ± 0,01) м.

[1]*Андреев Андрей Викторович – кандидат военных наук, доцент, директор высшей школы техносферной безопасности, СПбПУ, тел.:* + 7 (812) 294-22-62, *e-mail: office@mes.spbstu.ru*
[2]*Сычев Сергей Васильевич – ведущий специалист отдела НИОКР ООО «Холдинг Гефест» , тел.*: + 7 (921) 313 94 17, *e-mail: sichevs@yandex.ru;*
[3]*Лепешкин Михаил Олегович – студент кафедры пожарной безопасности, высшей школы техносферной безопасности, СПбГПУ, тел.:* +7 981 782 40 33, *e-mail: misha.lepeshckin@yandex.ru*

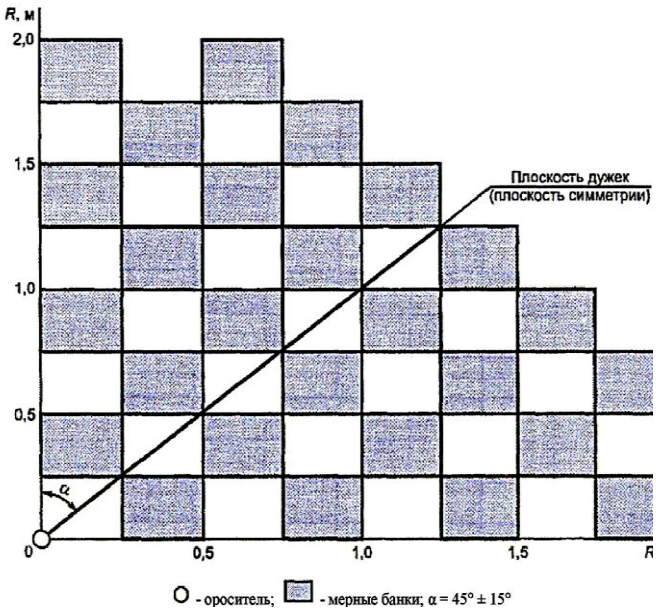


Рисунок 1 – **Схема расположения мерных банок при испытании водяных оросителей**

Распылитель устанавливали на высоте (2,50 ± 0,05) м от верхнего среза мерных банок. Одно из 4 отверстий распылителя диаметром 1,6 мм ориентировали по диагонали квадрата, на котором установлены мерные банки (рис. 2). Такое расположение объясняется тем, что распылитель формирует близкую к квадрату форму площади орошения и имеет два ряда отверстий. Нижний ряд состоит из 8 отверстий диаметром 1,45 мм, а верхний – из 4 отверстий диаметром 1,6 мм, направленных на углы квадрата.

Подачу воды из трубопровода осуществляли при давлении 0.50,6 МПа ± 5%; 0,8 МПа ± 5 %; 1,0 МПа ± 5 %. Продолжительность подачи воды не менее 160с или равна времени заполнения одной из мерных банок.

Среднюю интенсивность орошения водяного оросителя I, дм^3/(м^2*с), рассчитывали по формуле:

$$I = \frac{\sum_{i=1}^{n} i_i}{n}, \qquad (1)$$

где: i_i – интенсивность орошения в i-й мерной банке, дм^3/(м^3*с); n – число мерных банок, установленных на защищаемой площади.

Интенсивность орошения в i-й мерной банке i_i дм^3/(м^3*с), рассчитывали по формуле:

$$i_i = \frac{V_i}{0{,}0625t}, \qquad (2)$$

где: V_i – объем воды (водного раствора), собранный в i-й мерной банке, дм^3; t – продолжительность орошения, с.

Рисунок 2 – **Схема расположения мерных банок при испытании водяных оросителей**

Равномерность орошения, характеризуемую значением среднеквадратического отклонения S, дм^3/(м^2*с), рассчитывали по формуле:

$$S = \sqrt{\frac{\sum_{i=1}^{n} i_i^2 - \frac{\left(\sum_{i=1}^{n} i_i\right)^2}{n}}{n-1}}, \qquad (3)$$

Коэффициент равномерности орошения R рассчитывали по формуле:

$$R = \frac{S}{i_{cp}}. \qquad (4)$$

Распылитель считаем выдержавшим испытание, если средняя интенсивность орошения не ниже нормативного значения при коэффициенте равномерности орошения не более 0,5 и количество мерных банок с интенсивностью орошения менее 50 % от нормативной интенсивности не превышает двух [3].

При проведении испытаний дренчерный распылитель низкого давления с тонкораспыленной водой, имеющим аббревиатуру в соответствии с госстандартом ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32, был установлен в соответствии с ГОСТ 51043-2002 на высоте (2,50 ± 0,05) м от верхнего среза мерных банок. Время подачи воды 180с.

Испытания поочередно проводились при разных давлениях перед распылителем: 0,5; 0,6; 0,8; 1,0 МПа.

После окончания пролива осуществлялось построение эпюры орошения, где отражались данные о количестве воды в каждой из мерных банок. По результатам экспериментов составляли протокол гидравлического испытания оросителя [4]. Оросители считали выдержавшими испытания, если средняя интенсивность орошения была не ниже нормативного значения при

коэффициенте равномерности орошения не более 0,5 и количество мерных банок с интенсивностью орошения менее 50 % от нормативной интенсивности не превышала двух.

Результаты испытаний приведены в таблицах 1 – 4.

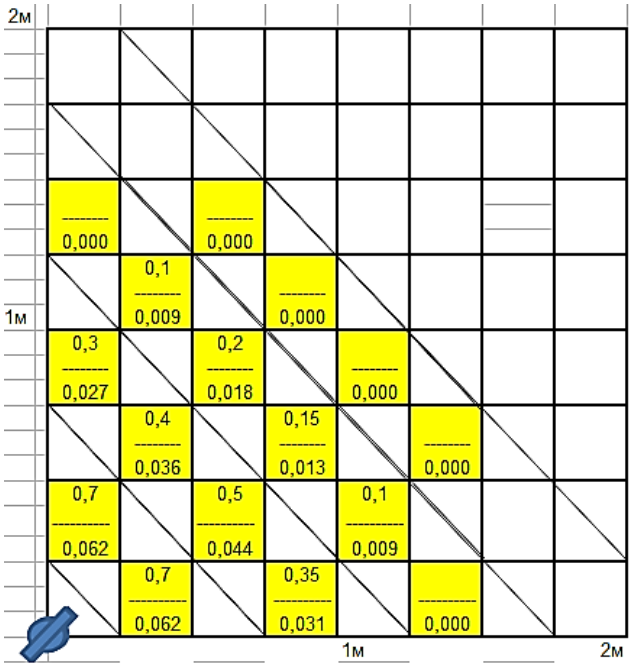


Рисунок 3 – **Карта орошения для распылителя при давлении 0,5 МПа**

Таблица 1 – **Результаты пролива для распылителя при давлении 0,5 МПа**

№	V, л	Qi, л/см^2
1	0,0	0,000
2	0,0	0,000
3	0,1	0,009
4	0,0	0,000
5	0,3	0,027
6	0,2	0,018
7	0,0	0,000
8	0,4	0,036
9	0,15	0,013
10	0,0	0,000
11	0,7	0,062
12	0,5	0,044
13	0,1	0,009
14	0,7	0,062
15	0,35	0,031
16	0,0	0,000
Qср		0,019
СКО		0,022
Rср		1,132

Пояснения: V – объем воды в мерной банке, л; Qi - интенсивность орошения в i-й банке, л/см^2; Qср – средняя интенсивность орошения, л/см^2; Rср – средний расход, л/с.

Испытание при давлении в 0,5 МПа.

Был произведен пролив распылителя ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 при давлении в 0,5 МПа и составлена карта орошения, представленная на рисунке 3.

Средняя интенсивность орошения составляет $Qg_{ср}$=0,019 л/с*м^2. Среднее квадратичное отклонение: S=0,022. Коэффициент равномерности орошения: К$_{ор}$=1,32. Коэффициент производительности при испытаниях: К=0,0247.

Результаты испытаний показали, что в данных условиях распылитель ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 не может считаться эффективным, т.к. коэффициент равномерности орошения более 0,5, в 7 мерных банках из 16 нет воды, нулевые замеры. Средний расход превысил нормальный, что также не удовлетворяет стандартам.

Испытание при давлении в 0,6 МПа.

Был произведен пролив распылителя ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32, при давлении в 0,6 МПа и составлена карта орошения, представленная на рисунке 4.

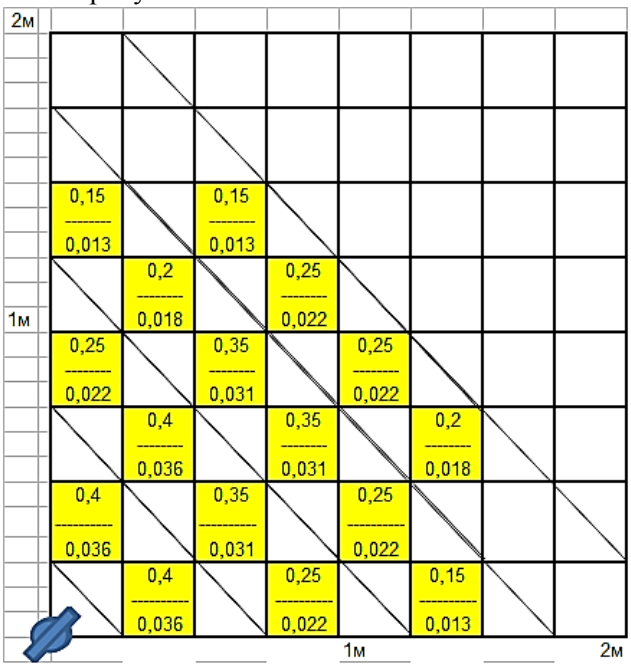


Рисунок 4 – **Карта орошения для распылителя давлении 0,6 МПа**

Средняя интенсивность орошения составляет Q$_{ср}$=0,024 л/с*м^2. Среднее квадратичное отклонение: S=0,008. Коэффициент равномерности орошения: К$_{ор}$=0,336. Коэффициент производительности при испытаниях: К=0,0281.

Результаты испытаний показали, что в данных условиях распылитель ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 может считаться эффектив-

ным, т.к. коэффициент равномерности орошения не более 0,5. Коэффициент производительности 0,0281.

Испытание при давлении в 0,8 МПа.

Был произведен пролив распылителя ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 при давлении в 0,8 МПа, составлена карта орошения, представленная на рисунке 5.

Таблица 2 – **Результаты пролива для распылителя при давлении 0,6 МПа**

№	V, л	Qi, л/см^2
1	0,15	0,013
2	0,15	0,013
3	0,2	0,018
4	0,25	0,022
5	0,25	0,022
6	0,35	0,031
7	0,25	0,022
8	0,4	0,036
9	0,35	0,031
10	0,2	0,018
11	0,4	0,036
12	0,35	0,031
13	0,25	0,022
14	0,4	0,036
15	0,25	0,022
16	0,15	0,013
Qср		0,024
СКО		0,008
Rср		0,34

Средняя интенсивность орошения, л/с*м^2: g$_{ср}$=0,044; Среднее квадратичное отклонение: S=0,011; Коэффициент равномерности орошения: К$_{ор}$=0,241;

Результаты испытаний показали, что в данных условиях распылитель ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 может считаться эффективным, т.к. коэффициент равномерности орошения не более 0,5. Коэффициент производительности составил 0,0447.

Испытание при давлении в 1,0 МПа.

Был произведен пролив распылителя ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 при давлении в 1,0 МПа, составлена карта орошения, представленная на рисунке 6.

Средняя интенсивность орошения, л/с*м^2: g$_{ср}$=0,063; Среднее квадратичное отклонение: S=0,010; Коэффициент равномерности орошения: К$_{ор}$=0,152;

Результаты испытаний показали, что в данных условиях распылитель ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 может считаться эффективным, т.к. коэффициент равномерности орошения не более 0,5. Коэффициент производительности составил 0,0571.

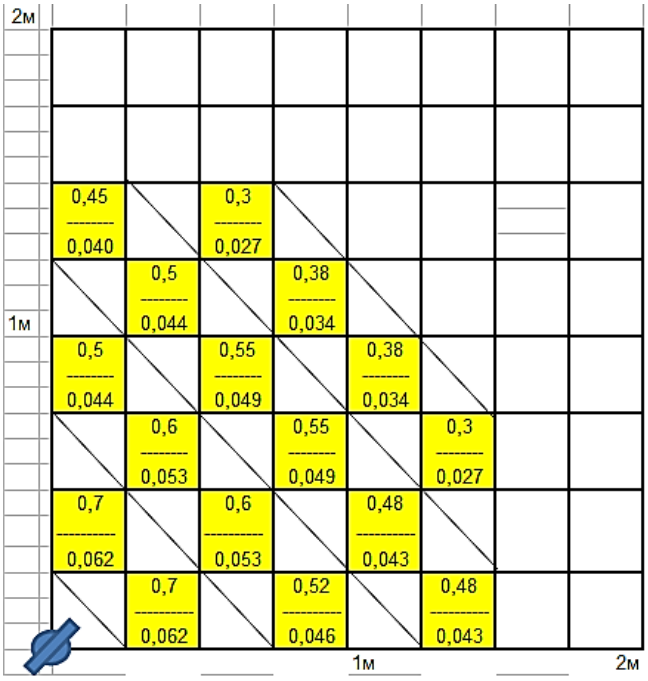


Рисунок 5 – **Карта орошения для распылителя при давлении 0,8 МПа**

Таблица 3 – **Результаты пролива для распылителя при давлении 0,8 МПа**

№	V, л	Qi, л/см^2
1	0,450	0,040
2	0,300	0,027
3	0,500	0,044
4	0,380	0,034
5	0,500	0,044
6	0,550	0,049
7	0,380	0,034
8	0,600	0,053
9	0,550	0,049
10	0,300	0,027
11	0,700	0,062
12	0,600	0,053
13	0,480	0,043
14	0,700	0,062
15	0,520	0,046
16	0,480	0,043
Qср		0,044
СКО		0,011
Rср		0,241

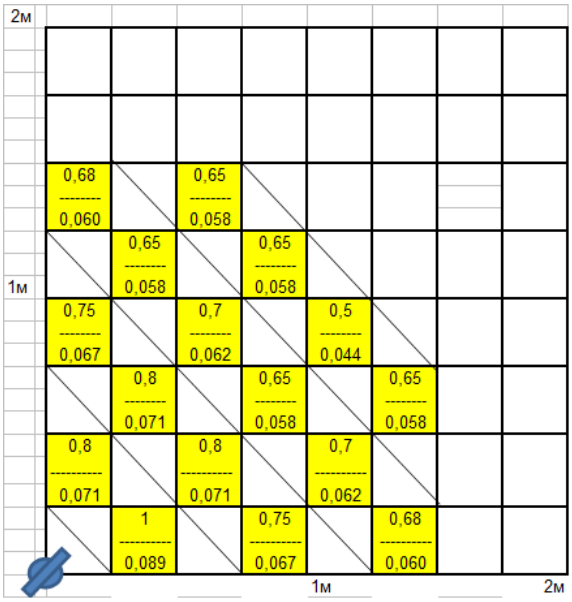


Рисунок 6 – **Карта орошения для распылителя при давлении 1,0 МПа**

По конструктивному исполнению распылитель низкого давления ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 является центробежным с завихряющими шнековыми вкладышами и 12-ю выходными отверстиями. Распылитель дренчерный предназначен для распыливания воды или водных растворов поверхностно-активных веществ по защищаемой площади и объёму путём создания тонкодисперсного потока огнетушащего вещества и применяется для тушения или локализации очагов пожара, создания водяных завес, охлаждения конструкций и технологического оборудования

Таким образом, распылитель низкого давления с тонкораспыленной водой ДУОЗЗ-ЦНГо/0,067-КУ$_2$ В32 считаем выдержавшим испытание при давлении в 0,6, 0,8, 1,0 МПа, так как полученные коэффициенты равномерности орошения и средний расход воды соответствуют государственному стандарту.

Однако при подаче давления в 0,5МПа распылитель эффективно использоваться не может, результаты не соответствующие государственному стандарту, коэффициент равномерности орошения и средний расход воды более 0,5. Поэтому данный распылитель может эффективно применяться при давлении от 0,6 до 1,0 МПа.

Таблица 4 – **Результаты пролива для распылителя при давлении 0,6 МП**

№	V, л	Qi, л/см^2
1	0,68	0,060
2	0,65	0,058
3	0,65	0,058
4	0,65	0,058
5	0,75	0,067
6	0,7	0,062
7	0,5	0,044
8	0,8	0,071
9	0,65	0,058
10	0,65	0,058
11	0,8	0,071
12	0,8	0,071
13	0,7	0,062
14	1	0,089
15	0,75	0,067
16	0,68	0,060
Qcp		0,063
СКО		0,010
Rcp		0,15

Литература

1. Андрюшкин А.Ю., Пелех М.Т. Эффективность пожаротушения тонкораспыленной водой/ А.Ю.Андрюшкин, М.Т. Пелех // Проблемы управления рисками в техносфере. – 2012. – № 1 (21). – С. 64-70.

2. ГОСТ Р 51043-2002 Установки водяного и пенного пожаротушения автоматические. Оросители. Общие технические требования. Методы испытаний. – М.: ИПК Издательство стандартов, 2002. – 27с.

3. Мешман Л.М. Методы испытаний на работоспособность водяных и пенных АУП / Л.М. Мешман, Р.Ю. Губин, А.Г. Дидяев, Л.Т. Танклевский, А.Л. Танклевский // Пожаровзрывобезопасность. – 2016. – № 2. – С. 28-50.

4. Павлов А.П. Опыт использования модульных установок пожаротушения тонкораспыленной водой для защиты объектов различного назначения // Алгоритм безопасности. – 2008. – № 5. – С. 29–31.

5. Саратов Д.Н., Решетов А.П., Бондарь А.А. К вопросу о совершенствовании способа получения тонкораспыленной воды/ Д.Н. Саратов, А.П. Решетов, А.А. Бондарь // Проблемы управления рисками в техносфере. – 2012. – № 1 (21). – С. 52-56.

УДК544.6.076

ИННОВАЦИОННЫЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ НАСЕЛЕНИЯ ЧИСТОЙ ПИТЬЕВОЙ ВОДОЙ

В.А. Камбуров[1], В.Л. Трушевский[2], Т.М. Потапова[3]

[1]*ООО «Институт Комплексного использования и охраны водных ресурсов»* (*КИОВР*), 196158, *Санкт-Петербург, Звёздная улица,* 4 *литер а, помещение* 5-*н;*
[2,3]*Санкт-Петербургский государственный университет* (*СПбГУ*), 199034, *Санкт-Петербург, Университетская набережная* 7–9.

Проведено комплексное исследование проблемных вопросов обеспечения населения РФ чистой питьевой водой. Разработан проект «Чистый водозабор», который предусматривает забор чистой воды, осуществляемого в верховьях рек с последующей транспортировкой ее танкерами-водовозами в специальные терминалы водопотребителей. Предложена последовательность работ при реализации новой технологии водоснабжения питьевой водой из поверхностных водоёмов.

Ключевые слова: вода, структура воды, источники чистой воды, водозабор, транспортировка воды, Северо-Западный регион, Ладожское озеро.

INNOVATIVE WAYS OF PROVIDING THE POPULATION WITH CLEAN DRINKING WATER

V.A. Камбуров, V.L. Трушевский, T.M. Потапова
OOO "Institute of Complex use and protection of water resources",
196158, *St.-Petersburg*, *Pionerskaya street*, 4 *liter a*, *room* 5-*n;*
Saint Petersburg state University, 199034, *St. Petersburg*, *Universitetskaya Naberezhnaya* 7-9.

A comprehensive study of the problematic issues of providing the population of the Russian Federation with clean drinking water. The project "Clean water intake" was developed, which provides for the intake of clean water, carried out in the upper reaches of rivers, followed by transportation of tankers-water carriers in the specialized terminals of water consumers. The proposed sequence of operations when implementing new technologies of water supply drinking water from surface water.

Key words: water, water structure, sources of clean water, water intake, water transportation, Northwest region, Ladoga lake.

Введение. Вопросы, связанные с водоснабжением населения, с каждым годом становятся все острее. Главной проблемой является обеспечение людей качественной питьевой водой.

Рассмотрим, есть ли в воде нечто такое, что мы не знаем, что может вызвать острый интерес, породить цепь каких-то новых и пока непредсказуемых событий? Для начала, обратимся к «Энциклопедическому словарю»: «ВОДА, H2O, жидкость без запаха, вкуса, цвета (в толстых слоях голубоватая); плотность 1,000 г/см3 (3,8°С). При температуре 0°С вода превращается в лед, при 100°С – в пар. Самое распространенное вещество в природе (гидросфера занимает 71% поверхности Земли). Воде принадлежит важнейшая роль в геологической истории планеты и возникновении жизни. Без воды невозможно существование живых организмов (около 65% человеческого тела составляет вода). Вода лежит в основе главного биологического процесса – фотосинтеза. Вода обязательный компонент практически всех технологических процессов как промышленного, так и с.-х. производства. Вода особой чистоты необходима в производстве продуктов питания и медицине, новейших отраслях промышленности (производство полупроводников, люминофоров, ядерная техника), в хим. анализе. Стремительный рост потребления воды и возросшие требования к воде определяют важность задач водоочистки, водоподготовки, борьбы с загрязнением и истощением водоемов».

Проблема строения воды и водных растворов различных неорганических и органических веществ, которыми и являются природные воды, служит предметом тщательного изучения многих исследований и принадлежит к разряду дискуссионных (Вернадский, 1936, Никаноров, 2003) [1, 2].

[1]*Камбуров Владимир Антонович – директор ООО «Институт КИОВР, официальный представитель Союза водопользователей России в Санкт-Петербурге и Ленинградской области, тел.:* +7 921 973 0397, *e-mai: vkamburov@yandex.ru; kiovr@mail.ru*
[2]*Трушевский Виктор Леонидович – кандидат технических наук, доцент факультета географии и геоэкологии Санкт-Петербургского государственного университета* (*СПбГУ*).
[3]*Потапова Татьяна Михайловна – кандидат химических наук, доцент факультета географии и геоэкологии Санкт-Петербургского государственного университета* (*СПбГУ).*

Особенности структуры воды. В последние годы в научных кругах возникло понятие «памяти» воды [3], связанное со способностью воды «запоминать» воздействие их веществ, определяющейся сохранением влияния загрязняющих веществ на структуру воды даже после их полного удаления. Эта способность связана со структурными особенностями воды, которая представляет из себя не одиночные молекулы, а связанные «водородной связью» «ассоциаты» из нескольких молекул, представляющих в пространстве тетраэдры, постоянно обменивающиеся друг с другом молекулами воды (рис.1)

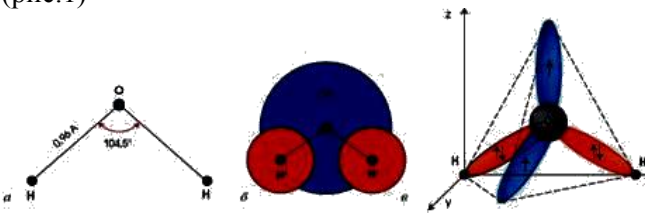


Рисунок 1 – **Строение молекулы воды:** геометрическая схема (а), плоская модель (б) и пространственная тетраэдрическая структура строения воды

Американскими учеными (Фрэком и Уэном) еще в1957 г. была предложена модель строения воды в виде «мерцающих кластеров», состоящих из связанных водородной связью образований, с высокой скоростью обменивающихся друг с другом молекулами воды (рис.2).

Опираясь на современные представления о воде [4] как высоко структурированной жидкости, становится понятным и термин о «памяти» воды как способности сохранять «память» о воздействии на нее различных загрязняющих веществ, растворение которых сопровождается разрывом водородных связей и нарушением ее структуры. Поэтому при загрязнении воды такими соединениями, как нефтепродукты. фенолы, полиароматические углеводороды даже после их полного удаления вода долгое время не может восстановить свои первоначальные свойства вследствие нарушения ее структуры.

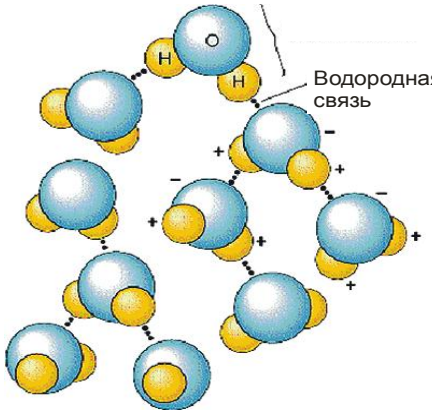


Рисунок 2 – **Модель «мерцающих кластеров» жидкой воды.** Энергия водородной связи ~ 0,17 эВ. Среднее время жизни воды в кластере ~10^{-10} с

Представления о структуре воды с позиций теории водородной связи объясняют и аномалии физико-химических свойств воды (теплоемкости, теплопроводности, плотности, поверхностного натяжения), которые определяют основные климатические и биологические процессы нашей планеты [5]. К наиболее значимым аномалиям воды относится ее высокая растворяющая способность – она растворяет большинство химических веществ, обеспечивая поступление питательных веществ в растения и живые организмы. Важнейшим условием существования жизни на Земле является способность воды за счет капиллярных сил благодаря высокому поверхностному натяжению подниматься по узким почвенным каналам и сосудам растений. Наиболее высокое из всех жидкостей поверхностное натяжение воды важно для физиологии клетки, т.к. обеспечивает процесс передвижения крови по кровеносным сосудам и капиллярного поднятия влаги из нижних слоев почвы в верхние, создавая возможность существования растений в аридной зоне пустынь и полупустынь.

Аномально высокая в сравнении с другими жидкостями теплоемкость воды уменьшает пределы колебаний температуры, обусловливает перенос тепла водными течениями, а также способствует сохранению постоянной температуры тела.

Высокие значения теплоты плавления и испарения определяют термостатирующий эффект воды, благодаря которому Мировой океан поддерживает среднегодовую температуру Земли в пределах 15°С. В противном случае климатические и сезонные перепады температур были бы гораздо резче и приводили бы к бурным ураганам. Достаточно температурному режиму океана дать сбой, как по всей Земле неминуемо прокатываются катаклизмы. Знаменитое явление Эль-Ниньо связано с появлением в тропической зоне Тихого океана теплого течения, которое, медленно продвигаясь от Индонезии к берегам Перу и Чили, вносит коварные поправки в климатические условия. Как правило, этот феномен возникает, когда в силу естественных колебательных процессов перераспределения энергии в океане слабеет сила пассатов, дующих вдоль экватора с востока на запад. В результате, течение устремляется через океан от Индонезии к Перу, и температура воды у побережья Перу поднимается на 3 – 5 °С. Затянувшееся с 1990 по 1995 г. Эль-Ниньо привело к тому, что начиная с 1996 г. по планете периодически прокатываются климатические катастрофы – наводнения там, где их никогда не бывало, великая засуха во влажных областях.

Чрезвычайно важной для биологических процессов является и аномалия плотности воды. которая состоит в том, что она имеет максимум плотности при 4°С, т.е. расширяется при замерзании. Благодаря этому в земных водоемах даже

под сплошным ледяным панцирем температура воды у дна не опускается ниже 4°С, а потому жизнь обитателей водоемов в зимнее время не прекращается. В настоящее время эта аномалия также объясняется с позиций структурных представлений (Самойлов. 1954, Никаноров, 2003) [3, 5]. При замерзании и образовании льда в воде происходит перестройка структуры с переходом из более плотной тетраэдрической в менее плотную «ажурную» гексагональную с образованием ассоциатов из шести молекул (рис.3).

Таким образом, при фазовом переходе из твердой воды в жидкую в узком интервале температур (0° – 4 °С) идет перестройка с частичным присутствием обеих структур, что, очевидно обуславливает особые «живительные» свойства талой воды, оказывающей благоприятное воздействие на растения, животных и человека. Общеизвестен и эффект очищения воды от примесей в процессе вымораживания, который определяется более низкими температурами замерзания солей по сравнению с чистой водой. При замерзании воды в ходе кристаллизации все "лишнее" вытесняется и не входит в структуру льда. Поэтому лед химически чист, даже если образуется из взвеси или раствора (вспомним чистые, прозрачные льдинки в грязной луже), свежевыпавший снег всегда сверкает белизной, а талая вода пленяет исключительной чистотой.

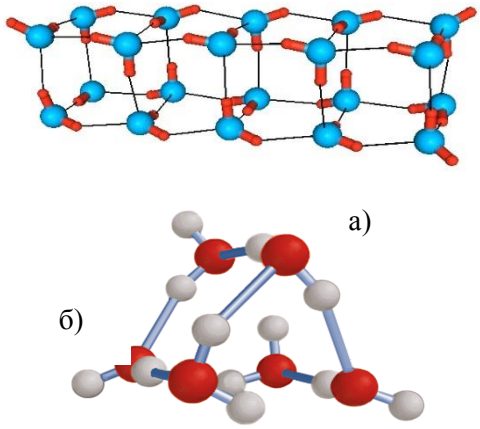


Рисунок 3 – **Гексагональная «ажурная» структура льда** (а) **и тетраэдрическая структура жидкой воды** (б)

Роль талой воды чрезвычайно велика в северных широтах, где большинство рек и озер питаются водами атмосферного происхождения. Так, в работах (Воронкова ,1963) [6] было показано, что доля талых поверхностных вод в северо-западном регионе составляет не менее 40% от общего поступления воды в реки, что определяет низкое содержание растворенных солей в воде.

Качество природных вод. Так как природные воды являются по составу сложными растворами солей, газов и органических веществ (гуминовых кислот) естественного происхождения, то в разных физико-географических условиях формируются воды различной солености, кислотности и жесткости, что и определяет качество природных вод.

При оценке качества вод необходимо иметь в виду принципиальное отличие подземных высокоминерализованных вод и поверхностных вод малой и средней минерализации. В соответствии с современными представлениями в нижних частях осадочного чехла Земли распространены весьма насыщенные солями и микроэлементами воды, в которых содержание «нормально структурированной» воды резко снижается, что и определяет принципиальное различие подземных и поверхностных вод (Никаноров, 1983, Блох, 1969) [7].

Влияние солености на биологические свойства воды носит двойственный характер. С одной стороны, чем ниже минерализация вод, характерная для поверхностных вод северных регионов нашей страны, тем в большей степени она приближается по структуре к дистиллированной воде с прочными водородными связями, что оказывает благотворное влияние на качество питьевой воды. С другой стороны, низкое содержание в такой воде необходимых живым организмам солей кальция, калия, фосфора требует обогащения питьевой воды Крайнего Севера этими элементами.

В аридной зоне сухих степей, наоборот, формируются воды повышенной минерализации, приближающиеся к границе пресных вод (1г/л), которые имеют измененную структуру водородных связей и содержат соли сульфатов и хлоридов в концентрациях, превышающих санитарно-гигиенические нормативы, что требует их специальной очистки. Так, по данным УГМС и экспедиции географического факультета СПбГУ в водах рек Северский Донец и Айдар Белгородской области фоновые (естественные) и современные содержания сульфатов и хлоридов значительно превышают санитарно-гигиенические и рыбохозяйственные нормативы, что не позволяет использовать эти воды для питьевого водопотребления без предварительной обработки.

Очистка природной воды. Сложной проблемой является и прямое питьевое водопотребление подземных вод, что связано не только с их повышенной минерализацией и структурными особенностями, но и с анаэробными условиями, формирующимися в условиях отсутствия контакта с атмосферой и способствующих появлению сапробной (болезнетворной) микрофлоры и увеличением содержания восстановительных газов (аммиака, сероводорода, метана).

Необходимо иметь в виду, что все методы очистки воды с целью уменьшения солености и концентраций взвешенных и органических веществ, связанные с пропусканием через ионообменные колонки, адсорбцией и озонированием приводят к получению воды с нарушенными водородными связями, которая отличаются от пер-

воначальной структуры, что, очевидно сказывается на биологических свойствах воды. Эти вопросы требуют специального комплексного междисциплинарного изучения силами гидрогеохимиков, гидрологов, микробиологов и биологов.

В связи с этим выясняется, что «самого распространенного вещества в природе» в наше время человечеству начинает не хватать, что способно привести к крупнейшим изменениям в мировой экономике и политике.

Водный рынок. О том, что мировое сообщество испытывает с каждым годом все больший дефицит пресной воды, известно давно. Об этом свидетельствуют многочисленные исследования, международные конференции, которые проводились и проводятся под эгидой ООН. Нехватка воды приводит к голоду, смерти, болезни, невозможности достойного существования и осуществления любых экономических программ.

Генеральная Ассамблея ООН провозгласила 2003 год Международным годом пресной воды, чему послужили серьезнейшие проблемы, связанные с острой нехваткой на планете чистой воды.

Около 1.1 миллиарда человек не имеют достаточного доступа к безопасной питьевой воде. Свыше 2.2 миллиона человек, большинство из них дети из развивающихся стран, каждый год умирают от болезней, связанных с дефицитом безопасной питьевой воды (рис. 4). Во многих регионах России и мира увеличивается дефицит качественной питьевой воды.

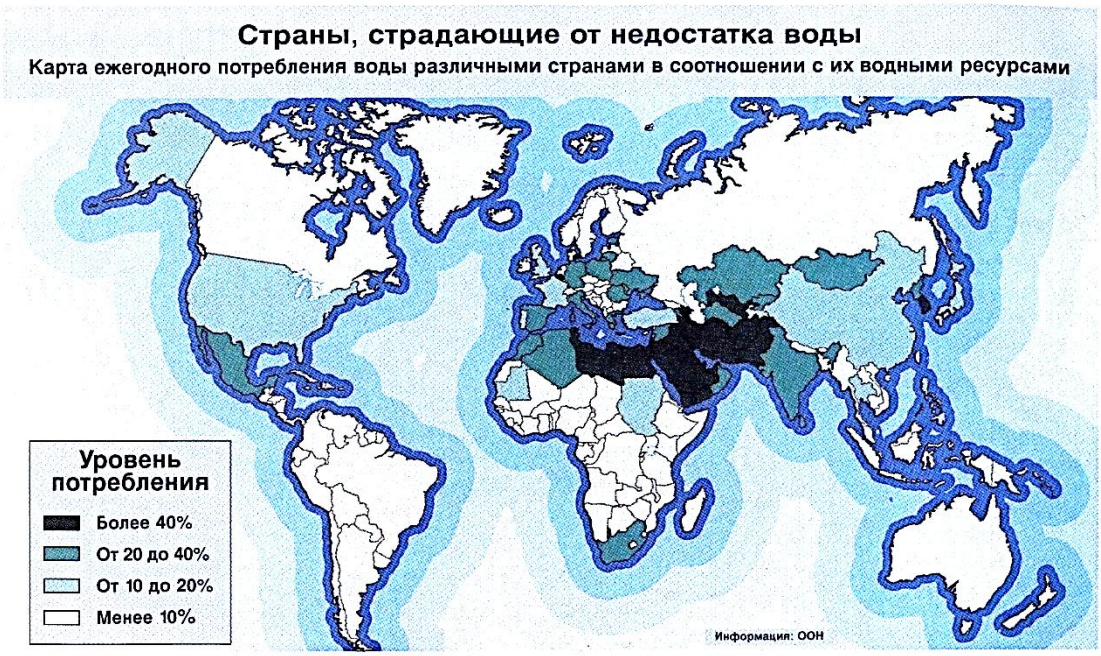


Рисунок 4 – **Карта уровня потребления воды различными странами**

В последние годы все чаще вода рассматривается как источник продовольственной безопасности планеты. Всемирный день защиты окружающей среды уже давно проходит под лозунгом: «Вода – за нее страдают два миллиарда людей!». Продовольственная и сельскохозяйственная организация ООН (ФАО) подсчитала, что через 30 лет воды потребуется еще на 60 процентов больше.

А между тем в ряде регионов мира – на юге Африки, в странах Африканского Рога, на Ближнем и Среднем Востоке – ситуация становится просто катастрофической. Поэтому даже не энергетика, а именно чистая вода стала главной проблемой мира XXI века.

Хотя общие ее запасы на земном шаре позволяют человечеству существовать вполне безбедно. Значит, дело просто в разумном ее накоплении, сбережении и перераспределении.

Сегодня формируется Большой водный рынок, и существуют примеры расчетов передачи водных ресурсов из одной страны в другую. Например, в восьмидесятые годы прошлого века Американские компании затеяли проект по поставке воды арабам из Великих Озер. Он был вполне реален. Но Великие Озера принадлежат как США, так и Канаде. Поэтому проект запутался в межгосударственных претензиях, в спорах фирм двух государств. И возникшие противоречия пока не преодолены. Добавим, что американским танкерам придется преодолевать Атлантический океан, да и воды столь высокого качества, как в России, в США нет. Положение нашей страны в этом смысле гораздо предпочтительнее.

Но какие бы трудности ни стояли на пути создания Большого рынка, он непременно будет сформирован. Учитывая уже сложившуюся ситуацию в мире, это является просто исторической необходимостью. И тот, кто раньше придет на этот рынок, «застолбит» свой участок, тот и получит наибольшие прибыли.

По имеющимся прогнозам, прибыли тут будут значительно выше, чем при продаже нефти и газа. Да еще стоит учесть, что запасы полезных ископаемых исчерпываются, а мы ведем речь о самовозобновляющихся природных источниках. И кто не успел к ним своевременно, тот, как говорится, опоздал. Не случайно в одном из своих выступлений бывший премьер РФ М.М.Касьянов заметил, что Россия могла бы направлять воду в Африку танкерами... Такие обсуждения давно ведутся как в международных, так и в политических и экономических кругах разных стран и СМИ. И Россия может осуществлять такие поставки, поскольку запасы пресной воды в стране огромны и составляют треть от общемировых. Это наше гигантское национальное богатство.

Нет сомнений, что на наших глазах вода становится товаром, но стоимость его окончательно определит только рынок. Пока в основном сформировался лишь рынок, который можно условно назвать Малым.

Малый рынок сегодня обусловлен тем, что в «перестроечные» годы прекратилось развитие и гидроэнергетики и гидромелиорации. Специалисты оказались без заказов, без работы и без зарплаты. Не построено было ничего. А ведь к этому моменту гидротехники вплотную подходили к главному, что обеспечивало благополучие России, – межбассейновому использованию водных ресурсов. Эта идея была загублена на корню. Можно сказать, что этими двумя факторами – общегосударственной бесхозяйственностью и отсутствием прогресса в гидротехнике – и объясняются те трудности в водоснабжении, которые все более начинают испытывать многие российские регионы и города. Хотя, по воле обстоятельств, к прошлому приходится возвращаться. В частности, разрабатывается чрезвычайно выгодный для России проект «Иртыш – Казахстан».

Сейчас в любом магазине или киоске вы можете приобрести бутилированную питьевую воду. Такая торговля в зарубежных странах развилась гораздо раньше. Множество конкурирующих фирм готовы поставлять воду куда угодно. В том числе и в африканские страны. Но она доступна лишь состоятельным людям, и никаких общенациональных проблем решить не может. Обратите внимание на цены: литр питьевой воды стоит гораздо дороже литра нефти.

По данным Всемирной организации здравоохранения, 15 процентов жителей Европы вообще не имеют доступа к воде, которая могла бы считаться питьевой. Ею располагают только Скандинавия и регионы, прилегающие к Альпам. А в остальной Европе нормальная вода – редкость. Но следует учесть, что тут свои традиции и сложилась даже привычка к плохой воде. Поэтому руководители некоторых европейских государств продолжают утверждать, что с водой у них вроде бы все в порядке. Но мы убеждены, что питьевую воду им все-таки придется закупать. Разумеется, в России.

Однако перспективы тут туманны. В перестроечные и последующие годы мы предлагали многим бизнесменам заняться перевозкой воды в больших объёмах. Все они обладали необходимыми капиталами, но наши предложения вызвали с их стороны только настороженность. Никто не оспаривал наших технологических идей и расчетов. Но отчетливо читалась мысль: «Если все так просто, то почему об этом никто раньше не догадался? Сомнительно, страшновато...». Можно вспомнить, что еще президент Джон Кеннеди неоднократно сетовал на косность бизнесменов, на то, что они не понимают собственной выгоды, а также на то, что когда им предлагают принять участие в решении общенациональных проблем, то они попросту скисают. Остается ждать появления нового поколения российских бизнесменов, которые будут более образованными, понимающими и энергичными. Можно, конечно, надеяться, что и государственные чиновники водного хозяйства проникнутся нашими идеями о целесообразности развития Большого рынка воды. В течение последних 20 лет мы давали свои предложения в различные инстанции государственных водных органов.

В настоящее время с 2009 года реализуется «Водная стратегия РФ до 2020 года», выполняются работы по программе Единой России «Чистая вода». В апреле 2012 года утверждена федеральная целевая программа «Развитие водохозяйственного комплекса РФ в 2012 – 2020 годах». Во многих субъектах РФ реализуются региональные экологические и водохозяйственные программы. Основные средства в этих программах направляются на технологии водоподготовки и водоотведения, т.е. на то, чем занимаются водоканалы всегда. Наши попытки «попасть» в какую-либо государственную программу не увенчались успехом.

Перспективы водопользования в Северо-Западном регионе. По нашему убеждению, Петербург и Ленинградская область имеют исключительный шанс стать одним из главных деятелей или, как нынче говорят, игроков на возникающем всемирном Большом рынке воды.

Действительно, наш город на протяжении долгого времени формировался как один из мировых центров гидротехники и гидрологии. ВНИИГ, «Гидропроект», Гидрологический институт, Институт озероведения... – начнешь перечислять, не остановишься. У нас десятки организаций, которые обладают всемирным авторитетом и славой, поскольку по их основаниям и

проектам построены и успешно работают сотни современных гидротехнических сооружений во многих странах мира. Необходимо отметить, что наш город является и крупным центром судостроения. Поэтому создание специального танкерного флота для перевозки воды, с технической точки зрения, не является для него проблемой.

Пусть простят нас коллеги, но перечисление научно-исследовательских и проектных организаций, конструкторских бюро, их работ и заслуг заняло бы больше места, чем сама идея статьи. По той же причине мы не можем в данном случае перечислить имена представителей питерского профессорского корпуса, замечательных специалистов, которые знают о воде, о реках и озерах буквально все. Это не только гидрологи, но и биологи, физики, химики, медики.

Под эгидой Союза водопользователей России в Петербурге при Институте Комплексного использования и охраны водных ресурсов сформировалась инициативная группа, состоящая из гидрологов, проектировщиков, инженеров и других специалистов. Мы предложили программу, которую утвердил Российский союз водопользователей. По ней и работаем, анализируя обстановку с водопользованием в мире и в нашей стране, разрабатывая на общественных началах различные рекомендации и проекты.

Мы живем на берегах уникального и огромного источника пресной воды – Ладожского озера. Надо представлять себе масштабы Ладоги. В ней 900 кубических километров пресной воды, ежегодный сток Невы – около 80 кубических километров. В 1980-е годы десятками научно-исследовательских и проектных институтов Академии наук и Министерства мелиорации и водного хозяйства СССР была обоснована экологическая возможность изъятия 20 процентов стока бассейна Невы и направления их в Волгу. Возможно, это была завышенная оценка. Однако танкерами из Ладожского и Онежского озёр по Волго-Балту можно перевезти не более нескольких сотых процента стока Невы.

В Ладогу впадает немало рек и речушек, которые несут отходы промышленного производства и деятельности человека. Но биологи хорошо знают, что в устьях таких рек образуется биологический барьер, состоящий из колоний микроорганизмов, которые перерабатывают всю органику. Это очень крепкая, надежная биологическая защита. Поэтому в центральной части Ладога вполне здорова, а вода ее, как и прежде, великолепна.

Кроме того, существует малоизвестный факт: в Северной части Ладоги, в ее водяной толще существуют гигантские линзы, состоящие из особо чистой, уникальной по своим характеристикам воды. Природа их изучена не до конца. Высказывается предположение, что их существование обусловлено подпиткой озера подземными водами. Но линзы существуют стабильно, иногда несколько изменяясь в объеме, но, практически не смешиваясь с донными и поверхностными слоями воды.

Идея нашего регионального Проекта состоит в том, чтобы обеспечить поставку этой, особо чистой, воды непосредственно на городские предприятия, занимающиеся производством различных алкогольных и безалкогольных напитков, соков и другой водоёмкой пищевой продукции. Ладога давно нуждается в рекламе. Разумеется, самой добросовестной. И вода из «ладожских линз» могла бы стать могучим брендом и для пищевой промышленности Ленинградской области и Санкт-Петербурга.

Проблемах существующей системы водоснабжения. Более 70% водозаборов питьевой воды в России производится из поверхностных водных объектов (в Ленинградской области – 80%). Плохое качество воды в местах поверхностных водозаборов объясняется большим количеством загрязнений, поступающих в водные объекты со стоками, расположенных выше по течению промышленных и сельскохозяйственных предприятий, а также ЖКХ. В последние годы из-за аварийных сбросов и цветения воды на водозаборах из рек возникали чрезвычайные ситуации, ликвидация которых стоила значительных материальных затрат (Хабаровск, Волгодонск, Краснокамск). По мнению Ветерана водного хозяйства РФ, академика РАСХН, Заслуженного деятеля науки и техники РФ Б.С.Маслова «Главной угрозой здоровью граждан России, национальной безопасности страны является критическое, а в ряде случаев прогрессирующее загрязнение водных объектов вредными веществами, а также истощение ресурсов подземных вод, активизированные пороками системы государственного управления водными объектами, противоречиями и изъянами в законодательстве… По данным Союза водопользователей России только 1% объёма воды, забираемой из поверхностных источников, соответствует нормативу класса качества для питьевых водозаборов… Не менее 50% населения страны потребляет некондиционную воду».

Основным видом деятельности специалистов «Водоканалов» и обслуживающих их научно-технических учреждений в части питьевого водоснабжения является разработка и внедрение технологий и технических средств очистки грязных вод до состояния, пригодного для питья, однако постоянно увеличивающиеся затраты на водоподготовку из-за ухудшающегося качества воды в водных объектах, к сожалению, не всегда дают ожидаемый результат и во многих населенных пунктах не достигаются показатели качества воды, установленные СанПиН 2.1.4.1074-01 для централизованных систем питьевого водоснабжения.

Отдельные положения Водного Кодекса привели к увеличению антропогенного воздействия на водоохранные зоны водных объектов, что также отрицательно повлияло на качество воды в них. Режимы пользования в зонах санитарной охраны (ЗСО) источников водоснабжения хозяйственно-питьевого назначения на большинстве водозаборов из поверхностных водных объектов не соответствуют требованиям СанПиН 2.1.4.1110-02 [8]. Целью мероприятий, предусмотренных этим документом, является максимальное снижение микробного и химического загрязнения воды источников водоснабжения, позволяющее при современной технологии обработки обеспечивать получение воды питьевого качества. Но, расположенные в зонах санитарной охраны водозаборов водопользователи- загрязнители водного объекта, имеющие конкретные планы мероприятий, согласованные с водоохранными и санитарными органами, к сожалению, не обеспечены финансированием. Во втором поясе ЗСО допускается только рубки ухода и санитарные рубки леса, но это требование часто нарушается. Несмотря на запрет сбросов сточных вод, содержание в которых химических веществ и микроорганизмов превышает установленные санитарными правилами гигиенические нормативы качества воды, водопользователи сбрасывают стоки в соответствии с утверждёнными нормативами, в которых содержание многих веществ превышает ПДК и за это загрязнитель перечисляет в бюджет больше платежей. У многих водопользователей даже нет проектов «Зон санитарной охраны источников водоснабжения и водопроводов питьевого назначения».

Резервирование источников питьевого водоснабжения, осуществляемое по Постановлению Правительства РФ № 703 от 20.11.2006 года, предусматривает в качестве альтернативы поверхностным водозаборам только подземные воды, которые зачастую не защищены от загрязнений, а в некоторых месторождениях они не чище поверхностных.

Отсутствует бассейновый принцип комплексного использования и охраны водных ресурсов, основанный на рациональном водопользовании всеми водными объектами, включая сопредельные малоосвоенные территории за пределами границ водосбора.

В условиях кризиса экономики и прогнозируемого снижения уровня жизни населения трудно ожидать увеличения потребления дорогостоящей бутилированной природной воды из уникальных источников и массового распространения качественных индивидуальных водоочистителей.

Вот лишь малый круг проблем существующей системы водоснабжения, обеспечения населения качественной питьевой водой.

Ряд Российских учёных считают, что в ближайшие годы произойдут перемены в водохозяйственной отрасли страны. Оптимизм просматривается в статье координатора федеральной программы Единой России «Чистая вода», директора ОАО «Института микроэкономики» С.Б.Гальперина: «Россия, являясь одной из богатейших стран мира по запасам пресной воды, может и должна в полной мере использовать свой потенциал для гуманитарных задач обеспечения жителей планеты чистой питьевой водой, борьбы с бедностью и нищетой, стать активным участником развития мирового водного рынка. Уже в недалёком будущем России потребуется решать задачи экспорта воды и осваивать этот бизнес».

Президент Союза водопользователей России, Член-корреспондент Международной инженерной академии, лауреат Государственной премии СССР, бывший первый заместитель министра природных ресурсов РФ Н.Н. Михеев, рассуждая о проблемах с питьевым водоснабжением маловодных регионов, написал: « …. Можно было бы эффективно решить эту проблему за счёт воды из Ладоги, где она чистейшая, отстоянная. Были проекты забирать Ладожскую воду танкерами и привозить хоть в Питер, хоть в Калининград, хоть в Эмираты. Но не получилось- танкеров нет, все заняты нефтью». Предложения эти выдвигались во время обсуждения проектов «Переброски стоков», но, ни те, ни другие не были реализованы. «Переброску» «завалили» экологи, а на ТЭО танкерной транспортировки чистой воды не выделили средств.

Возможно, сегодня ситуация изменилась. Итак, несколько осовремененные предложения тридцатипятилетней давности.

Проект «Чистый водозабор». В России много малоосвоенных территорий, где водные объекты практически незагрязненные и отсутствует хозяйственная деятельность (так называемые депрессивные районы). Это – часть территории Северо-Запада Нечерноземья, Сибири, Дальнего Востока и др. Водные объекты этих регионов, в большинстве своем, связаны водными путями с городами, где качество воды в поверхностных водозаборах плохое.

Предлагается доставлять воду из чистых акваторий водных объектов водопользователям, у которых неудовлетворительное качество воды на водозаборах. В качестве средств транспортировки возможны специальные плавучие водовозы простой конструкции, изготовление которых может освоить любая судостроительная верфь.

При отсутствии судоходства или для межбассейновой доставки можно построить каналы или провести водопроводы до судоходных участков рек.

При дефиците воды на территории расположения чистых водозаборов может быть создана система водохранилищ, аккумулирующих паводковый сток, который по каналам или водопроводам поступит в судоходную часть водного

объекта, откуда водовозами будет транспортироваться водопользователям.

В местах доставки необходимо построить водные терминалы, организовать инфраструктуру распределения и доставки воды потребителям. При терминале целесообразно разместить водоемкие пищевые предприятия. При необходимости доочистка может производиться на водовозе или в водном терминале.

Методом экспертных оценок в 2002 году стоимость транспортировки воды на 100 км составляла 30 рублей за кубометр, с учетом окупаемости капитальных вложений, включая водовозы и терминалы, а также зимние удорожания (без учета затрат на инфраструктуру распределения, строительство каналов, водопроводов и водохранилищ). Также не учитывалась плата за водозабор из-за ее незначительности в то время.

На начальной стадии реализации проекта потребителями могут быть социальные, детские, медицинские и др. учреждения на бюджетном финансировании.

После создания современных водовозов и отработки технологий можно будет приступить к экспорту больших объемов воды из Ладожского озера в страны с дефицитом пресной воды. Эта проблема актуальна для многих стран в настоящее время, а в перспективе ситуация ухудшится и количество их будет расти. В засушливом 2008 году обычными танкерами доставляли воду в Барселону и на Кипр.

Эффект от реализации предлагаемой системы водоснабжения населения чистой питьевой водой:

- положительно скажется на здоровье населения в городах, где существуют серьезные проблемы с водоснабжением;
- расширит возможности резервирования существующих водозаборов;
- повысит занятость населения в депрессивных районах;
- реанимирует гидротехническое строительство и судостроение;
- даст существенные дополнительные поступления в федеральный и территориальные бюджеты за счет экспорта воды.

Использование водных ресурсов Северо-Запада России для обеспечения питьевой водой маловодных регионов.

В озерах Северо-Запада имеются значительные запасы высококачественных вод. Вода из Ладожского и Онежского озер может доставляться потребителям танкерами по Волго-Балтийскому водному пути в Поволжье, Москву, Калининград и далее в отдаленные районы и в зарубежные страны. Кроме того, во многих верховьях бассейна Волги также есть места с чистыми поверхностными водными объектами, которые связаны водными путями с низовьями Волги, где вода грязная. Это наиболее экономически выгодный вариант.

Для реализации проекта необходимо построить специальные танкеры-водовозы или специальные плавучие контейнеры, модернизировать Волго-Балтийский водный путь и соорудить терминалы-водохранилища в местах потребления воды (рис. 5).

Наличие качественной питьевой воды позволит развить в маловодных регионах водоемкие пищевые производства. Воду из терминалов целесообразно использовать для производства кондиционированной питьевой воды; безалкогольных и алкогольных напитков и пива; а также отправлять железнодорожными и автомобильными цистернами для доставки потребителям, отдаленным от терминала, а в Калининграде для экспорта в страны ЕЭС.

В настоящее время годовой оборот Волго-Балта равен 15 мл.т. Можно предположить, что при круглогодовой навигации, реконструкции сооружений и фарватеров, объем перевозок будет многократно увеличен.

Рисунок 5 – **Вариант планировки терминала и водоемких производств**

Исходя из очень осторожных оценок, проект экономически целесообразен, т.к. себестоимость чистой воды, доставленной потребителю (с учетом нормативной окупаемости капитальных вложений) не более 1 рубля за литр, а цена реализации свыше 4 рублей.

Косвенным подтверждением этого может служить успешно реализованный проект “Байкальский транзит”, динамично развивающийся мировой рынок бутилированной питьевой воды, энергичные попытки канадских компаний транспортировать воду из Великих озер Северной Америки в Азию, а также проекты транспортировки Антарктических айсбергов.

Для сравнения: высококачественная вода сегодня дороже нефти, а затраты на добычу и транспортировку воды значительно ниже.

Экологических опасений проект не вызывает, т.к. ограниченная пропускная способность водных путей позволяет перевезти не более 0.4 % от объема годового стока р. Невы.

В случае водозабора, осуществляемого в верховьях рек танкерами-водовозами с последующей транспортировкой в специальные терминалы водопотребителей, последовательность работ при реализации новой технологии водоснабжения питьевой водой из поверхностных водоёмов следующая.

Последовательность работ:

- Разработка ТЭО: Определение зон чистого водозабора с использованием ГИС технологий. Расчёт размеров зон особо охраняемых территорий, зон санитарной охраны чистых водозаборов и водоохранных зон. Разработка планов водоохранных мероприятий, включая восстановление водоохранных лесов.

- Корректировка бассейновых соглашений с учётом охраны территорий чистых водозаборов.

- Определение транспортных характеристик водных объектов в зонах чистых водозаборов с предложениями по увеличению их судоходных возможностей, а также с учётом межбассейновых переброс воды.

-Изучение качества питьевой воды в проблемных по водопотреблению регионах.

-Изучение рынка питьевой воды РФ и в зарубежных странах. Переговоры с администрациями и коммунальными службами потенциальных водопотребителей.

-Разработка логистических схем транспортировки воды из чистых водозаборов.

-Разработка предложений по межбассейновым переброскам вод с созданием водохранилищ и гидротехнических сооружений.

-Разработка предложений по водным терминалам водопотребителей.

- Разработка технологий: водозабора; конструкций водовозов и технологий транспортировки воды.

- Расчёты экономических эффектов для разных вариантов и разработка бизнес-планов для разных водопотребителей.

- Выбор пилотных объектов и проектирование: разработка конструкций танкеров-водовозов; изготовление опытных образцов; строительство терминалов у водопотребителей; организация инфраструктуры доставки воды потребителям; опытно-производственная проверка технологий. Разработка бассейновых программ водоснабжения питьевой водой.

- Учреждение ОАО «ТРАНСВОД».

- Включение в список национальных проектов.

-Изучение возможности экспорта воды.

Таким образом, наше предложение социально значимо и, кроме того, создаст новые производства в гидротехническом строительстве, судостроении, пищевой промышленности, торговле, значительно увеличится объем морского и речного судоходства на Северо-Западе.

Первым этапом проекта может быть обеспечение г. Калининграда питьевой водой из Ладожского озера и городов Поволжья из Онежского озера или из чистых судоходных водных объектов в верховьях бассейна Волги. Калининград может стать городом-экспортером питьевой воды и высококачественных напитков в Европу.

Реализация проекта потребует определенных капитальных вложений, т.к. фактически связана с необходимостью создания на “пустом месте” без каких-либо заделов нового сектора экономики. Предстоит решение комплекса технических и технологических проблем. К работе желательно приступить раньше т.к. по прогнозам ученых на Третьем Всемирном форуме по водным ресурсам (16 – 23 марта 2003г., в Киото, Япония) кризис с питьевой водой уже наступил.

Предложение поддержано Союзом Водопользователей России

Литература

1. Вернадский В.И. История природных вод М., ОНТИ 1936- 562с.

2. Никаноров А.М. Гидрохимия.- СПб, Гидрометеоиздат, 2003-356с.

3. Никаноров А.М., Тарасов М.Г. Гидрохимия и формирование подземных вод и рассолов. - Л., Гидрометеоиздат, 1983.-244с.

4. Самарина В.С. Гидрогеохимия- учебное пособие. - Л., Изд-во ЛГУ,1977-380с.

5. Самойлов О.Я. Структура водных растворов электролитов и гидратация ионов М., Изд-во АН СССР, 1957.-182с.

6. Воронков П.П. Формирование химического состава атмосферных вод и влияние его на почвенные растворы и склоновые воды.- Труды ГГИ, 1963 вып.102 с.21-50.

7. Блох А.М. Структура воды и геологические процессы М., Недра, 1969.- 218с.

8. СанПиН 2.1.4.1110-02: Зоны санитарной охраны источников водоснабжения и водопроводов питьевого назначения.

9. Правила резервирования источников питьевого водоснабжения. Утверждены Постановлением Правительства РФ от 20.11.2006 г. №703.

10. «Ещё раз о воде и водном кодексе» Маслов Б.С. « Природно-ресурсные ведомости» №8(347) 2009 г.

11. «Страница редактора» Гальперин С.Б. журнал «Чистая вода» №1, 2010 г.

12. «Вода - природный ресурс для сотрудничества и для жизни» Михеев Н.Н. журнал «Экология и жизнь» №7, 2010г.

УДК_504.75

К ВОПРОСУ ОБ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ АВТОНОМНОЙ РЕСПУБЛИКИ КРЫМ

И.Р. Дубровин[1], Е.Р. Дубровин[2]

НИИ Военно-Системных Исследований МТО ВС РФ Военной Академии МТО имени генерала армии А.В. Хрулёва, 199034, *Санкт-Петербург, наб. Макарова, д.*8

Экологическая безопасность Автономной Республики Крым представляет собой один из важнейших составляющих экологической безопасности Российской Федерации, которая, в свою очередь, является неотъемлемой частью национальной безопасности России.

Ключевые слова: экологическая безопасность, Республика Крым, интересы, угрозы, защита.

TO A QUESTION ABOUT ECOLOGICAL SAFETY OF THE AUTONOMOUS REPUBLIC OF CRIMEA

I.R. Dubrovin, E.R. Dubrovin

Research Institute of the Military System Researches MTO the armed forces Military Academy MTO the name of the army General A. V. Khrulyov, 199034, *Saint-Petersburg, nab. Makarova,* 8

Ecological safety of the Autonomous Republic of Crimea represents one of the most important components of ecological safety of the Russian Federation which, in turn, is an integral part of national security of Russia.

Keywords: ecological safety, Republic of Crimea, interests, threats, protection.

Краткая справка. Автономная Республика Крым один из южных регионов Российской Федерации, расположена на Крымском полуострове, находящимся в северной части Черного моря, и омываемом с запада и юга Черным морем, а с востока и северо-востока Азовским морем, соединенным с континентом узким (до 8 км) Перекопским перешейком. Площадь Крыма – 26860 кв. км, из которых 72% – равнины, 20% – горы, которые образуют полосу (около 160 км длиной и около 40 км шириной), разделяющую Крым на три различные климатические области: степную, горную и южнобережную, остальные 8% – озера, реки и другие водные объекты. Население Республики Крым по переписи 2014 года составляет 2284400 человек. Крупнейшие города: Симферополь (столица Республики), Севастополь, Керчь, Евпатория и Феодосия. Основные отрасли экономики Крыма: промышленность (более 530 крупных и средних предприятий), туризм, строительство, здравоохранение, сельское хозяйство, торговля. Республика Крым имеет развитую транспортную сеть, которая обслуживается автомобильным, троллейбусным, железнодорожным и морским транспортом.

С позиций экологии Крым представляет собой уникальную природную экологическую систему, формируемую географическим расположением, черноморским бассейном мирового океана, рельефом местности и геологическим строением полуострова. Речная система Крымского полуострова характеризуется небольшими показателями плотности и водности. На территории Крыма насчитывается 1657 постоянных и временных водотоков общей длиной 5996 км, из которых только около 150 имеют статус рек, а остальные представляют собой балки или сухие русла, заполняющиеся водой во время ливней и таяния снега.

Большая часть крымских рек имеют длину менее 10 км. Самой длинной рекой полуострова является река Салгир протяженностью более 200 км, из которых почти половина не заполнена водой постоянно.

Экологическая безопасность и её базисные основы. Полное и научно-обоснованное толкование термина «экологическая безопасность» дает возможность не только раскрыть суть данного понятия, но и объективно оценить сегодняшнее экологическое состояние полуострова Крым и правильно выбрать реальные направления, способы и методы практической реализации экологических мероприятий при минимальных затратах.

Э*кологическую безопасность* следует рассматривать, как минимум в 3-х различных аспектах [1, 2, 3], а именно как:

[1]*Дубровин Игорь Рэмович – кандидат технических наук, старший научный сотрудник, тел.*: +7 911 750 85 55;
[2]*Дубровин Евгений Рэмович – кандидат технических наук, старший научный сотрудник, тел.:* +7 911 904 10 24, *e-mail:* dir-er@mail.ru

1) *Составной элемент/составную часть* национальной безопасности Российской Федерации.

2) *Состояние или положение*, при котором отсутствуют реальные и потенциальные угрозы экологическим интересам АР Крым, его регионам, областям и районам, а также отдельным людям, группе людей, отдыхающим, населению, флоре и фауне, возникающие в результате:

- нарушения природного баланса,
- ухудшения качества природной среды,
- истощения природных ресурсов,
- уничтожения естественных экосистем и других негативных последствий, вызванных антропогенным (техногенным) воздействием человека на окружающую среду, а также природными процессами и явлениями.

3) *Сложное комплексное свойство* любого продукта общественного труда, проявляющееся на всех этапах его жизненного цикла и состоящее в способности не нарушать качество окружающей среды и не создавать угрозу жизни людей, фауны и флоры.

Применительно к продуктам общественного труда экологическая безопасность отождествляется с экологической чистотой или экологичностью используемого продукта.

Из представленного определения экологической безопасности следует, что в Крыму в первую очередь необходимо защищать окружающую природную среду, составляющие ее элементы/составные части и экосистемы полуострова, от антропогенной/техногенной деятельности человека. В тоже время население и АР в целом следует защищать от катастроф, бедствий и ситуаций, вызванных как природными, так и антропогенными/техногенными причинами.

Экологические интересы, экологические угрозы, экологическая защита. Экологическая безопасность АР Крым, впрочем, как и других регионов Российской Федерации, базируется на трех основных взаимосвязных понятиях: *экологические интересы жителей и гостей Крыма, экологические угрозы, экологическая защита* [1, 2].

Под экологическими интересами *жителей* и гостей АР Крым понимаются их объективные потребности и нужды жить, трудиться и отдыхать в гармонии с природой, дышать чистым воздухом, пить чистую воду, потреблять безопасные продукты, рационально использовать природные богатства полуострова.

Экологические интересы АР Крым и её районов являются важными и долговременными. Суть всех экологических интересов сводится к сохранению естественной среды обитания Крымского полуострова и его отдельных экосистем в процессе производственной, хозяйственной, курортной, военной и иной другой деятельности людей. Объективно сохранение естественной среды необходимо с целью физического выживания жителей и гостей Крыма, дееспособности полуострова перед экологическими угрозами, а также во время природных и антропогенных/техногенных катастроф и стихийных бедствий.

Сохранение естественной среды обитания и уникальных экосистем Крыма, в свою очередь, возможно лишь за счет поддержания в допустимых пределах качественных и количественных показателей природной и искусственной среды обитания, а также рационального использования природных ресурсов. К экологическим интересам Крыма относится и восстановление естественных экологических систем жизнедеятельности человека (атмосферы, воды, земли), внедрение и использование безотходных высокоэффективных технологий, безопасная утилизация экологически опасных отходов и т. п.

Экологические угрозы Крыму могут быть реальными и потенциальными и исходить как изнутри, так и извне вследствие действия различных антропогенных/техногенных факторов, например, непродуманного, хищнического использования природных ресурсов, внедрения и использования технологий и технологических процессов реально или потенциально опасных для природной среды и человека. Кроме того, в настоящее время экологические угрозы представляют последствия стихийных процессов и явлений, демографическое давление населения на ограниченные ресурсы Крыма, его отдельных районов, истощение природных ресурсов, уничтожение или отравление систем жизнедеятельности человека, животного и растительного мира, накопление радиоактивных, ядовитых, взрывоопасных и других подобного рода технологий и оружия. В последнее время особую угрозу экологической безопасности Крыму, его районам представляет низкая экологическая культура и утрата интереса жителей и гостей полуострова к экологическим проблемам, а также равнодушие абсолютного большинства людей к состоянию окружающей природной среды.

Под *экологической защитой* Крыма понимаются, прежде всего, меры природоохранного назначения, направленные на обеспечение и поддержание экологической безопасности. Природоохранные меры, направленные на предупреждение угроз экологическим интересам относятся к пассивной защите или пассивному обеспечению экологической безопасности. Меры, связанные с ограничением и ликвидацией последствий возникшей экологической опасности,

представляют собой активную экологическую защиту или активное обеспечение экологической безопасности.

Сегодня к пассивной экологической защите Крыма с натяжкой можно отнести природоохранное законодательство АР Крым и требования по его обеспечению; контроль над состоянием природной среды; проектирование систем и конструкций экологического назначения; экологическое обучение и воспитание; эколого-просветительскую агитацию и пропаганду; экологическую паспортизацию, сертификацию, мониторинг и др.

К активному обеспечению экологической безопасности относится реализация экологических мероприятий, практическое выполнение экологических законов и требований, внедрение и использование систем и конструкций экологического назначения, безотходных технологий и технологических процессов, действия людей по предотвращению экологической опасности стихийных бедствий и катастроф.

Основные экологические проблемы современного Крыма. Основными факторами (движущими силами) процесса ухудшения экологической обстановки в АР Крым, по мнению авторов, являются:

- увеличение и сезонная неравномерность антропогенного/техногенного давления на окружающую природную среду, вызванное бытовой, производственной, военной и другой деятельностью людей, а также значительным притоком отдыхающих в курортный сезон. На сегодняшний день на территории Республики Крым имеется 28 официально зарегистрированных полигонов, где накопилось около 18,3 млн. тонн твердых отходов, включая 10,6 млн. тонн токсичных, из которых 866,9 тонн отнесено к запрещенным и неопознанным пестицидам. Количество неофициальных свалок – не учтено.

Большая часть полигонов и свалок давно уже исчерпали свои территориальные и технические возможности, и сегодня представляют собой опасные санитарно-гигиенические объекты. Проблема полигонов и свалок не решается много лет ввиду отсутствия финансирования и дефицита свободных земель.

- комплексное загрязнение среды обитания: территории, воздушного и водного (морского, речного, озерного) бассейнов, а также курортных ресурсов; накопление различных отходов жизнедеятельности населения, промышленных и сельскохозяйственных предприятий, использование устаревших малоэффективных канализационных очистных сооружений;

- постоянное снижение территорий для полезного природопользования и отдыха за счет увеличения площадей полигонов для складирования и хранения промышленных, бытовых и прочих отходов, а также расширения территорий кладбищ для захоронения людей и могильников для захоронения животных;

- дефицит пресной воды (до 70 – 80% в курортный период) и ухудшение ее качественных показателей из-за неудовлетворительного технического состояния водопроводных сетей.

Крымский полуостров имеет крайне сложные условия водоснабжения. Собственные источники пресной воды малочисленны и удовлетворяют потребности полуострова всего лишь на 28%. При этом на 100 подземных водозаборах наблюдается повышенная минерализация, превышающая нормативные показатели ГОСТ в 3 – 4 раза, что представляет собой потенциальную угрозу здоровью людей, являясь одной из причин заболеваний желчекаменной и мочекаменной болезнями. Использование в сельском хозяйстве больших количеств удобрений привело к значительному загрязнению почвы и подземных вод азотистыми соединениями, в том числе нитратами, во многих районах Крыма.

Указанные проблемы резко обостряются в период курортного сезона в связи с притоком большого количества отдыхающих, особенно неорганизованных, и увеличения количества транспортных средств, прибывших из других регионов страны.

Следует особо отметить, что практически во всех зонах отдыха Крыма отмечается заметное антропогенное/техногенное загрязнение курортных ресурсов. В прибрежных морских водах, лечебных грязях и источниках минеральных вод найдены и присутствуют патогенные микробы, пестициды, тяжелые металлы, нефтепродукты, ПАВ, фенолы, радионуклиды, диоксины, полихлорированные бифенилы и дифенилы, что вынуждает постоянно закрывать до 11 пляжей и периодически – многие другие пляжи Крыма в курортный сезон.

Актуальными для Крыма являются проблемы водоотведения. Отсутствие во многих районах полуострова систем централизованной канализации создает экологическую опасность для населения, флоры и фауны и приводит к значительному загрязнению водоемов и почв, чему способствует, в том числе, и несоответствие экологическим требованиям используемых канализационных очистных сооружений.

Дальнейшему ухудшению экологической обстановки на Крымском полуострове способствует низкое качество проводимого мониторинга загрязнения зон отдыха, малоэффективный контроль за содержанием поллютантов в минеральных водах, лечебных грязях и субстратах пля-

жей, а также отсутствие научно-обоснованной концепции по экологическому оздоровлению Крыма и единого подхода к обеспечению его экологической безопасности.

В настоящее время экологических проблем в Крыму достаточно много, однако наиболее значимыми, а, следовательно, и приоритетными в решении являются следующие:

- значительное антропогенное/техногенное загрязнение атмосферного воздуха, поверхностных и подземных вод и почвы, а также химическое и микробное загрязнение курортно-рекреационных ресурсов;

- недостаточное водоснабжение и неудовлетворительное водоотведение во многих районах;

- накопление большого количества токсичных промышленных, сельскохозяйственных и бытовых отходов в населенных пунктах и рекреационных зонах;

- постоянное увеличение площадей несанкционированных свалок, полигонов для хранения отходов, кладбищ и могильников;

- не соответствующая современным требованиям экологическая чистота энергообъектов ТЭК, ЖКХ, промышленных и сельскохозяйственных предприятий, торговых и военных объектов;

- предельная экологическая нагрузка на природную среду в курортных зонах.

Основные загрязнители окружающей природной среды и их источники

Основными загрязнителями окружающей природной среды (территорий, воздушной и водной среды) Крыма являются:

- газообразные загрязнители: выхлопные, дымовые и другие газы, сбрасываемые в атмосферу при работе передвижных (автомобильного, железнодорожного, морского транспорта, кораблей и судов ВМФ) [4] и стационарных топливосжигающих установок (энергообъекты ТЭК, ЖКХ, промышленных и сельскохозяйственных предприятий и др.), технические средства предприятий, торговых и военных объектов (склады ГСМ, газокомпрессорные станции, холодильные установки и т.п.)

Анализ динамики выбросов вредных веществ в атмосферу Крыма показывает, что, начиная с 1998 года среди всех газообразных загрязнителей, доминируют выхлопные газы автомобильного транспорта. В городах Ялте, Симферополе и Евпатории на долю автотранспорта приходится до 70 – 80% выбросов вредных веществ в воздушный бассейн.

- жидкие загрязнители: нефтесодержащие воды, загрязненные ливневые и сточные воды, жидкие отходы промышленных и сельскохозяйственных предприятий, бытовые воды и естественные жидкие продукты жизнедеятельности людей и животных.

Что понимается под обеспечение экологической безопасности. Под обеспечением экологической безопасности Автономной Республики Крым понимается практическая реализация комплекса конструктивных, организационно-технических и эрготических мероприятий, направленных на сохранение и восстановление естественной природной среды Крыма. Реализация этих мероприятий позволяет значительно снизить, а в отдельных случаях, и устранить угрозы, вызванные экологически вредным воздействием человека, промышленных, сельскохозяйственных, военных и других объектов на флору, фауну, личность, общество и регион в целом. Одновременно использование этих мероприятий способно повысить экологическую безопасность/чистоту антропогенных/техногенных объектов Крымского региона, его отдельных районов, территорий и акваторий.

Основные направления повышения экологической безопасности.

Улучшение экологической обстановки в АР Крым целесообразно проводить путем разработки, внедрения и использования мероприятий по трем основным направлениям, а именно: конструктивным; организационно-техническим; эрготическим.

Поскольку ухудшение окружающей природной среды Крыма обусловлено, главным образом, техногенной деятельностью человека, то основным направлением улучшения экологической обстановки является реализация конструктивных мероприятий.

К конструктивным мероприятиям относятся:

- разработка и внедрение систем, устройств и механизмов, в основу функционирования которых положены безотходные экологически чистые технологии;

- практическое использование безотходных экологически чистых технологий;

- оборудование работающих предприятий системами, механизмами и устройствами, позволяющими снижать, а в отдельных случаях устранять, выбросы и сливы вредных веществ в окружающую природную среду;

- создание экологически чистых центров утилизации отходов (мусороперерабатывающих и мусоросжигающих заводов, крематориев и утилизационных комплексов для животных) и другие.

Это самые сложные и затратные мероприятия, поскольку требуют привлечение боль-

шого количества высококвалифицированных специалистов с техническим образованием.

Организационно-технические мероприятия включают в себя:

- правовые, хозяйственные, экономические, социальные, медицинские, научные, технические и иные меры, направленные на сохранение и улучшение окружающей природной среды;
- разработку и введение экологического законодательства [3] (не путать с природоохранным законодательством) Автономной Республики Крым;
- разработку и введение системы штрафных санкций, адекватных загрязнению природной среды;
- разработку и внедрение системы поощрений за сохранение (оздоровление) природной среды, за внедрение и практическое использование экологических технологий;
- разработку и введение научно обоснованных норм и показателей загрязнения окружающей среды;
- разработку и введение способов оценки экологической опасности (безопасности) продуктов общественного труда, включая промышленные и сельскохозяйственные объекты различной формы собственности;
- создание многоуровневой системы экологического воспитания и обучения;
- разработка наглядной агитации, учебников, пособий, плакатов и рекламного материала по экологической тематике;
- создание и расширение экологически чистых зон на Крымской полуострове;
- реформирование, а при необходимости и создание, органов экологического управления и контроля;
- создание центров подготовки и переподготовки экологических кадров и управленцев всех уровней и другие.

Это менее затратные мероприятия, однако, и они требуют привлечения специалистов-экологов различного профиля.

Не менее важным для экологического состояния Крымского полуострова является реализация комплекса *эрготических мероприятий*, а именно:

- экологическое воспитание и образование населения;
- экологическая реклама и агитация;
- экологическая подготовка и переподготовка кадров и управленцев всех уровней и другие.

Данный комплекс мероприятий может быть реализован за счет привлечения подготовленных педагогов, инженеров и специалистов по рекламе.

Очевидно, что все представленные мероприятия следует реализовывать одновременно, поскольку это позволит повысить эффективность процесса оздоровления естественной природной среды Крымского полуострова в целом.

Заключение. Значимость и приоритет внедряемых экологических мероприятий должны определяться, прежде всего, исходя из интересов окружающей природной среды, ее реальных возможностей толерантности, саморегулирования и самоочищения от загрязнителей антропогенного/техногенного происхождения.

Оздоровление естественной природной среды Крымского полуострова априори невозможно без постоянной экологической и эколого-просветительной работы, комплексного и системного подхода к решению экологических проблем, использования современных высокоэффективных экологических технологий, экологического мониторинга и постоянного контроля за состоянием окружающей природной среды. И, главное к экологической работе необходимо привлекать широкий круг специалистов и других людей, не равнодушных к будущему нашей Родины.

Литература

1. Дубровин Е.Р., Дубровин И.Р. Экологическая безопасность в системе национальной безопасности Росси. Мир человека. Том 9, № 1. -С-Пб.: ГУСЭ, 2009 год, с.73-79.

2. Дубровин И.Р., Дубровин Е.Р., Венцюлис Л.С. Экологический аспект концепции национальной безопасности России. Мониторинг. Безопасность жизнедеятельности. № 4, 1996 год, с. 37-40. С-Пб, Издательство «Элмор».

3. Дубровин И.Р., Дубровин Е.Р. Отчет о выполнении НИР «Анализ современного международного законодательства, законодательства Российской Федерации и Санкт-Петербурга в области обеспечения экологической безопасности для подготовки экспертного заключения о целесообразности внесения изменений и (или) дополнений в законодательство Санкт-Петербурга». Законодательное Собрание г. Санкт-Петербурга. Санкт-Петербург 2008.

4. Дубровин Е.Р., Дубровин И.Р. Комплексная система охраны водной среды на Северном флоте. Экология и атомная энергетика. Научно-технический сборник. Выпуск № 2, 2003, с.32-34.

УДК 332.1

МОНИТОРИНГ СОСТОЯНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ И ЦЕНТРАЛЬНОГО ФЕДЕРАЛЬНОГО ОКРУГА

Я.А. Медведева[1]

Санкт-Петербургский-экономический университет,
192007*, Санкт-Петербург, ул. Прилукская, д.* 3

В статье сравнивается состояние экономической безопасности по Центральному федеральному округу и по РФ в целом. Для сопоставления используется система индикаторов экономической безопасности и их пороговые значения.

Ключевые слова: экономическая безопасность, система индикаторов экономической безопасности, пороговые значения

MONITORING OF A CONDITION OF ECONOMIC SECURITY OF RUSSIA AND CENTRAL FEDERAL DISTRICT

Ya.A. Medvedeva

Saint-Petersburg State University of Economics,192007, *Saint-Petersburg, Prilukskaya st.*, 3

The article compares the condition of economic security in Central Federal District and in the Russian Federation in general. The system of indicators of economic security and threshold values is used for comparison.

Keywords: economic security, system of indicators of economic security, threshold values

Индикатор (показатель) экономической безопасности является инструментом для мониторинга и оценки состояния экономических систем и объектов с учетом особенностей их внутреннего функционирования и внешней среды. Оценка состояния экономических систем и объектов требует наличия широкого круга аналитических индикаторов, способных всесторонне характеризовать социально-экономическое состояние исследуемого объекта. Система показателей, определенная Стратегией экономической безопасности [1], выступает совокупностью исследуемых индикаторов для определения уровня безопасности экономики Российской Федерации в целом. Однако региональных показателей законодательно не закреплено.

Рисунок 1 – **Классификация показателей экономической безопасности**

[1]*Медведева Яна Андреевна – студентка Санкт-Петербургского экономического университета, тел.:* +79112838207, *e-mail: medvedeva*1906*@mail.ru*

Показатели экономической безопасности, представленные в Стратегии 2030, имеют разную информационную нагрузку ситуации в экономике. Данную систему следует классифицировать (см. рис. 1) для организации наиболее структурированного подхода к анализу экономической безопасности объектов, а также для определения уровня безопасности не только экономической системы в целом, но и функционирования ее сфер общественной жизни.

Пороговые значения – это количественные и качественные параметры состояния экономики, выход за пределы которых вызывает угрозу экономической безопасности страны, характеризующие различные экономические сферы [2].

На сегодняшний день пороговые значения сорока показателей, необходимые для конкретизации исследований, самостоятельно разрабатываются экспертами. Данный факт является причиной высокой доли субъективизма в значениях, отсутствия единого мнения по поводу состояния, в котором находится экономический объект, а соответственно, и отсутствия единой политики по обеспечению состояния защищенности экономических систем.

Федеральный закон № 172-ФЗ «О стратегическом планировании в Российской Федерации» определяет макрорегион как «часть территории Российской Федерации, которая включает в себя территории двух и более субъектов Российской Федерации, социально-экономические условия в пределах которой требуют выделения отдельных направлений, приоритетов, целей и задач социально-экономического развития при разработке документов стратегического планирования». [3] Соответственно, Центральный федеральный округ можно определить, как макрорегион.

Для сравнения уровня экономической безопасности выбранного федерального округа целесообразно использовать приведенную в Стратегии 2030 систему индикаторов экономической безопасности регионов России, а также учитывать научные труды авторов, определяющих уровень экономической безопасности региона [4, 5, 6, 7, 8, 9].

Сравнение фактических значений индикаторов с пороговыми было проведено по сферам (проекциям) экономической безопасности. Для предметного изучения состояния экономической безопасности использовались пороговые значения, разработанные В.К. Сенчаговым, К.К. Логиновым, С.Н. Митяковым, А. В. Калина, И.П. Савельевой [4, 5, 6, 7].

Далее в приведенных таблицах (см. таблицы 1-4) используется перечень показателей, по мнению автора, наиболее полно отражающий положение каждой из сфер, фактические и пороговые значения по Центральному федеральному округу (ЦФО) и в среднем по России. В расчетах автора использовались данные Федеральной службы государственной статистики [8], Министерства финансов РФ [9]. Ввиду отсутствия значений некоторых индикаторов в базах данных на 2016-2017 года и во избежание временного лага при сопоставлении показателей для сравнения был выбран 2015 год.

В таблице 1 рассмотрена проекция экономического развития.

Таблица 1 – **Система индикаторов экономической безопасности по РФ и ЦФО за 2015 год** (проекция экономического развития)

Индикатор	ЦФО	РФ	Пороговое значение
Отношение годового объема ВРП к среднему по стране	1,31	1	не менее 1
Индекс потребительских цен	113,7 %	112,9 %	не более 106 %
Уровень безработицы	3,5 %	5,6 %	не более 4 % (по МОТ)
Объем экспорта на душу населения (тыс. долл.)	4,3	2,3	не менее 2 тыс. долл.
Инвестиции в основной капитал, % к ВРП (ВВП)	15,8 %	19,6 %	не менее 25 %
Сальдо консолидированного бюджета региона (% к ВРП)	- 0,56 %	-	не менее -3 % и не более 4 %

По результатам выбранных в таблице 1 показателей, отражающих экономическое развитие, можно сделать вывод о том, что только по одному из четырех значений уровень экономической безопасности России выше пороговых значений состояния системы. Существуют проблемы в отношении инвестиций в основной капитал по сравнению с ВРП государства. Инвестиции в основной капитал – совокупность затрат, направленных на создание и воспроизводство основных средств (новое строительство, расширение, а также реконструкция и модернизация объектов) [10]. Исходя из фактических данных, ор-

ганам государственной власти стоит обратить внимание на значение данного показателя ввиду его значимости, а также организовать соответствующую политику в отношении решения данного вопроса. Уровень безработицы в РФ (5,6 %) не удовлетворяет пороговому значению (не более 4 %). Значение индекса потребительских цен по РФ в целом (112,9 %), а соответственно, и по ЦФО (113,7 %) связано с кризисными явлениями 2014-2015 годов.

Уровень экономической безопасности ЦФО в проекции экономического развития по четырем из шести значений показателей оказался выше пороговых значений, а по уровню безработицы ситуация в макрорегионе лучше, чем по России в целом. Угрозы состоянию системы проявляются в значениях индекса потребительских цен и инвестиций в основной капитал, дублируя неудовлетворительное состояние экономической безопасности по стране. В таблице 2 рассмотрена проекция промышленной безопасности.

Таблица 2 – **Система индикаторов экономической безопасности по РФ и ЦФО за 2015 год** (проекция промышленной безопасности)

Индикатор	ЦФО	РФ	Пороговое значение
Степень износа основных фондов промышленных предприятий	43,7 %	47,7 %	не более 60 %
Индекс промышленного производства (в % к пред. году)	97,2 %	96,6 %	не менее 105 %

Промышленная безопасность РФ (таблица 2) по степени износа основных фондов промышленных предприятий в сравнении с пороговым значением находится на допустимом уровне (47,7 %). Однако индекс промышленного производства в 2015 году составил 96,6 %, что ниже порогового значения (105 %).

В отношении промышленной безопасности ЦФО можно сделать вывод о ее более высоком уровне по сравнению с уровнем РФ: значения показателей выше, чем по государству в целом. Однако проблема также связана с индексом промышленного производства. Его значение (97,2 %) ниже требуемого экономически безопасного порога. В таблице 3 рассмотрена социальная проекция.

Проекция социальной сферы (таблица 3) в России находится в зоне риска по всем выбранным показателям: действительные значения каждого из них ниже, чем требуемые экономически безопасные пороговые. Коэффициент фондов почти в 2 раза превышает требуемое пороговое значение. Отношение средней пенсии к средней заработной плате на 4,5 % ниже минимального безопасного уровня (40 %). Ожидаемая продолжительность жизни при рождении составляет 71,39 года, что ниже безопасного значения (75 лет) почти на 4 года. Общий уровень преступности по России в целом превышает допустимое число зарегистрированных преступлений в расчете на 100 тыс. чел. населения (1600) и составляет 1631 случай.

Таблица 3 – **Система индикаторов экономической безопасности по РФ и ЦФО за 2015 год** (социальная проекция)

Индикатор	ЦФО	РФ	Пороговое значение
Отношение средней пенсии к средней заработной плате	29, 0 %	35,5 %	не менее 40 %
Коэффициент фондов (соотношение доходов 10% наиболее и 10% наименее обеспеченного населения)	13,3	15,7	не более 8
Ожидаемая продолжительность жизни при рождении (лет)	72,72	71,39	не менее 75
Общий уровень преступности (число зарегистрированных преступлений в расчете на 100 тыс. чел. населения)	1426	1631	не более 1600

Сложившаяся ситуация в социальной сфере ЦФО по выбранным показателям оказалась частично хуже состояния экономической безопасности в РФ. По отношению средней пенсии к средней заработной плате значение (29,0 %) ниже порогового, а также ниже показателя по России на 6,5 %. Коэффициент фондов в 2015 году составил 13,3, что не удовлетворяет пороговому значению, однако меньше, чем по РФ (15,7). Ожидаемая продолжительность жизни (72,72 года) так же не удовлетворяет минимальному пороговому значению (75 лет), однако немного выше, чем по РФ (71,39 года). Однако единственный показатель ЦФО в данной проекции – «Общий уровень преступности» удовлетворил пороговому значению (1600) и составил 1426 зарегистрированных преступлений в расчете на 100 тыс. чел. населения.

Государство в последние годы активно направляет усилия проводимой политики в социальной сфере, а также подчеркивает ее значимость путем сохранения расходных статей бюджета, имеющих социальную направленность. Тем не менее, необходимо обращать внимание на исполнение положений социальной политики, а также на их результативность. Социальная проекция - одна из важнейших проекций экономической безопасности, однако ее состояние как в России, так и в ЦФО находится в зоне риска. В таблице 4 рассмотрены инновационная и кадровая проекции.

Таблица 4 – **Система индикаторов экономической безопасности по РФ и ЦФО за 2015 год** (инновационная и кадровая проекции)

Индикатор	ЦФО	РФ	Пороговое значение
Внутренние затраты на исследования и разработки (% к ВРП)	2,12 %	1,41 %	не менее 2,2 %
Доля инновационной продукции промышленности (% от общего объема отгруженных товаров, выполненных работ, услуг)	12,8 %	8,4 %	не менее 15 %
Прирост численности населения (%)	0,4 %	0,2 %	не менее 1,35 %
Число лиц, занятых НИР (на 10 тыс. занятого населения)	92,2	52,5	не менее 120 чел.
Число студентов ВПО (на 10 тыс. населения)	372	325	не менее среднего по РФ

Уровень действительных значений выбранных показателей (таблица 4), характеризующих состояние инновационной проекции экономической безопасности России, ниже, чем уровень пороговых значений. Данные обстоятельства свидетельствуют о том, что инновационная проекция так же находится в зоне риска. Внутренние затраты на исследования и разработки минимально должны составлять 2,2 % к ВРП. Значение приведенного показателя по РФ всего 1,41 %. Доля инновационной продукции промышленности по РФ составляет 8,4 % от общего объема отгруженных товаров, выполненных работ, услуг, в то время как пороговое значение по данному индикатору составляет 15 %, что почти в 2 раза выше, чем действительное.

Тем временем инновационная проекция экономической безопасности в ЦФО так же не удовлетворяет пороговым значениям. Вместе с тем, в 2015 году значения показателей были выше, чем в целом по России. Внутренние затраты на исследования и разработки составили 2,12 % к ВРП, что более близко к пороговому значению (2,2 % к ВРП). Доля инновационной продукции промышленности в ЦФО составила 12,8 % от общего объема отгруженных товаров, выполненных работ, услуг, что на 2,2 % меньше, чем пороговое значение, необходимое для уровня состояния защищенности макрорегиона.

Экономическая безопасность РФ в кадровой проекции аналогично находится в зоне риска. Прирост численности населения в 2015 году составил всего лишь 0,2 %, при пороговом значении этого показателя минимум 1,35 %. На 10 тыс. занятого населения число лиц, занятых НИР, по всей стране составило 52,5 человека. Пороговое значение по данному показателю составляет 120 человек, что больше действительного более, чем в 2 раза.

Ситуация в ЦФО относительно кадровой безопасности несколько лучше, чем по РФ в целом, но все же находится в зоне риска. Прирост численности населения в ЦФО на 0,2 % больше, чем по России (0,4 %), однако все-таки ниже порогового значения (1,35 %). Число лиц, занятых НИР, по ЦФО составило 92,2 на 10 тыс. занятого населения. Превышение значения данного показателя над значением по РФ объясняется большой концентрацией ВУЗов, научно-исследовательских центров в ЦФО. В то же время порогового значения (120 чел.) по этому показателю в ЦФО в 2015 году все же не удалось достигнуть. Возможно, что географическое положение, научно-техническое развитие ЦФО повлияло на значение следующего показателя – «Число студентов ВПО», которое в 2015 году составило 372 человека на 10 тыс. населения. Значение выбранного показателя оказалось выше среднего по РФ (325 чел. на 10 тыс. населения), что удовлетворяет условию по пороговому значению.

Таким образом, уровень экономической безопасности России почти по всем выбранным показателям проекций находится в зоне риска. Возможно, большинство неудовлетворительных значений связаны с кризисными явлениями 2014-2015 годов, но государственным органам следует обратить внимание на состояние всех сфер жизни российского общества, а также проводить по-

литику, которая соответствует как времени, так и потребностям общества. Такой подход обеспечит повышение уровня экономической безопасности в целом, а индикаторы и их пороговые значения выступают непосредственным инструментом, позволяющим более качественно и рационально оценить и изменить сложившуюся ситуацию.

Экономическая безопасность ЦФО в разрезе выбранных проекций и с учетом приведенных показателей характеризуется более высокими их значениями. Данный факт непосредственно связан с опережающим развитием ЦФО по сравнению с другими федеральными округами. Однако многие значения индикаторов по Центральному ФО так же не удовлетворяют минимальным пороговым значениям. Определения степени риска в отношении какой-либо проекции и показателя поможет выбрать необходимые и действенные меры урегулирования ситуации.

Проведенное исследование системы индикаторов и пороговых значений экономической безопасности РФ позволило выяснить суть необходимости существования исследуемых показателей. Удалось проанализировать существующую систему, а также выявить пробелы в законодательстве, в частности, отсутствие закрепленных пороговых значений не позволяет однозначно относиться к сложившейся ситуации в экономике. Недостатком на сегодняшний день является и полное отсутствие в законодательстве перечня региональных показателей экономической безопасности, который позволил бы региональным органам власти более детально подходить к оценке собственного уровня экономической безопасности, разрабатывать конкретные меры для его повышения. Важно отметить, что мониторинг и оценка состояния экономической безопасности необходимо осуществлять на всех уровнях государственной власти, независимо от стадии экономического цикла. Такой подход позволит предвидеть надвигающийся кризис, а также максимально возможно избежать его дестабилизирующего воздействия.

В мае 2017 года был сделан серьезный законодательный шаг – разработка современной «Стратегии экономической безопасности Российской Федерации на период до 2030 года», в которой закреплен перечень показателей состояния экономической безопасности. Важно, чтобы положения разработанного документа исполнялись, учитывались при проведении экономической политики. А самое главное для того, чтобы мониторинг и оценка экономической безопасности были предметными, необходимо выражать и сравнивать количественные значение показателей с использованием научно обоснованных методов.

Литература

1. Указ Президента Российской Федерации от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»
2. Указ Президента Российской Федерации от 29.04.1996 г. № 608 «О Государственной стратегии экономической безопасности Российской Федерации (Основных положениях)» (утр. силу - Указ Президента РФ от 13.05.2017 г. N 208)
3. Федеральный закон от 28 июня 2014 г. N 172-ФЗ «О стратегическом планировании в Российской Федерации» (с изменениями и дополнениями)
4. Сенчагов В. К. Инновационные преобразования как императив экономической безопасности региона: система индикаторов / Сенчагов В. К., Максимов Ю. М., Митяков С. Н., Митякова О. И. // Инновации. – 2011. – № 5. – С. 56–61.
5. Логинов К.К. Анализ индикаторов региональной экономической безопасности // Вестник СибАДИ. 2015. № 2 (42). С.132-139.
6. Митяков С.Н. Экономическая безопасность регионов Приволжского федерального округа / С.Н. Митяков, Е.С. Митяков, Н.А. Романова // Экономика региона. 2013. № 3. С. 81-91.
7. Калина А.В. Формирование пороговых значений индикативных показателей экономической безопасности России и ее регионов. / Калина А.В., Савельева И.П. // Вестник Южно-Уральского государственного университета. Серия «Экономика и менеджмент». 2014. Т. 8. N 4. С. 15–24.
8. Новикова И.В. Индикаторы экономической безопасности региона / Новикова И.В., Красников Н.И. // Вестник томского государственного университета. — 2010. — №330 (янв.). — С. 132-138.
9. Чичканов В.П. Анализ подходов к оценке региональных процессов формирования социально-экономической безопасности / Чичканов В.П., Беляевская-Плотник Л.А. // Экономика региона. 2016. № 3. - С. 654-669.
10. Федеральная служба государственной статистики [Электронный ресурс] - URL: http://www.gks.ru/ (дата обращения 24.11.2017).
11. Официальный сайт Министерства финансов РФ [Электронный ресурс] – URL: https://www.minfin.ru/ru/ (дата обращения 24.11.2017).
12.
13. Методологические пояснения [Электронный ресурс] – URL: http://www.tatstat.ru/digital/region5/DocLib1/metod_invest.pdf (дата обращения 24.11.2017).

МЕТОДИЧЕСКИЕ ОСНОВЫ СОВЕРШЕНСТВОВАНИЯ ПРОЕКТИРОВАНИЯ И ПРОИЗВОДСТВА ТЕХНИЧЕСКИХ СИСТЕМ

УДК 004

МОДЕЛЬ УПРАВЛЕНИЯ ТРАНСПОРТНЫМИ СИСТЕМАМИ, УЧИТЫВАЮЩЕЙ ВОЗМОЖНОСТИ ИННОВАЦИЙ

В.Г. Бурлов[1], М.И. Грачев[2]

[1]*Санкт-Петербургский Политехнический Университет Петра Великого,* 195251*, Санкт-Петербург, Политехническая ул.,* 29
[2]*Санкт-Петербургский университет МВД России*, 198206, *Санкт-Петербург, ул. Летчика Пилютова, д.* 1.

В работе предложена математическая модель управления транспортными системами на основе управленческого решения лица принимающего решения. Рассматривается синтез адекватной модели управления с учетом инновационных Web-технологий. Разработанная модель. позволит повысить оперативность управления транспортными системами при удовлетворении требований гарантии достижения цели управления

Ключевые слова: Транспортные системы, управленческое решение, инновационные WEB-технологии, математическая модель, синтез.

THE MODEL OF TRANSPORT SYSTEMS MANAGEMENT, TAKING INTO ACCOUNT THE POSSIBILITIES OF INNOVATION

V. G. Бурлов, M. I. Grachev

St.Petersburg Polytechnic University, 195251, *St. Petersburg, Politekhnicheskaya St.*, 29
St. Petersburg University of the Russian interior Ministry, 198206, *St. Petersburg, st. Letchika Pilyutova*, 1

The paper proposes a mathematical model of transport systems management on the basis of the managerial decision of the person making the decision. The synthesis of an adequate management model is considered taking into account innovative Web technologies. The developed model. will improve the efficiency of the management of transport systems, while meeting the requirements of guaranteeing the achievement of the management objective

Keywords: Transport systems, management decision, innovative web-technologies, mathematical model, synthesis.

Введение. С развитием интернет инновационных технологий (Web-технологий) происходит автоматизация многих направлений жизнедеятельности человека, но и соответственно повышается контроль за транспортными системами, например, в соблюдении участниками движения правил дорожного движения. На основе моделей повышения эффективности управления безопасностью дорожного движения (БДД) с применением инновационных Web-технологий происходит постоянный мониторинг и отслеживание соблюдения правил дорожного движения (ПДД).

БДД – состояние данного процесса, отражающее степень защищенности его участников от дорожно-транспортных происшествий и их последствий.

Обеспечение безопасности дорожного движения – деятельность, направленная на предупреждение причин возникновения дорожно-транспортных происшествий, снижение тяжести их последствий.

[1]*Вячеслав Георгиевич Бурлов – доктор технических наук, профессор, тел.:* +7(911)100-41-01, *e-mail: burlovvg@mail.ru;*
[2]*Михаил Иванович Грачев –* Старший инженер информационного центра, *Санкт-Петербургский университет МВД России, e-mail: mig*2500*@mail.ru, тел.: +7* 911 100 41 01

Инновационные Web-технологии позволяют совершенствовать процесс управления БДД. Для этого необходимо разработать модель управления БДД**,** учитывающей возможности инновационных технологий/ В основе деятельности, как участника движения, так и специалиста по организации и безопасности дорожного движения лежит решение человека. Человек осуществляет свою деятельность на основе модели [1,2]. Поэтому, для осуществления деятельности, адекватной дорожной обстановке, необходимо располагать адекватной математической моделью решения человека. Сложилась интересная ситуация – в публикациях по выработке управленческого решения утверждается, что построить математическую модель решения человека весьма проблематично, если не сказать, что нельзя. А в публикациях представлены только результаты обоснования решения, но не модель самого решения! Но без математической модели решения весьма сложно гарантировать достижения цели управления БДД. Такая же ситуация и с построением системы обеспечения БДД, так как отсутствует критерий синтеза правильно построенной системы. Данная совокупность факторов определяет актуальность настоящей работы. А целью является выбор и обоснование условия гарантированного достижения цели управления БДД на основе синтеза математической модели решения управления безопасностью дорожного движения, учитывающей возможности Web-технологий.

Естественно-научный подход к синтезу модели управления безопасностью дорожного движения, учитывающей возможности Web-технологий. В процессе деятельности по организации и управлению БДД зачастую возникают ситуация, когда результаты деятельности не гарантируют достижение цели управления. Неудовлетворительный результат управления обоснован противоречивыми выводами. Для исключения противоречивых выводов следует использовать аксиоматический метод. Только этот метод позволяет исключить произвол в рассуждениях [3-5].

Для формирования условий, гарантирующих достижения цели деятельности, используется естественно-научный подход (ЕНП) к управлению БДД. ЕНП определяется интеграцией свойств Мышления человека, окружающего Мира и Познания [3-5] реализуется научно-педагогической школой «Системная интеграция процессов государственного управления» [6]. Трёхкомпонентность отражается в трёх принципах [3-5].

1.Принцип трёхкомпонентности познания.

2.Принцип целостности Мира**.** Реализуется ЗСЦО [3-5]**.** Это устойчивая, объективная, повторяющаяся связь свойств объекта и действия при фиксированном предназначении.

3.Принцип познаваемости Мира. Реализуется методами. Декомпозиция. Абстрагирование. Агрегирование.

В процессе деятельности человек оперирует с категориями «система», «модель» и «предназначение». Известно два направления разработки системы (модели). Разработка на основе решения задачи анализа и решение на основе синтеза. Такой подход известен из системотехники [7]. Ещё академик АН СССР Анохин П.К. [1] указывал и экспериментально подтвердил, что для синтеза системы необходимо выявить «основную закономерность» общей теории функциональных систем [1]. В том числе обращался к ведущим специалистам в области создания и исследования систем (например, к М. Месаровичу и др. [10]) с вопросом о разработке формализованного критерия построения системы. Вопрос ответа не получил в известных публикациях, но разрабатывается научно-педагогической школой «Системная интеграция процессов государственного управления» в форме закона сохранения целостности объекта (ЗСЦО) [6]. В настоящей работе для синтеза модели решение используется ЗСЦО [3-5]. Наиболее приемлемым подходом для оценивания адекватности является «полнота учёта основных закономерностей предметной области». Если в области естественных наук для оценивания адекватности модели используются законы физики, химии. То в области сложных систем, социальных, экономических, технико-технологических систем и прочих предлагается использовать ЗСЦО [3-5].

Общий подход к синтезу модели управлении безопасностью дорожного движения, учитывающей возможности Web-технологий. С развитием интернет технологий (Web-технологий) осуществляется автоматизация процессов управления БДД. На основе моделей управления БДД с применением Web-технологий происходит постоянный мониторинг и отслеживание условий адекватной деятельности участников дорожного движения в интересах формирования ЛПР. А реализует данное решение - автоматизированная система. Модель позволяет принимать управленческие решения, соответствующие сложившейся дорожной обстановке.

Известно, что при управлении, единственным невосполнимым ресурсом является время. Использование Wed-технологий позволяет ЛПР сокращать временные характеристики

управленческого решения. Для реализации отмеченных возможностей Wed-технологий необходимо разработать математическую модель решения ЛПР по обеспечению БДД.

ЛПР осуществляет деятельность по обеспечения БДД. Специфическая человеческая форма отношения к окружающему миру, содержание которой составляет его целесообразное изменение в интересах людей, (удовлетворение их потребностей) называется «деятельность» [8]. В основе деятельности по управлению БДД всегда лежит решение человека (лица принимающего решения (ЛПР)) [9].

Человек принимает на основе модели. Под моделью объекта будем понимать описание или представление объекта, соответствующее объекту и позволяющее получать характеристики об этом объекте. Решение – модель процесса, с которым работает человек. Процесс – это объект в действии при фиксированном предназначении. Для синтеза применяем ЕНП, базирующийся на ЗСЦО.

В процессе деятельности человек оперирует с категориями «система», «модель» и «предназначение» («результат») [1,2,3]. Поэтому особенно корректно необходимо рассматривать и использовать эти категории.

Известно всего два направления разработки системы (модели) [7]. При анализе (решение проблемы выбора) проектировщику выдают набор физических элементов и требуют предсказать возможный результата функционирования системы. То есть проектировщик сформирует один вариант системы, другой и так далее, анализирует результат функционирования каждого и выбирает тот вариант, который наиболее полно удовлетворяет требуемым условием. То есть осуществляется перебор вариантов, решается прямая задача. Такой подход принципиально не позволяет гарантировать цели деятельности [7].

При синтезе проектировщику дают набор выходных характеристик системы и требуют определить количественный и качественный состав системы [7]. Главная трудность в том, что надо знать закон построения и функционирования разрабатываемой системы [3].

Также следует рассмотреть особенность синтеза модели объекта (процесса). Ключевым моментом является условие её адекватности. Наиболее приемлемым подходом является «полнота учёта основных закономерностей предметной области» [3]. Если в области естественных наук для адекватности разрабатываемой модели используются законы физики, химии. То области сложных систем, социальных, экономических, технико-технологических систем и прочих предлагается использовать ЗСЦО [3-5].

В соответствии с разработанным ЕНП [3-5] каждый процесс должен быть представлен тремя компонентами, соответствующих свойствам «объективность», «целостность» и «изменчивость» (или понятиям «объект», «предназначение» и «действие»), Эти три компонента располагаются по горизонтали. С одной стороны, они могут интерпретироваться в трёх различных уровнях познания мира (абстрактном, абстрактно-конкретном, конкретном). Такой подход определяет наличие трёх уровней по вертикали.

Введём следующие определения. *Управленческое решение* – условия обеспечение субъектом условий реализации предназначения объекта, которым он управляет, в соответствующей обстановке в интересах достижения цели управления. *Обстановка* – совокупность факторов и условий, в которых осуществляется деятельность. *Информационно-аналитическая работа* – непрерывное добывание, сбор, изучение, отображение и анализ данных об обстановке (маркетинг, разведка, мониторинг). Разложив понятие «управленческое решение» на три базовых элемента «обстановка», «информационно-аналитическая работа» и собственно «решение» необходимо перейти к синтезу модели решения. На рис.1. представлена структурная схема синтеза модели. Такой подход позволяет получать гарантию достижения цели. Руководствуясь принципами Трёхкомпонентности познания, Целостности и Познаваемости осуществим синтез модели [5].

Рисунок 1 – **Структурная схема развёртывания содержания процесса синтеза математической модели решения**

На 1-ом уровне, применяя метод декомпозиции, расчленяем решение именно на три элемента «обстановка», «решение» и «инфор-

мационно-аналитическая работа», которые соответствуют «объекту», «предназначению» и «действию». Применяя на 2-ом уровне метод абстрагирование мы отождествляем «объект» («обстановка») с периодичностью проявления проблемы перед человеком – $\Delta t_{\text{пп}}$. «Предназначение» («Решение») отождествляем с периодичностью нейтрализации проблемы (средним временем адекватным реагированием на проблему) человеком – $\Delta t_{\text{нп}}$. «Действие» («Информационно-аналитическая работа») отождествляем с периодичностью идентификации проблемы (средним временем распознания ситуации) – $\Delta t_{\text{ип}}$**.** Временные характеристики обоснованы тем, что только временные ресурсы для человека невосполнимы. Также результаты исследования в теории функциональных систем академика АН СССР Анохина П.К. показали, что решение человека формируется в схеме «возбуждение», «распознание», «реакция на обстановку». Поэтому в работе при синтезе осуществляется формализация этих трёх элементов.

С позиций ЕНП [3-6] и результатов экспериментальной деятельности Анохина П.К. [1], механизм формирования решения можно представить следующей диаграммой изменения базовых компонентов формирования модели решения (рис.2).

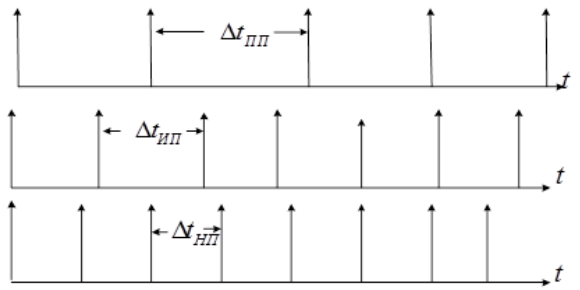


Рисунок 2 – **Диаграмма проявления базовых элементов формирования модели решения**

Синтез модели управления безопасностью дорожного движения, учитывающей возможности Web-технологий. В результате применения методов декомпозиции, абстрагирования и агрегирования мы преобразовали понятие «управленческое решение» в агрегат – математическую модель управленческого

$P = F(\Delta t_{\text{ПП}},\ \Delta t_{\text{ИП}},\ \Delta t_{\text{НП}})$, где P есть вероятность того, что проблема возникающая перед ЛПР распознается и разрешается. Это есть условие существование процесса управления БДД. Среднее время идентификации проблемы $\Delta t_{ИП} = \Delta t_{ИП}^{ЧФ} + \Delta t_{ИП}^{ТО}$; имеет 2 составляющие:

- человеческий фактор (ЧФ), учёт которого в модели решения осуществляется средним временем идентификации проблемы (распознания ситуации) $\Delta t_{ИП}^{ЧФ}$ исходя из персональных психо-физиологических характеристик (ПФХ) ЛПР;

- фактор технической оснащённости (ТО), учёт которого в модели решения осуществляется средним временем задействования возможностей Web-технологий по сокращению времени идентификации проблемы; $\Delta t_{НП}^{ТО} \le 0;$ (данная характеристика всегда величина не положительная, так как, по определению, сокращает длительность) .

Среднее время нейтрализации проблемы $\Delta t_{НП} = \Delta t_{НП}^{ЧФ} + \Delta t_{НП}^{ТО};$ имеет 2 составляющие:

- ЧФ, учёт которого в математической модели решения осуществляется среднем временем нейтрализации проблемы (выработки команды по задействованию ресурсов на нейтрализацию проблемы) $\Delta t_{НП}^{ЧФ}$ исходя из персональных ПФХ ЛПР;

- фактор ТО, учёт которого в модели решения средним временем задействования возможностей Web-технологий по сокращению времени нейтрализации проблемы; $\Delta t_{НП}^{ТО} \le 0;$ (величина не положительная, так как, по определению, сокращает длительность $\Delta t_{ПП}$);.

Такая интерпретация базовых компонентов математической модели решения человека позволила увязать данные элементы с характеристиками возможностей Web-технологий $\Delta t_{ИП}^{ЧФ}$ и $\Delta t_{НП}^{ЧФ}$ через показатель эффективности реализации управленческого решения P (вероятность того, что каждая проблема, возникающая перед ЛПР, распознается им и нейтрализуется). Общий вид зависимости имеет следующий вид.

$$P = F(\Delta t_{\text{ПП}},\ \Delta t_{\text{ИП}},\ \Delta t_{\text{НП}}, \Delta t_{ИП}^{ЧФ}, \Delta t_{НП}^{ТО})$$

Для получения данной зависимости поступим следующим образом. Введем следующие обозначения. λ – величина, обратная среднему времени проявления проблемы; ν_1 – величина, обратная среднему времени идентификации проблемы; ν_2 – величина, обратная среднему времени нейтрализации проблемы. ЛПР при управлении БДД может выполнять в различных сочетаниях две функции: идентифицировать проблему и нейтрализовывать проблему (задействовать ресурсы обеспечения БДД) [1-3]. Используя подход, изложенный в работе [4], поступим следующим образом. Модель решение ЛПР характеризует четыре базовых состояния: A_{00} – ЛПР не идентифицирует и не нейтрализует; A_{10} – ЛПР идентифицирует и не нейтрализует; A_{01} – ЛПР не идентифицирует и нейтрализует; A_{11} – ЛПР идентифицирует и нейтрализует. В соответствии с описанной особенностью управленческого решения необходимо ввести вероятности нахожде-

$\Delta t_{ИП}^{ТО}$

ния нашей системы управления в этих четырёх состояниях. Мы, соответственно, получаем четыре вероятности P_{00}, P_{10}, P_{01}, P_{11}, нахождению системы в состояниях A_{00}, A_{10}, A_{01}, A_{11}. Процесс формирования решения можно рассмотреть, как цепь Маркова, например в работе по исследованию безопасности [11]. Такой подход не позволяет в достаточной мере учитывать динамику процесса, поэтому в работе целесообразно использовать непрерывные цепи Маркова. Для этого используем систему дифференциальных уравнений Колмогорова – Чемпена для рассмотренных состояний нашей системы [4]. Сделав допущения о стационарности процесса, преобразуем систему дифференциальных уравнений к системе алгебраических уравнений и получим решение в следующем виде:

$$P_{01} = \frac{\lambda\nu_1}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2},$$

$$P_{11} = \frac{\lambda\nu_1}{(\nu_1+\nu_2)[(\lambda+\nu_1+\nu_2)+\nu_1\nu_2]}.$$

Получив эти соотношения, мы можем выработать требования к свойствам процесса обеспечения БДД, учитывающим возможности Web-технологий.

$$P_{00} = P_{ОБСЛ}\frac{\nu_1\nu_2}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2} \quad (1)$$

В этом соотношении связаны три параметра, которые зависят от возможности Web-технологий. Таким образом мы установили аналитическую зависимость обобщённых характеристик обстановки ($\Delta t_{пп}$), информационно-аналитической деятельности .

($\Delta t_{ИП} = \Delta t_{ИП}^{ЧФ} + \Delta t_{ИП}^{ТО}$) и нейтрализации проблемы

($\Delta t_{НП} = \Delta t_{НП}^{ЧФ} + \Delta t_{НП}^{ТО}$), возникшей при управлении БДД. Следую работе академика Анохина П.К. [1], мы получили системообразующий фактор создания системы управления БДД в форме соотношения (1).

Выводы. Рассматривая соотношение (1) как условие существования процесса управления БДД и задавая уровень БДД в виде $P_{ОБСЛ}$, располагая характеристикой обстановки $\Delta t_{ПП} = f_1(x_1, x_2, ..., x_n)$, формируется, исходя из условия обеспечения показателя БДД требуемый показатель процесса распознания ситуации $\Delta t_{ИП} = f_2(y_1, y_2, ..., y_m)$ и требуемый показатель результата деятельности по управлению БДД $\Delta t_{НП} = f_3(z_1, z_2, ..., z_k)$. Где вектор X характеризует процесс образования проблемы при управлении БДД, Y характеризует процесс распознания ситуации, а Z характеризует процесс нейтрализации проблемы при правлении БДД. В целом, работе предложен метод управления БДД, позволяющий учитывать возможности инновационных Web-технологий. Синтез системы управления БДД на основе системы дифференциальных уравнений позволил реализовать гарантированный подход к управлению БДД. Модель управления, может быть далее усложнена, введением дополнительных обратных связей и учётом других условий. Данный подход с одной, стороны позволяет синтезировать адекватную модель управления безопасностью дорожного движения, с другой стороны позволяет достаточно полно для практики учитывать возможности инновационных Wed-технологий. Внедрение в систему управления БДД разработанную модель позволит отображать на экране браузера все технологические объекты процесса управления БДД, оперативно получать информацию о ходе дорожного движения, отслеживать состояния объектов дорожного движения с любого рабочего места, в любой точке города в режиме on - line и оперативно принимать решения по дальнейшей логике деятельности. Разработка системы управления БДД на основе предлагаемой в статье модели позволит повысить оперативность управления БДД при удовлетворении требований гарантии достижения цели управления безопасностью дорожного движения.

Литература

1.Анохин П.К. Системные механизмы высшей нервной деятельности. М. "Наука", 1979, - 453 стр.

2.Арбиб М. Метафорический мозг. М.: Мир, 1976. — 296 с.

3.Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы) СПб: Факультет Комплексной Безопасности, СПБГПУ.2007г.-265 с.

4.Бурлов В.Г. Математические методы моделирования в экономике. Часть 1, -С-Пб. СПбГПУ, Факультет безопасности, НП «Стратегия будущего», 2007.-330с.

5.Бурлов В.Г. О концепции гарантированного управления устойчивым развитием арктической зоны на основе решения обратной задачи. Информационные технологии и системы: управление, экономика, транспорт, право. 2015. № 2 (16). С. 99-111.

6. Реестр ведущих научных и научно-педагогических школ Санкт-Петербурга. http://is.ifmo.ru/aboutus /2013 / science -schools.pdf

7. Goode H.H., Machol R.E. System Engineering: An Introduction to the Design of Large-Scale Systems. McGraw-Hill Book Co. New York, 1957. 551p

8. Большой энциклопедический словарь / Ред. А. М. Прохоров . – 2-е изд. – М. : Большая Российская энциклопедия, 2000 . – 1456 с.

9..Моисеев Н.Н. Математические задачи системного анализа. М.: Наука, 1981. -468 с.

10. M. D. Mesarovic, Yasuhiko Takahara, General Systems Theory: Mathematical Foundations. ACADEMIC PRESS New York, San Francisco, London 1975.

11. Burlov, V.G., Volkov, V.F. Method of consecutive expert estimates in control problems for the development of large-scale potentially dangerous systems / Engineering Simulation 12 (1) , pp.110

УДК 324

ПРИМЕНЕНИЕ ИННОВАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ВЫБОРОВ И РЕФЕРЕНДУМОВ

П.О.Захаров[1]

Территориальная избирательная комиссия (*ТИК*) №30, 191167*, Санкт-Петербург, Невский проспект, дом* 176

Приведен анализ применявшихся в России за последние годы избирательных систем и технологий. Выявлено их несовершенство, обусловившее возможности для фальсификаций, которые проиллюстрированы на основе результатов голосования по отдельным избирательным комиссиям Санкт-Петербурга. Показана эффективность использования инновационных систем и технологий при проведении президентских выборов 18 марта 2018 года. Даны предложения, направленные на дальнейшее повышение информационной безопасности при проведении выборов и референдумов.

Ключевые слова: выборы, голосование, избирательные комиссии, инновационные системы и технологии, QR-код, информационная безопасность**.**

APPLICATION OF INNOVATIVE SYSTEMS AND TECHNOLOGIES FOR INFORMATION SECURITY IN THE ELECTIONS AND REFERENDUMS

P.O. Zakharov

Territorial election Commission (*TEC*) *№* 30,191167*, Saint Petersburg, Nevsky prospect,* 176

The analysis applied in Russia in recent years, electoral systems and technologies. Revealed their imperfection, giving rise to opportunities for falsifications which are illustrated on the basis of the results of the voting on separate electoral commissions in St. Petersburg. Shows the efficiency of the use of innovative systems and technologies in the conduct of the presidential elections March 18, 2018 year. Given the proposals aimed at further enhancement of information security for the elections and referendums.

Keywords: elections, voting, election commissions, innovative systems and technologies, QR code, information security.

По действующему избирательному законодательству [1] проведение голосования в участковых избирательных комиссиях (УИК) возможно с применением автоматизированных систем и технологий. Для этого предназначены программно-технические комплексы обработки избирательных бюллетеней (КОИБ) и оборудование для электронного голосования [2]. С их помощью данные протокола УИК об итогах голосования могут передаваться в вышестоящую комиссию с использованием автоматизированной системы ГАС "Выборы".

При использовании КОИБ до передачи протокола УИК осуществляет распечатку протокола из КОИБ, оглашает и заносит уточненные данные в соответствующие строки увеличенной формы протокола об итогах голосования, а затем проводит проверку контрольных соотношений данных, внесенных в протокол об итогах голосования. Если соотношения не выполняются, УИК принимает решение о дополнительном подсчете по всем или по отдельным строкам протокола об итогах голосования, в том числе о дополнительном ручном подсчете бюллетеней. Если контрольные соотношения снова не выполняются, участковая комиссия принимает соответствующее решение, прилагаемое к протоколу об итогах голосования.

В случае совмещения дней голосования на выборах разных уровней использование технических средств подсчета голосов, комплексов для электронного голосования обязательно при подсчете голосов на выборах всех уровней. При этом решением Центральной избирательной комиссии РФ (ЦИК) может быть предусмотрено, что в пределах территории, на которой действует одна территориальная избирательная комиссия (ТИК), не менее чем на пяти процентах определяемых жребием избирательных участков, (но не менее чем на трех избирательных участках), на которых использовались такие технические

[1]*Захаров Петр Олегович – кандидат техническихъ наук, доцент, член УИК №* 2241 *с правом решающего голоса, тел.* +7 (812) 995-18-74,*e-mail: petr.z@bk.ru;*

средства, проводится контрольный подсчет голосов избирателей непосредственно членами УИК с правом решающего голоса (ручным подсчетом голосов).

Такая жеребьевка проводится вышестоящей комиссией в течение получаса после окончания времени голосования, а результаты жеребьевки доводятся до сведения каждой участковой комиссии незамедлительно. По итогам ручного подсчета голосов либо составляется новый протокол об итогах голосования, на котором делается отметка: "Повторный" и который вместе с первоначальным протоколом участковой комиссии об итогах голосования направляется в вышестоящую комиссию, либо составляется дополнительный акт о совпадении данных, полученных в ходе повторного подсчета голосов, с первоначальными данными.

Председатель участковой комиссии избирательного участка, определенного жребием для проведения контрольного (ручного) подсчета голосов, непосредственно после установления результатов контрольного (ручного) подсчета голосов информирует о полученных результатах вышестоящую комиссию. Она незамедлительно принимает соответствующее решение, в том числе решение о проведении ручного подсчета голосов на всех избирательных участках, на которых не проводился ручной подсчет голосов и которые расположены на соответствующей территории.

При проведении выборов в органы государственной власти и органы местного самоуправления данные протоколов участковых комиссий об итогах голосования в порядке, определяемом ЦИК, размещаются также в информационно-телекоммуникационной сети "Интернет".

Во всех случаях использования информационных систем и технологий для представления данных, содержащихся в протоколах комиссий об итогах голосования, о результатах выборов, в аппарат каждой избирательной комиссии субъекта Российской Федерации в качестве структурного подразделения вводится информационный центр. В его функции входят техническое и информационное обеспечение деятельности этой избирательной комиссии, автоматизация информационных процессов, реализуемых в ходе подготовки и проведения выборов, а также эксплуатация и развитие части ГАС "Выборы", функционирующей на территории данного субъекта Российской Федерации. Работники такого информационного центра организуют и осуществляют работы по эксплуатации и развитию ГАС "Выборы" на всей территории субъекта Российской Федерации, в том числе в территориальных комиссиях, а также в избирательных комиссиях муниципальных образований, на территориях которых сформировано более одной территориальной комиссии.

Если после ввода данных протокола участковой комиссии об итогах голосования в ГАС "Выборы" обнаружены допущенные при вводе технические ошибки, по мотивированному решению непосредственно вышестоящей комиссии в ГАС "Выборы" вводятся требующие корректировки данные.

Из-за указанных выше процедурных и технических сложностей в Санкт-Петербурге, как и в других российских регионах, при проведении выборов в органы власти такие автоматизированные технические средства пока применялись лишь ограниченно и в тестовом режиме. При этом была выявлена недостаточно высокая надежность используемого оборудования, в отдельных случаях приводящая к сбоям в работе.

Вместе с тем при проведении голосования после 2012 года начала использоваться система видеонаблюдения и трансляции изображения для дальнейшей передачи изображения на соответствующий сайт [3]. Она состоит из средств видеонаблюдения и трансляции изображения, устанавливаемых в помещениях для голосования, а также средств записи и хранения видеоинформации, средств обработки данных видеотрансляций, расположенных в региональных центрах обработки данных Министерства связи и массовых коммуникаций Российской Федерации.

При этом объектами видеонаблюдения служили:

- помещение для голосования в целом (камера видеонаблюдения № 1);
- места выдачи избирателям избирательных бюллетеней (при использовании комплексов для электронного голосования – места выдачи избирателям карточек со штрих-кодом для доступа к электронному голосованию) и работы со списком избирателей – камера видеонаблюдения №1;
- стационарные и переносные ящики для голосования, а также комплексы обработки избирательных бюллетеней, переносные устройства для электронного голосования в случае их использования – камера видеонаблюдения № 2;
- места подсчета и погашения неиспользованных бюллетеней, подсчета бюллетеней, извлеченных из ящиков для голосования (при использовании комплексов для электронного голосования – места погашения неиспользованных карточек со штрих-

кодом для доступа к электронному голосованию) – камера видеонаблюдения № 2;

- место проведения итогового заседания участковой избирательной комиссии, увеличенная форма протокола участковой комиссии – камера видеонаблюдения № 1 или № 2.

Таким образом, территориальные комиссии системами видеонаблюдения на предыдущих выборах не оборудовались. Поэтому до 2018 года результаты голосования определяли преимущественно путем подсчета бумажных избирательных бюллетеней вручную членами УИК с правом решающего голоса под контролем наблюдателей и камеры видеонаблюдения № 2, а председатели УИК оформляли протоколы результатов голосования и самостоятельно доставляли их в территориальные избирательные комиссии (ТИК). Там результаты голосования вводились в приемное устройство ГАС «Выборы» операторами вручную и практически бесконтрольно. При такой системе имелась возможность искажать в ТИКах конечные результаты голосований: председателями УИК – заново переоформляя протоколы, а операторами – вводя ошибочные данные.

Ниже проиллюстрированы выявленные автором настоящей статьи факты несоответствия данных из протоколов отдельных УИК официальным результатам, размещенным на сайте Санкт-Петербургской избирательной комиссии (Избиркома) по выборам в 2011 и 2016 годах депутатов Государственной Думы Федерального Собрания Российской Федерации (ГД) и депутатов Законодательного собрания Санкт-Петербурга (ЗАКС).

Как видно из рисунка 1, наиболее заметные расхождения наблюдаются у избирательных объединений, получивших наибольшее (в процентном измерении) количество голосов: политических партий СПРАВЕДЛИВАЯ РОССИЯ (СР), ЯБЛОКО, Коммунистическая партия Российской Федерации (КПРФ) и ЕДИНАЯ РОССИЯ (ЕР). При этом на сайте Избиркома у первых трех партий значения ниже, а у ЕР – существенно (более чем в 2 раза) выше величин, которые были зафиксированы в протоколах УИК. В меньшей степени несоответствие относится к Либерально-демократической партии России (ЛДПР) и практически не заметно для партий ПАТРИОТЫ РОССИИ (ПР) и ПРАВОЕ ДЕЛО (ПД). О достоверности запротоколированных результатов голосования при выборах в ЗАКС свидетельствует близость их величин по партиям к значениям, полученным при выборах в ГД. Это закономерно с учетом наличия одинаковых политических предпочтений у одних и тех же избирателей к представителям партий независимо от вида органов власти, формируемых путем выборов.

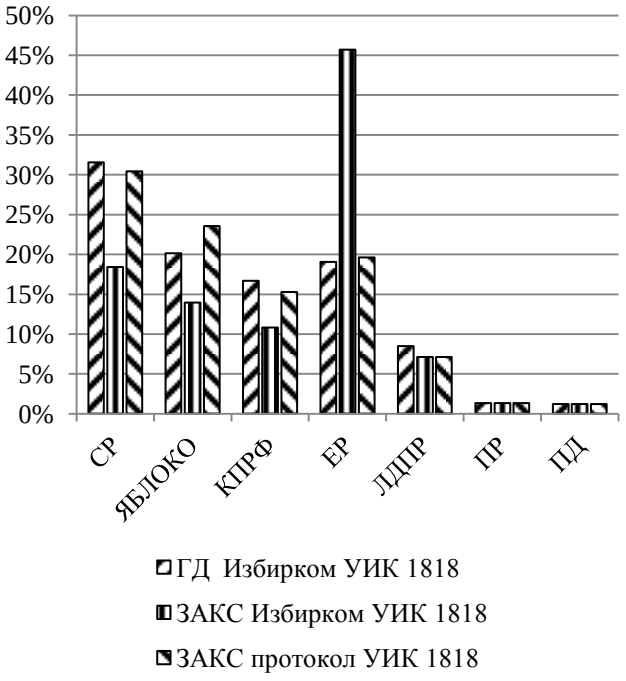


Рисунок 1 – **Результаты голосования 04 декабря 2011 года** на УИК 1818, входящей в ТИК территории №8 (по выборам в ЗАКС), и в ТИК №30, относившуюся к многомандатным избирательным округам территории Санкт-Петербург – Восточная (по выборам в ГД)

Из рисунка 2 видно, что общее количество избирателей, проголосовавших за ЕР на половине из числа участковых комиссий ТИК 30, согласно подписанным членами комиссии протоколам должно было составить 32,44% от числа принявших участие в выборах депутатов ЗАКС (линия из коротких штрихов). А по результатам, представленным в Горизбирком, эта величина равна 55,94% (линия из длинных штрихов), т.е. существенно выше.

Также сомнительны приведенные в таблице 1 аномальные значения некоторых других показателей с сайта Избиркома по официальным итогам выборов 04 декабря 2011 года по единому избирательному округу.

Согласно данным таблицы 1, при извлечении избирательных бюллетеней из стационарных ящиков на некоторых участках отсутствовали в сумме тысячи бюллетеней, выданных избирателям в помещениях для голосования, причем нигде не было зафиксировано ни одного утраченного бюллетеня. Опыт работы на избирательных участках показывает, что избиратели весьма редко уносят с собой полученные бюллетени.

Кроме того, в результатах голосования по большинству избирательных участков отсутствует разница между числом выданных и числом извлеченных бюллетеней. Поэтому такую разницу по отдельным участкам можно объяснить умышленным уничтожением на них бюллетеней за одних кандидатов для перераспределения количества голосов в пользу других кандидатов.

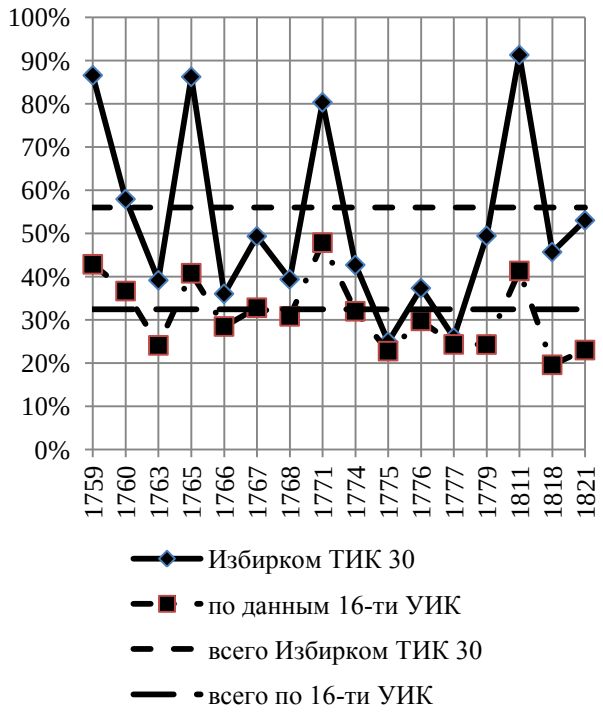


Рисунок 2 – **Результаты голосования 04 декабря 2011 года** по выборам в ЗАКС за ЕР по данным Избиркома и протоколам 16-ти из 32-х УИК, входящих в ТИК № 30.

Таблица 1 – **Показатели с сайта Избиркома** по официальным итогам выборов 04 декабря 2011 года по единому избирательному округу

Показатель	Выборы в ЗАКС	Выборы в ГД
	ТИК по территории № 8	по территории Санкт-Петербург-Восточная
Разница между числом бюллетеней, выданных избирателям в помещении для голосования и числом бюллетеней в стационарных ящиках для голосования	1686	4394 (ТИК № 16); 1526 (ТИК № 30)
Кол-во голосов, отданных за партию Единая Россия	91,28% (УИК 1811)	36,85% (УИК 1811)
	15,59% (УИК 1758)	16,50% (УИК 1758)

Некорректным показателем представляется и существенный разброс результатов голосования на разных избирательных участках. Например, как видно из таблицы 1, процент одновременно проголосовавших за партию Единая Россия на участке УИК № 1811 по выборам в ЗАКС составил 91,28%, а по выборам в ГД – 36,85%. Такое разительное отличие противоречит результатам вышепроведенного анализа, показавшего закономерную близость результатов голосования по выборам разных уровней власти на одном участке. Для сравнения, на участке УИК № 1758 эти показатели составляют соответственно 15,59% и 16,50%, то есть весьма близки друг другу и существенно ниже, чем на участке УИК № 1811.

Рисунок 3 – **Результаты голосования 18 сентября 2016 года** на выборах по партийным спискам в ГД и ЗАКС из протокола УИК-2241 и данных Избиркома по ТИК-30

Согласно гистограмме на рис. 3 результаты голосования 18 сентября 2016 года по выборам в ЗАКС, приведенные на сайте Избиркома на территории ТИК 30, существенно отличаются (по ЕР значительно выше, а по остальным партиям, за исключением ЛДПР, – ниже) от приведенных там же результатов по выборам в ГД. При этом, как и ранее по УИК 1818 (см. рисунок 1), на участке УИК 2241 итоги выборов в ГД по всем партиям отчетливо близки к итогам выбо-

ров в ЗАКС, что, как и в 2011 году, вполне закономерно.

Примечательно, что приведенные на рисунке 3 результаты голосования на участке УИК 2241 за партию Единая Россия по партийному списку в ГД существенно ниже и официальных данных в целом по России (соответственно 32% и 54%), но в ЗАКС – близки к официальным показателям по всему Санкт-Петербургу (соответственно 33% и 37%).

Обнаружено, что фальсификации осуществлялись и на выборах Президента РФ 04 марта 2012 года. Так, согласно протоколу УИК 1820 кандидат Прохоров М.Д. получил 266 голосов, а кандидат Путин В.В. – 501 голос избирателей. Однако на официальном сайте Горизбиркома размещены иные данные – соответственно, 166 и 601 голос.

По факту такого искажения результатов голосования членом УИК 1820 было своевременно заявлено председателям этой и территориальной комиссий, в Горизбирком и в Прокуратуру. Однако, вопреки постановлениям Прокуратуры о проведении расследований, дознаватели полиции восемь раз выносили свои постановления об отказе в проверке материалов и возбуждении уголовного дела. При этом жалобу на бездействие полиции Смольнинский районный суд и Санкт-Петербургский городской суд оставили без рассмотрения.

Осмысление фальсификаций результатов голосования и отсутствие возможности восстановления истинных итогов выборов вызвало потерю доверия со стороны населения РФ к избирательной системе. Это, с учетом также невозможности проголосовать для части избирателей, находящихся в день голосования вдали от своих избирательных участков, негативно отразилось на явке избирателей. Сравнение официальных данных показало, что за последние пять лет она существенно снизилась: если в 2011 году проголосовало более половины избирателей, то в 2016 году на выборы пришла лишь одна треть от граждан, обладающих активным избирательным правом.

Это обусловило необходимость использования при проведении выборов и референдумов современных информационных систем и технологий, позволяющих повысить защищенность результатов голосования от внешних воздействий и приблизить избирательный процесс непосредственно к избирателям. Международный опыт показывает, что наиболее перспективным является электронное голосование, при котором избиратель осуществляет свое волеизъявление через информационно-телекоммуникационную сеть «Интернет» из любого места своего нахождения.

В России интернет-системы получили развитие в связи с переходом с 2014 года к оказанию государственных и муниципальных услуг в электронной форме. Для этого Минкомсвязи РФ в рамках инфраструктуры электронного правительства создало Единую систему идентификации и аутентификации (ЕСИА) [4] с защитой пользователей путем оперативной регистрации их учетной записи на Едином портале государственных и муниципальных услуг (ЕПГУ). ЕСИА может обеспечить надежную защиту и избирательной системы с электронным голосованием. Например, в 2014 году на платформе интернет-ресурса «Российская общественная инициатива», также использующего ЕСИА, были избраны 43 члена Общественной Палаты РФ, за которых пользователями отдано 2 344 769 голосов [5].

Внедрение подобной инновационной избирательной системы позволило бы всем гражданам России реализовать свое активное избирательное право путем свободного волеизъявления с использованием компьютера, планшета или смартфона на любом избирательном участке, либо в удаленном доступе. В результате могли бы снизиться возможность фальсификации результатов голосования, повыситься явка избирателей и сократиться затраты на проведение выборов.

Следует отметить высокие темпы работ по устранению цифрового неравенства среди регионов России в условиях успешного развития передовых разработок отечественного программного обеспечения, а также стремительный рост популярности ЕПГУ. Количество его зарегистрированных пользователей, согласно сведениям Минкомсвязи РФ, за 2017 год увеличилось на 25 млн и составило 65 млн. человек. Однако оно пока составляет лишь немного более половины от общего числа обладателей активного избирательного права в России, что недостаточно для полного перехода на систему электронного голосования, как например в Эстонии.

Поэтому при проведении выборов Президента РФ 18 марта 2018 Россия для обеспечения информационной безопасности были ис-

пользованы современные инновационные технологии.

Во-первых, использование системы видеонаблюдения и трансляции изображения было предусмотрено не только для участковых, но и для территориальных комиссий. Это позволило контролировать процесс ввода данных из протоколов УИК в приемное устройство ГАС "Выборы".

Кроме того, в соответствии с Федеральным законом «О выборах Президента Российской Федерации» был разработан Порядок подачи заявления о включении избирателя в список избирателей по месту нахождения на выборах Президента Российской Федерации [6]. Он предоставил возможность любому избирателю, который будет находиться в день голосования вне места своего жительства, заранее подать заявление о включении его в список избирателей по месту нахождения в день голосования. Причем такое заявление в обусловленный Порядком срок избиратель вправе подать лично на бумажном носителе при предъявлении паспорта гражданина Российской Федерации на любой избирательный участок, либо через любой многофункциональный центр предоставления государственных и муниципальных услуг (МФЦ) или в электронном виде через ЕГПУ.

Для обработки информации о заявлениях была сформирована централизованная база данных ГАС "Выборы" (далее - база обработки заявлений). А в целях информирования избирателей о порядке и сроках подачи заявлений, а также о номерах избирательных участков, адресах и номерах телефонов, соответствующих участковых и территориальных избирательных комиссий (адресах помещений для голосования) ЦИК России организовал работу Информационно-справочного центра.

Известно, что регистрация и установление численности избирателей на территории муниципального образования, субъекта Российской Федерации, в Российской Федерации и за пределами территории Российской Федерации осуществляются по состоянию на 1 января и 1 июля каждого года с использованием специальной государственной системы регистрации (учета) избирателей. Она представляет собой комплекс мер по сбору, систематизации и использованию сведений об избирателях и обеспечивается комплексом средств автоматизации (КСА), призванных обеспечивать единый порядок учета избирателей.

Очевидно, что состав избирателей и сведения о них могут изменяться, например, в результате изменения места жительства, замены паспортов, смерти, призыва (поступления по контракту) на военную службу (увольнения с военной службы), содержания в местах лишения свободы по приговору суда, признания судом недееспособности. Поэтому соответствующие службы должны оперативно представлять возникающие уточнения в исполнительные органы власти для корректировки списков избирателей.

Важным условием информационной безопасности является создание эффективной системы передачи информации о заявлениях между избирательными комиссиями с целью включения избирателей, подавших заявления, в список избирателей по месту нахождения и исключения из списка избирателей по месту регистрации.

Вместе с тем предусмотрено, что не ранее чем за четыре дня до дня голосования (вторник) и не позднее 14 часов по местному времени в день, предшествующий дню голосования (суббота), избиратель может оформить в УИК избирательного участка, где он включен или имеет право быть включенным в список избирателей специальное заявление, при предъявлении которого в день голосования избиратель включается в список избирателей на указанном в специальном заявлении избирательном участке. При этом в целях защиты специального заявления от подделки используется специальный знак – марка строгой отчетности, имеющая единую нумерацию на всей территории Российской Федерации. Следует отметить, что такая технология специального заявления не является инновационной, так как она применялась и ранее в форме открепительного удостоверения. На выборах Президента РФ она предусмотрена лишь в ограниченном по времени масштабе.

Примененная на выборах технология подачи заявлений, позволила достаточно существенно повысить явку избирателей. Так, в Москве перед началом голосования было включено в списки 430162 избирателя и исключено 242109 избирателей [7]. Если учесть, что в Москве всего порядка 7 млн. избирателей, то можно предположить, что дополнительно около 10 процентов из них удалось осуществить свое волеизъявле-

ние, проголосовав по месту своего нахождения в день выборов.

Другой инновационной технологией на последних президентских выборов послужило использование впервые машиночитаемого QR-кода как на заявлениях о включении избирателя в список избирателей по месту нахождения, так и на протоколах УИК о результатах голосования. В первом случае это позволило защитить заявления от подделок, а во втором – исключить возможность фальсификации результатов голосования в территориальных комиссиях.

При этом исполнителем по оказанию услуг по организации видеонаблюдения за ходом выборов Президента РФ в марте 2018 года было назначено ПАО «Ростелеком». Оно организовало видеонаблюдение на более чем 43 тысячах УИК с периодом трансляции 51 час и на 2775 ТИК с максимальным периодом трансляции 72 часа [8]. Это обеспечило дополнительный контроль (по сравнению с предыдущими выборами) над деятельностью территориальных комиссий.

Таким образом, прошедшие 18 марта 2018 года выборы Президента РФ отличались использованием таких инновационных систем и технологий, как КОИБ либо электронное голосование, видеонаблюдение и трансляции изображения, а также возможность подачи заявления о включении избирателя в список избирателей по месту нахождения с использованием машиночитаемого QR-кода для этого заявления и для протокола о результатах голосования.

В дальнейшем для более надежной защиты избирательных прав граждан представляется перспективным разработка дистанционной информационно-коммуникационной системы на базе успешной отечественной разработки – портала «Госуслуги» Департамента развития электронного правительства Минкомсвязи РФ. Причем для защиты от несанкционированного вмешательства в проведение голосования может быть использована достаточно апробированная на практике Единая система идентификации и аутентификации.

Реализация такой инновационной системы позволит в значительной степени упростить избирательные процедуры, сэкономить бюджетные средства, повысить количество участников и получить достоверные результаты голосования. В результате будут созданы приоритетные условия для повышения информационной безопасности при проведении выборов и референдумов.

Литература

1. Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 N 67-ФЗ.

2. Постановление ЦИК России от 6 марта 2013 г. № 165/1212-6 «О порядке использования при голосовании на выборах в органы государственной власти субъектов Российской Федерации, органы местного самоуправления, референдумах технических средств подсчета голосов – комплексов обработки избирательных бюллетеней и комплексов для электронного голосования».

3. Постановление ЦИК России от 26.09.2012 N 142/1076-6 «О Порядке применения средств видеонаблюдения и трансляции изображения в помещениях для голосования на выборах и референдумах, проводимых в Российской Федерации».

3. Приказ Минкомсвязи России от 30.06.2014 № 179 «О вводе в эксплуатацию модернизированной версии Единой системы идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»

4. Указ Президента Российской Федерации от 04.03.2013 г. № 183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса "Российская общественная инициатива"

5. Формирование Общественной палаты Российской Федерации на 2014-2017 годы. [Электронный ресурс] – 18.03.2018. – http://2014.oprf.ru

6. Порядок подачи заявления о включении избирателя в список избирателей по месту нахождения на выборах Президента Российской Федерации. Утвержден постановлением Центральной избирательной комиссии Российской Федерации от 1 ноября 2017 г. N 108/900-7.

7. Эхо Москвы. [Электронный ресурс] – 18.03.2018. – https://echo.msk.ru/blog/aav/2167264-echo/

8. Петербургский дневник. [Электронный ресурс] – 18.03.2018. – https://www.spbdnevnik.ru/news/2018-03-18/rostelekom--zapustil-portal-dlya-videonablyudeniya-za-vyborami-prezidenta-rf/

УДК 336

КОНФЛИКТЫ МЕЖДУ ПАРТНЕРАМИ В БИЗНЕСЕ

Д.А. Забалуева[1], П.П. Дергаль[2]

Санкт-Петербургский государственный экономический университет (*СПбГЭУ*),
191023, *Санкт-Петербург*, *ул. Садовая*, 21

В статье изложены положительные и отрицательные стороны бизнес-партнерства; исследованы причины возникновения конфликтов между партнерами в бизнесе и дана им характеристика, а также раскрыты способы их разрешения.
Ключевые слова: бизнес, партнёры, конфликты, причины, способы разрешения.

CONFLICTS BETWEEN BUSINESS PARTNERS

D.A. Zabalueva, P.P. Dergal
St. Petersburg state economic university (*СПбГЭУ*),
191023, *St. Petersburg*, *Sadovaya St.*, 21

Abstract: the article describes the positive and negative aspects of business partnership; the causes of conflicts between business partners is investigated in the article, as well as the ways to solve them.
Keywords: business, partners, conflicts, reasons, ways of resolution.

Тема «Конфликты между партнерами в бизнесе» является актуальной и значимой, особенно для России, так как предпринимательство является достаточно молодой сферой деятельности.

Бизнес-партнерство имеет, как положительные, так и отрицательные стороны.

К положительным следует отнести:

1. Становление бизнеса, его развитие и процветание ложится на плечи нескольких человек – партнеров, – поэтому решение вопросов проще решать коллективно, нежели в одиночку.

2. В партнерстве, не только увеличивается творчество, но есть и свежие мысли, таланты и идеи, что повышает результативность бизнеса.

3. Партнерские взаимоотношения позволяют выиграть время, а, как известно, время – деньги.

4. Партнерские отношения позволяют увеличить стартовый капитал, что рождает массу идей с возможностью их воплощения и реализации.

5. Надежное плечо и помощь всегда рядом, когда у бизнесмена есть партнер.

6. Ответственность перед партнером дисциплинирует.

Отрицательные аспекты бизнес-партнерства:

1. Сложности взаимоотношений, особенно когда взгляды ведения дел у партнеров не совпадают. Подобные разногласия могут привести к дележке предпринимательства, а порой и вовсе к его распаду и банкротству.

2. Противоречия с партнером или партнерами могут оттягивать сроки решения важных задач и вопросов.

Исследуя конфликты в бизнес-партнёрстве, был сделан вывод о том, что их причинами являются:

1. Отсутствие четкой и согласованной стратегии создания и развития компании

Многие считают, что стратегия – прерогатива исключительно крупных компаний. Это одно из самых распространенных заблуждений. Поскольку многие start-up не уделяют данному вопросу должного внимания, то, даже став более крупной компанией, они продолжают плыть по течению. Как показывает практика, отсутствие четкой и согласованной стратегии развития компании не редко становится причиной конфликтов между собственниками, что зачастую приводит к ухудшению ее финансово-экономического состояния, а в некоторых случаях и к развалу компании.

2. Неоднородная структура начальных вложений в бизнес. Психология человека так устроена, что не многие из нас способны совладать с чувством зависти. Логически мы все понимаем,

[1]*Дарья Алексеевна Забалуева – магистрант СПбГЭУ, тел.*:+7 981 771 96 23*, e-mail: dashazab10@gmail.com,*
[2]*Пётр Петрович Дергаль – доцент кафедры Безопасность населения и территорий от чрезвычайных ситуаций, СПбГЭУ, тел.:* +7 911 210 53 92*, e-mail: dergal*1946*@mail.ru*

что тот, кто больше вложил в бизнес, и должен больше получать дивидендов, однако в том случае, когда бизнес-партнеры вносят в уставный капитал разные активы, вероятность возникновения в будущем конфликтов очень высока. [1]3.

Отсутствие четкой системы оплаты труда и распределения прибыли у владельцев бизнеса. Часто при создании нового бизнеса собственники выступают в двух ролях: владельцы и сотрудники компании. При этом они договариваются только о распределении прибыли в соответствии с начальными вложениями каждого, но никак не прорабатывают вопрос оплаты труда каждого из них. Кому-то из партнеров может показаться, что он работает и вносит гораздо больший вклад в развитие компании, чем другие, а значит он должен больше получать, что, как правило в последующем создаёт почву для конфликтов.

4. Профессиональные знания, навыки и эффективность владельцев бизнеса

Если владельцы компании понимают, что кто-то из них упёрся в потолок в саморазвитии и не хочет дальше самосовершенствоваться, то в таком случае это может стать причиной конфликтов между партнёрами в бизнесе. Особенно это характерно в том случае, когда партнёры выполняют определённые функции в оперативном управлении бизнесом,что может негативно сказаться на развитии компании и заработке всех бизнес-партнеров.

5. Отсутствие заранее проработанных сценариев выхода из бизнеса

Причин возникновения серьезных конфликтов между бизнес-партнерами может быть отсутствие договоренностей между ними о том, как они будут выходить из бизнеса, если кто-то захочет это сделать. Тот, кто захочет выйти из бизнеса, будет заинтересован в более высокой оценке, а его бизнес-партнеры наоборот в более низкой. При этом могут возникнуть конфликты, которые могут привести к тому, что контроль над бизнесом вообще может быть потерян или к тому, что все бизнес-партнеры потеряют на продаже своей компании. [2]

6. Внешние угрозы. Бывает, что возникшая внешняя угроза выводит наружу скрытые противоречия. Начинается поиск виноватых, который ведет к взаимным обвинениям и разладу между совладельцами. Каждый участник отстаивает собственную точку зрения по вопросу, как спасти предприятие, а это еще сильнее осложняет ситуацию.

7. Компаньоны не подходят друг другу по своим психологическим и морально- деловым качествам.

Результаты исследования причин приведены на диаграмме (рисунок 1).

Исследуя причины конфликтов, очень важно определить способы их предотвращения. Полностью исключить вероятность конфликтов получится вряд ли, однако снизить ее вполне возможно. Нам представляется, что такими способами могут быть:

Во-первых. При создании нового бизнеса с нуля необходимо заранее подготовиться к возможным конфликтам между бизнес-партнерами. Такой подход может позволить избежать существенных конфликтов либо минимизировать их негативное влияние на дальнейшее бизнес-партнерство и развитие компании.

Рисунок 1 – **Результаты исследования**

Нужно отдавать себе отчет в том, что начальный энтузиазм и некая эйфория от создания своего бизнеса со временем значительно уменьшаются. На первое место выходит трезвый расчет и максимально объективная оценка уже произошедших событий, а также планов по развитию компании. [3]

Думается, что лучше заранее до "боевых действий" проговорить, а еще лучше прописать все позиции по максимуму. Даже если все эти договоренности не будут соответствующим образом юридически оформлены, то это уже будет намного лучше по сравнению с тем вариантом, когда вообще ничего не прописано на бумаге.

Во-вторых. Необходим стратегический менеджмент, отсутствие которого не редко становится причиной конфликтов между собственниками, что зачастую приводит к ухудшению ее финансово-экономического состояния, а в некоторых случаях и к развалу компании.

Стратегический план – это вполне конкретный документ, а не просто какой-то набор мыслей в голове у собственников бизнеса. Причем это именно согласованный (между всеми совладельцами бизнеса) документ. [4]

Если будущие совладельцы компании разработали и согласовали стратегический план, то теперь необходимо определиться с уставным капиталом, поскольку и в этом может заключать-

ся причина существенных конфликтов между бизнес-партнерами в будущем.

В-третьих. Необходимо определиться с уставным капиталом, поскольку и в этом может заключаться причина существенных конфликтов между бизнес-партнерами в будущем.

Создание любого бизнеса требует начальных вложений. Начальные инвестиции для создания бизнеса могут быть не обязательно денежными. В уставный капитал помимо денег могут быть внесены и другие активы, причем как материальные (например, основные средства) так и нематериальные (нематериальные активы). Самый лучший вариант, когда все совладельцы бизнеса вносят в уставный капитал именно денежные средства, а не какие-либо другие активы. Идеальный вариант, когда все вносят в уставный капитал равные суммы денег в одинаковой валюте. В таком случае вероятность возникновения в будущем конфликтов между бизнес-партнерами минимальна. Это относится не только к уставному капиталу, но и к последующим возможным инвестициям учредителей.

Если есть возможность, то лучше всем бизнес-партнерам вкладывать в бизнес именно деньги, поскольку со временем у кого-то из них может измениться оценка начальных вложений, сделанных основными средствами или нематериальными активами. Появление таких мыслей у кого-то из совладельцев может спровоцировать его к тому, что он решит проститься со своими партнерами. Вероятность подобного случая становится значительно меньше, если в компании внедрен управленческий учет и система владельческого контроля.

В-четвёртых. Необходимо заранее проработать еще один очень важный вопрос – систему оплаты труда и распределения прибыли между владельцами бизнеса.

Для того, чтобы минимизировать вероятность возникновения такой проблемы нужно совладельцам бизнеса изначально договориться о системе оплаты. Труд всех бизнес-партнеров, которые будут принимать самое непосредственное участие в оперативной работе компании, должен оплачиваться. Даже если пока у компании прибыль отсутствует и в ней работают только бизнес-партнеры без наемных сотрудников, то и в этом случае сразу же должна действовать система оплаты труда. Очевидно, что в начале никаких выплат может и не быть, но это не значит, что не должна начисляться заработная плата тем, кто непосредственно работает в компании. Выплачиваться она может и потом, когда компания заработает прибыль и финансовый поток, необходимый для этих выплат. Если бы вместо бизнес-партнеров их функции выполняли наемные сотрудники, они же не делали бы это бесплатно. Так почему же владельцы, выполняя определенные оперативные функции в компании, не должны за это ничего получать? То, что они являются совладельцами бизнеса, не отменяет того, что они являются сотрудниками компании. Никто из сотрудников компании (в том числе и бизнес-партнеры) не должны работать бесплатно.

Итак, в самом начале нужно спроектировать организационно-функциональную структуру компании, которая, кстати, должна соответствовать ее стратегии, которую также следует разработать еще до создания компании. Для каждой должности нужно прописать функционал и определить систему оплаты труда, которая может состоять как из постоянной, так и из переменной части. Затем нужно распределить должности между бизнес-партнерами и в будущем начислять заработную плату каждому из них в соответствии с должностями. [5] В дополнение к оплате труда, которую будут получать бизнес-партнеры в качестве сотрудников, они естественно будут получать и свою долю прибыли, определяемую в соответствии с начальными вложениями в уставный капитал компании.

Следует отметить, что данная работа по распределению должностей между бизнес-партнерами покажет, смогут ли они договориться. Ведь у разных должностей может быть разный уровень оплаты труда и это является нормальным. Если в самом начале начнутся споры, в том числе потому, что кто-то из бизнес-партнеров в качестве сотрудника компании будет получать больше чем другие, то совместный бизнес лучше и не начинать.

Кто-то может возразить, сказав, что такой подход к организационному проектированию и определению уровня оплаты труда не подходит для стартапа, в отличие от уже действующей компании. Никто не утверждает, что в стартапе на каждую должность нужно брать отдельного человека. Безусловно, в начале, не будет большого объема работы. Это значит, что бизнес-партнеры в самом начале могут занимать (по факту, а не юридически) сразу несколько должностей и выполнять достаточно широкий функционал. То, что, что они будут занимать сразу несколько должностей, вовсе не означает, что суммарный уровень их оплаты труда будет очень большим, поскольку объем работы на каждой должности пока будет небольшим. Со временем по мере роста объема работ количество должностей, которые они занимают, будет сокращаться до тех пор, пока каждый из бизнес-партнеров не будет занимать только одну должность. Все остальные должности будут занимать наемные сотрудники.

Если кто-то из бизнес-партнеров вообще никак не будет участвовать в оперативной работе компании, то он и не должен получать никакой заработной платы. Он будет получать только свою долю от прибыли и все. В таком случае и не будет споров и взаимных упреков в том, что

кто-то работает больше, а получает как все остальные или даже меньше.

В-пятых. Важно, чтобы была достигнута договоренность о том, что преимущественное право выкупа доли совладельца компании имеют его бизнес-партнеры. Конечно же, даже такая договоренность не гарантирует полного отсутствия конфликтов, поскольку оценка бизнеса - неоднозначный процесс. При любых обстоятельствах лучше заранее прописать все возможные сценарии выхода из бизнеса, в том числе и полной продажи компании всеми бизнес-партнерами, что позволит в значительной мере устранить почву для конфликтов. [2]

В-шестых. Чтобы предотвратить конфликты, возникающие от внешних причин, еще при создании компании думается необходимо зафиксировать в договоре с партнером все возможные нюансы будущего сотрудничества. Предсказать, как человек поведет себя через несколько лет, сложно – а время летит быстро.

В-седьмых. Бывают и иные конфликты – на эмоциональном уровне. Их причина – в том, что компаньоны по-человечески не подходят друг другу. Думается, что при создании своего нужно выбирать такого партнера, который бы дополнял Вас. Кто-то силен в расчетах, кто-то прекрасный оратор, кто-то умеет работать с командой, кто-то хороший стратег и т. д. Там, где людям комфортно работать друг с другом, конфликта не будет. [6]

В-восьмых. Необходимо закрепить порядок разрешения конфликтов в акционерном соглашении. С лета 2009 года необходимость принятия этих документов закреплена законодательно. Большинство акционерных соглашений содержат разделы о предотвращении и разрешении конфликтных ситуаций. Значит, собственники допускают возможность того, что в будущем их отношения могут испортиться, а точки зрения по вопросам ведения бизнеса – разойтись. Решить подобные проблемы при отсутствии заранее одобренного компаньонами плана действий весьма непросто. Совсем другое дело, когда соглашение акционеров предусматривает особый порядок разрешения конфликтов, а также цивилизованного «развода» партнеров и справедливого раздела бизнеса.

Многие акционеры предпочитают указывать в соглашениях особый орган, разрешающий внутрикорпоративные споры. В этом качестве может выступать как отечественный третейский суд, так и иностранные судебные инстанции. В последнее время нередки условия о привлечении к разрешению подобных конфликтов профессиональных посредников (медиаторов).

В-девятых. Важно установить режим максимальной открытости во взаимоотношениях между партнерами. Закрепите в акционерном соглашении, что стороны обязуются раскрывать друг другу максимум информации о своих контактах, деятельности, связанной с бизнесом компании. Часто предусматривается преимущественное право участников соглашения на приобретение акций, принадлежащих другим участникам. В таком случае стороны специально оговаривают, что, если одному из акционеров поступит предложение от третьих лиц о приобретении у него всех или части акций, он обязан сообщить об этом другим акционерам, не скрывая существенных условий предложенной сделки. [7]

В-десятых. Как поступить, если возникла тупиковая ситуация (когда стороны не могут достичь согласия по какому-либо вопросу)?

Если на двух или более собраниях акционеров, созванных для решения таких вопросов, к единому мнению прийти не удается, любой из совладельцев вправе объявить ситуацию тупиковой и направить соответствующее письменное уведомление иным участникам соглашения. Порядок разрешения тупиковых ситуаций фиксируется в акционерном соглашении. Самый распространенный выход – «русская рулетка». Он заключается в том, что в течение определенного времени после того, как сложилась тупиковая ситуация, один или несколько акционеров направляют другому акционеру предложение о покупке его акций. При этом в соглашении указывается либо твердая цена за одну акцию, либо способ ее определения. У акционера, получившего предложение, есть два варианта: либо согласиться и продать свой пакет, либо направить встречное предложение – о покупке акций компаньона по такой же цене. Вне зависимости от выбранного варианта в компании останется только одна группа акционеров, и спор будет исчерпан.

Список использованной литературы

1. Конфликты между бизнес-партнерами. [Электронный ресурс]. URL: http://smart-venture.ru/conflicts_between_business-partners.html (дата обращения 22.11.2017 г.)
2. Александр Молотников. Деловой мир. Как решать конфликтные ситуации между совладельцами компаний. [Электронный ресурс]. URL: https://delovoymir.biz/kak_reshat_konfliktnye_situacii_mezhdu_sovladelcami_kompaniy.html (дата обращения 24.11.2017 г.)
3. Грин 48 законов власти. М., Рипол классик, 2002г.
4. Плещиц С.Г. Основы конфликтологии: Учебное пособие / СПб: Изд-во СПбГУЭФ, 2012.,229 с.
5. Фишер Р., Юрии У. Путь к согласию или переговоры без поражения. М., 1992.
6. Гришина Н.В. Психология конфликта, 3-е издание, учебное пособие для ВУЗов. Питер, 2015г.
7. Егидес А.П. Психология конфликта, учебное пособие, издательский дом «Синергия» МФПУ, 2013г.

УДК 004.056.53

ЗАДАЧИ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

В.С. Коломойцев[1]

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (*ИТМО*)/, 197101*, Кронверкский проспект, д.*49

В работе исследуются методы и средства обеспечения информационной безопасности информационной системы предприятия. Проанализировано влияние вариантов объединения различных средств защиты в систему и организации процессов обеспечения информационной безопасности на эффективность защиты и функционирования информационной системы в целом.

Ключевые слова: информационная безопасность, несанкционированный доступ, межсетевые экраны, сетевая организация, надежность.

OBJECTIVES AND MEANS OF ENSURING INFORMATION SYSTEMS SECURITY IN A DIGITAL ECONOMY

V. S. Kolomoitsev

St. Petersburg national research University of information technologies, mechanics and optics, 197101, *Kronverksky prospect*, 49

The paper investigates the methods and means of information security information system of the enterprise. The influence of the variants of combining different means of protection in the system and organization of information security processes on the effectiveness of the protection and operation of the information system as a whole is analyzed.

Keywords: information security, unauthorized access, firewalls, network organization, reliability.

Введение. Несанкционированный доступ (НСД), отказ узла в обслуживании, потеря информации, а также нарушение режима секретности на узле информационной экономической системы (ИЭС) может привести к значительным экономическим и иным потерям. Угроза атаки на вычислительные устройства системы может исходить как извне – посредством удаленных сетевых атак, так и изнутри подзащитной сети – за счет различных закладочных программных или аппаратных средств. Поэтому знание и понимание структуры защиты ИЭС, какие средства и меры обеспечения информационной безопасности (ИБ) можно применить и использовать для устранения угроз безопасности информации является одной из ключевых задач [1-4].

Стандартная структура соединения ИЭС с узлами внешней сети показана на Рисунке 1 и включает в себя три уровня:

- Уровень 1 (У-1) – в нем размещены оконечные узлы ИЭС (например, рабочие места пользователей системы или хранилища данных).

- Уровень 2 (У-2) – является уровнем организации сетевой архитектуры корпоративной сети.

- Уровень 3 (У-3) – включает в себя канал передачи данных (соединяющий ИЭС с внешней сетью).

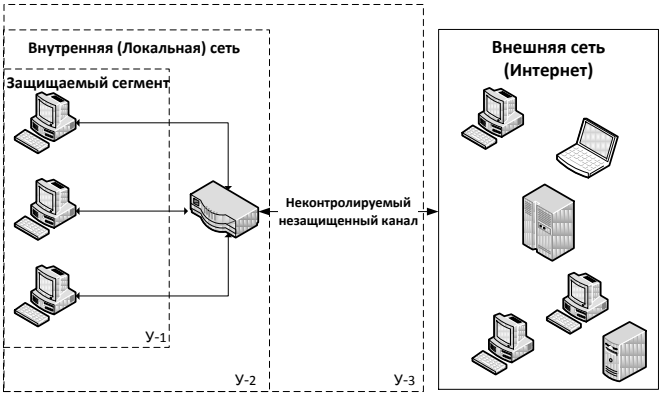


Рисунок 1 **– Структура соединения информационной экономической системы с узлами внешней сети**

В.С. Коломойцев – аспирант кафедры Вычислительной техники, ИТМО, тел.: +7 961 607 27 98, e-mail: dek-s-kornis@yandex.ru

На каждом из уровней ИЭС потенциальным нарушителем могут быть реализованы те или иные угрозы ИБ. Например, на У-3 возможны угрозы неправильной работы канала передачи информации. У-2 – подвержена угрозам отказа работы отдельных вычислительных устройств сети, их подмены или угрозам некорректной работы узлов (например, передача данных на завышенной скорости) в результате их повреждения или заражения. Угрозами в У-1 являются получение злоумышленником НСД к оконечным узлам и устройствам, заражение вычислительных устройств вирусами и иным вредоносным программным обеспечением (ПО), внедрение аппаратных и аппаратно-программных закладочных устройств, отказ оконечного вычислительного узла в обслуживании, уничтожение или подмена хранящихся на узле данных.

В результате, появляется необходимость в обеспечении комплексной ИБ ИЭС и, в частности, исследовании существующих методов борьбы с наиболее частыми угрозами ИБ.

Методы борьбы с угрозами безопасности на уровнях информационной экономической системы. Для ликвидации описанных выше угроз могут применяться следующие меры и средства:

- Шифрование трафика.

- Резервирование ключевых узлов и устройств системы.
- Использование межсетевых экранов (МЭ).
- Создание копий критически важной и ценной информации.
- Использование защищенного хранилища информации на узле.
- Использование средств обнаружения вторжения.
- Применение программных, аппаратных и программно-аппаратных средств защиты от НСД.
- Использование антивирусного программного средства на узлах.
- Соблюдение ключевых организационно-технических мер ИБ, при взаимодействии с системой.
- Проведение проверок и стресс-тестов программных, аппаратно-программных и аппаратных средств, применяемых в системе и своевременное их обновление.

Применение тех или иных из указанных выше средств и мер позволяет устранить или же существенно снизить вероятность возникающих угроз ИБ на каждом из уровней ИЭС. Так, для устранения угроз на Уровне 3, можно не только соблюдать ключевые организационно-технические меры безопасности (например, контроль за передаваемыми данными) и применение шифрования трафика в канале передачи данных, а также применять более специфичные способы защиты трафика передаваемого по сети, с использованием не только криптографических методов, но и методов стеганографии [5, 6]. Такие методы, например, целесообразно использовать в тех зонах взаимодействия ИЭС (или ее частей), где происходит передача информации высокого уровня конфиденциальности и, где задача обеспечения защиты информации (ЗИ) от перехвата и/или модификации является более приоритетной, чем скорость передачи информации по такому каналу связи.

На Уровне 2 помимо использования МЭ и/или средств предотвращения вторжений, резервирования ключевых элементов защиты системы и контроля их работоспособности, следует также проводить проверки и стресс-тесты всех использующихся средств ЗИ и, если требуется, своевременно их обновлять или заменять [7, 8]. Также необходимо серьезно отнестись к выбору схемы взаимного расположения сетевых элементов ИЭС между собой. Это позволит не только снизить потери в производительности или надежности всей системы в целом, но позволит снизить экономические затраты на создание и обеспечение ИЭС [5, 9].

Все большим набирающим популярность решением становится использование средств виртуализации для создания более гибких в плане производительности и надежности ИЭС [10-13]. Использование вычислительных мощностей виртуальных средств, зачастую физически расположенных даже не в одной локальной вычислительной сети, позволяет, например, снизить риск атак, направленных на отказ в обслуживании. Так как при осуществлении атаки клиент (организация) может с легкостью перераспределить вычислительные мощность с атакуемого узла (или сети, где он расположен) на уже совершенно другой и продолжить свою деятельность в штатном режиме. Само взаимодействие между вычислительными узлами осуществляется по защищенным каналам передачи информации [14]. Сложностью применения таких решений может стать то, что обрабатываемые данные могут нести конфиденциальный характер, а значит либо должны будут обрабатываться на тех узлах, где выполняются все необходимые требования к обеспечению их безопасности и секретности, либо обеспечить выполнение данных требований на всех задействованных в работе узлах. Это может принести к огромным экономическим затратам или быть физически невыполнимо, если виртуальные мощности предоставляются как услуга извне, т.е. проконтролировать выполнимость требований по ИБ практически невозможно.

В ИЭС может вестись работа с информацией различного уровня конфиденциальности или по обработке сведений составляющих государственную тайну. Поэтому может потребоваться следовать требованиям, предъявляемым к

таким ИЭС при их проектировании (элементы защиты какого класса безопасности необходимо использовать). Также необходимо знать к какому классу защищенности следует отнести данную ИЭС (или отдельные ее части) и каким образом можно включить данную ИЭС, в вычислительные системы (в том числе, экономические системы) большего уровня и масштаба [6, 7, 13]. Нередко при детальном рассмотрении вопроса проектирования ИЭС и понимании, какой элемент (или их группу) системы, где лучше всего расположить, можно получить такую схему ИЭС, в которой ее высокий уровень информационной защищенности достигается без существенных экономических затрат [15].

Для обеспечения ИБ на Уровне 1 желательным является использование на каждом оконечном узле антивирусного средства (со встроенным в него МЭ) и средства защиты от НСД (того или иного вида, в зависимости от инфраструктуры системы ЗИ). При работе на конкретном оконечном узле с информацией ограниченного доступа также необходимо иметь защищенное хранилище данных.

Как и на других уровнях ИЭС, на Уровне 1 следует соблюдать все ключевые организационно-технические меры безопасности, в особенности необходимо следить не только за правильной и надежной работой всех используемых устройств, путем их своевременного обновления и тестирования, но и также за тем, чтобы каждый из сотрудников организации правильно и точно исполнял свои обязанности и не наносил вред (в том числе неосознанно) ее работе.

Предлагаемые выше меры и средства позволяют повысить уровень ИБ и надежной работы ИЭС на всех уровнях ее структуры, а также обеспечить выполнение требований руководящих документов в области обеспечения ИБ и защиты персональных данных [16-18]. Рассмотрим более подробно, принцип работы некоторых (наиболее часто используемых) из показанных ранее аппаратно-программных средств обеспечения ИБ, с целью исследования их взаимного влияния и на проектирование системы ЗИ в целом.

Средства обеспечения информационной безопасности на различных уровнях информационной экономической системы. Каждый метод обеспечения информационной защищенности обладает характерными способами борьбы с угрозами ИБ и может быть использован в определенных местах ИЭС [5].

Межсетевые экраны. Одним из основных элементов обеспечения ИБ сетей и ИЭС являются МЭ. В зависимости от выбранного типа МЭ (или их набора) становится возможным решить задачи защиты курсирующей по сети информации, разграничении доступа по сети и защиты оконечных узлов сети от угроз извне.

В зависимости от типа МЭ применяемого в ИЭС, влияние МЭ на различные ее аспекты (безопасность, производительность, надежность и т.д.) может разниться от несущественного до критически влияющего на процесс работы с сетью.

В настоящее время выделяют три основных типа МЭ, в зависимости от уровней сетевой модели OSI [6], на которых они осуществляют свою работу и, соответственно, их возможностей по обеспечению сетевой безопасности:

1. МЭ с фильтрацией пакетов (МЭ-Ф). МЭ-Ф располагаются на сетевом уровне сетевой модели OSI и предназначены для фильтрации пакетов, поступающих в корпоративную сеть, на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором. Такие МЭ практически не оказывают влияние на производительность ИЭС и способны бороться с поврежденными пакетами и спамом, поступающим в корпоративную сеть, тем самым снижая риск атак, направленных на отказ в обслуживании. Однако у МЭ-Ф имеется уязвимость механизма защиты для различных видов сетевых атак, таких как подделка исходных адресов пакетов, несанкционированное изменение содержимого пакетов и т.д.

2. МЭ с адаптивной проверкой пакетов (МЭ-А). В сравнении с МЭ-Ф, МЭ данного типа, способны более «глубоко» бороться с угрозами ИБ в канале передачи данных. «Глубина» работы данного типа МЭ, зависит от возможностей конкретной используемой модели МЭ и точности установленных настроек. Однако МЭ-А, в сравнении с МЭ-Ф, имеют высокую стоимость, возможную сложность настройки и слежения за правильностью установленных параметров, а также (в зависимости от «глубины проверки» пакетов) могут снижать производительности сети.

3. МЭ прикладного уровня (МЭ-П). МЭ-П, как и МЭ-А, способны анализировать содержимое пакетов. Ключевой стороной данного типа МЭ является то, что их можно установить на любой оконечный узел и, в зависимости от имеющихся вычислительных мощностей устройства и настроек МЭ, он будет способен обеспечивать защиту оконечного узла или же всей сети в целом на требуемом от него уровне. Однако применение МЭ-П – может вызвать снижение производительности (в данном случае, узла системы), в зависимости от «глубины проверки» пакетов.

С целью повышения скорости работы и увеличения степени отказоустойчивости каждого из ранее указанных типов МЭ, ведутся исследования по оптимизации работы с базой правил (в

том числе методе хранения в ней самих правил). Представляет интерес применения автокоррекции баз правил фильтрации в средствах межсетевого экранирования. Метод автокоррекции, позволяет "переносить" наиболее часто используемые правила в начало списка, тем самым уменьшая время на их поиск и выполнение. Это способствует тому, что злоумышленник уже не может воспользоваться методом атаки, заключающейся в частом использовании правил находящихся в конце списка, что позволяло ему с меньшими вычислительными мощностями выводить узел из строя (осуществлять его отказ в обслуживании).

Для создания комплексной системы обеспечения сетевой безопасности, требуется использовать МЭ каждого типа в наиболее подходящих для них условиях (в местах, где их положительные стороны будут иметь наибольший эффект) [8, 14, 20] . Так, желательно на входе в корпоративную сеть и большие участки вычислительной сети организации, устанавливать МЭ-Ф для предотвращения попадания в сеть спама и однотипно-сформированных пакетов от неизвестных источников из внешней сети (узлов). После чего, при попадании пакетов уже в саму корпоративную сеть (или ее подсеть), пакеты должны анализироваться более подробно и тщательно. Тем самым, требуется применять МЭ-А для «глубокого» анализа пакетов по тем правилам, которые необходимы в данной конкретной подсети. После того как пакет будет проанализирован и допущен для дальнейшей движения внутри сети, его может проанализировать МЭ-П на отдельные (частные) угрозы (которым наиболее подвергнуты узлы в данной подсети) или же сразу отправлен на оконечный узел, на котором также имеется МЭ-П, но уже предназначенный (настроенный) для обеспечения ИБ строго данного узла. Для обеспечения надежности и отказоустойчивости МЭ должны резервироваться при консолидации их ресурсов в кластеры с учетом балансировки их нагрузки при динамическом распределении запросов [19-21].

Средства защиты от НСД. Под средствами защиты от НСД подразумевают программные, аппаратно-программные и аппаратные средства ЗИ, позволяющие исключить возможность доступа злоумышленников или инсайдеров к несанкционированному получению возможности управления узлом, а также получения доступа к персональным данным, коммерческой тайне или другой конфиденциальной информации [6, 12].

В соответствии с действующими руководящими документами Государственной технической комиссии технические средства, реализующие функции защиты от НСД можно разделить на: встроенные и внешние.

К встроенным средствам относятся средства парольной защиты BIOS, операционной системы и средств управления базами данных. Внешние средства призваны подменить встроенные средства с целью усиления защиты, либо дополнить их недостающими функциями. К внешним средствам можно отнести: аппаратные средства доверенной загрузки; аппаратно-программные комплексы разделения полномочий пользователей на доступ; средства усиленной аутентификации сетевых соединений.

Аппаратные средства доверенной загрузки представляют собой устройства, иногда называемыми "электронным замком", чьи функции заключаются в надежной идентификации пользователя, а также в проверке целостности ПО компьютера. Обычно, они представлены в виде платы расширения персонального компьютера, с необходимым программным обеспечением, которое записано в память самой платы или же на жесткий диск компьютера. В процессе загрузки стартует BIOS и плата защиты от НСД, при этом запрашивается идентификатор пользователя и сравнивается с тем, что хранится в памяти карты. Затем стартует встроенная операционная система платы или компьютера, после чего запускается программа проверки целостности программного обеспечения. Как правило, проверяются системные области загрузочного диска, загрузочные файлы и файлы, задаваемые самим пользователем для проверки.

Результат проверки сравнивается с хранимыми данными в памяти карты. В случае, когда при проверке идентификатора или целостности системы выявляются различия с теми данными, что хранятся в памяти карты, то плата заблокирует дальнейшую работу, и выдаст соответствующее сообщение на экран. Если проверки дали положительный результат, то плата передает управление персональному компьютеру для дальнейшей загрузки операционной системы.

Все процессы идентификации и проверки целостности фиксируются в журнале. Достоинства устройств данного класса – их высокая надежность, простота и невысокая цена.

Примерами таких средств являются: USB-идентификаторы Rutoken; смарт-карты и usb-ключи eToken; электронный замок ПАК Соболь; ПАК "Росомаха"; идентификатор iButton.

Аппаратно-программные комплексы разделения полномочий на доступ используются в случае работы нескольких пользователей на одном компьютере, если встает задача разделения их полномочий на доступ к данным друг друга. Решение данной задачи основано на: запрете пользователям запусков определенных приложений и процессов; разрешении пользователям и запускаемым ими приложениям лишь определенного типа действия с данными.

Реализация запретов и разрешений достигается различными способами. Как правило, в процессе старта операционной системы запускается и программа защиты от НСД. Она присутствует в памяти компьютера, как резидентный модуль и контролирует действия пользователей на запуск приложений и обращения к данным. Все действия пользователей фиксируются в журнале, который доступен только администратору безопасности. Данные системы можно использовать и в однопользовательской системе для ограничения пользователя по установке и запуску программ, которые ему не нужны в работе.

Методы работы таких комплексов для реализации разграничительной политики доступа к ресурсам при ЗИ ограниченного доступа чаще всего основываются на мандатном (назначение меток конфиденциальности) или дискреционном (настройки списка возможных действий с каждым отдельным ресурсом системы) управлении доступом. Однако, в виду того, что каждый из данных методов имеет свои недостатки, то ведутся исследования направленные на решение тех или иных проблем в каждом из этих методов управления доступом.

Примерами таких комплексов могут стать: Dallas Lock; Secret Net; система ЗИ от НСД "Аура"; система ЗИ от НСД Блокпост; система ЗИ от НСД Щит-РЖД; система ЗИ Crypton Lock.

Существуют более специфичные методы защиты от НСД. Например, разграничение доступа к информации на основе скрытого мониторинга пользователей ИЭС. Данный метод предполагает постоянный скрытый мониторинг за действиями каждого пользователя ИЭС, анализируя действия интересующего ее пользователя, сохраняя себе в память данные о том, как он работает с интерфейсами программ, клавиатурой (частота нажатий на клавиши), мышкой и т.д. и, в дальнейшем, сопоставляя их с поступающими в реальном времени данными. В виду того, что сценарий поведения каждого отдельного пользователя может меняться с течением времени, то такая система защиты от НСД требует обновления данных (в заданный период времени) обо всех пользователях, которые в ней зарегистрированы. Однако вероятность ложного срабатывания у таких систем до сих пор остается высокой.

Эффективность системы защиты информации. Оценка степени защищенности ИЭС является трудоемкой и сложной задачей. Так, в процессе исследования защищенности ИЭС требуется оценить: сложность реализации той или иной угрозы информационной безопасности для потенциального нарушителя; готовность злоумышленника к реализации угрозы информационной безопасности соответствующей сложности; экономической целесообразности и эффективности применяемых проектных решений; влияние угроз ИБ на эксплуатационные характеристики системы ЗИ. На сегодняшний день ведутся множество исследований в вопросе выбора наиболее точного и полноценного метода оценки информационной защищенности и того, какой из них является более объективным [11-13].

Распространенным методом до сих пор остается метод экспертных оценок, заключающийся в том, что группа экспертов (специалистов в области ИБ) тем или иным способом (чаще в ходе опроса) решают насколько защищенной является исследуемая система в целом или ее отдельные элементы. По причине того, что опрашиваемые эксперты могут обладать различным уровнем знаний, опыта (в том числе работы с конкретными аппаратными или программными элементами ЗИ) и ответственности, то и уровень доверия к оценкам каждого из них также должен быть разным. Например, предлагается, чтобы каждый эксперт, оценивая средство (систему) обнаружения сначала делает оценку уровня своей информированности по данному средству на качественном уровне с градациями: 1 – система незнакома; 2 – имею представление о данной системе; 3 – участвовал в эксплуатации данной системы. Также каждый эксперт дает оценку вероятности правильности суждений экспертов по каждой категории: 1 – специалист в области технических средств ЗИ не знакомый с оцениваемой системой; 2 – специалист в области технических средств ЗИ, имеющий представление об оцениваемой системе; 3 – специалист в области технических средств ЗИ участвующий в эксплуатации, данной системы. На основе выявленных суждений вычисляется среднеарифметическая оценка весового коэффициента для каждого эксперта по каждому оцениваемому средству (системе) технической защиты.

Возможен выборочный метод оценки уровня защищенности ИЭС, основываясь на имеющихся требованиях по ЗИ от НСД [11]. Данный метод предполагает применение выборочного контроля для оценки соответствия ИЭС требуемому классу защищенности. Иными словами, за полноценно информационно защищенную ИЭС берется та, у которой наличие и работоспособность всех требуемых элементов ЗИ (в соответствии с классом, к которому она принадлежит) было проверено, а менее защищенную – та система, у которой либо части элементов защиты нет, либо проверено наличие не каждого из элементов. Каждый элемент ЗИ имеет свою цену (которая определяется экспертной оценкой) и, тем самым, их полное наличие в соответствии с предъявляемыми требованиями дает 100% защищенность системы.

Для получения количественных оценок показателей безопасности необходимо решать задачи математического моделирования [7, 13].

Заключение. В работе исследованы основные методы обеспечения комплексной ин-

формационной безопасности вычислительной системы.

Показано, что только комплексное использование взаимодополняющего набора средств и методов защиты делает возможным создать полноценную информационно защищенную вычислительную систему, ориентированную на решение задач цифровой экономики. Показана необходимость оценки защищенности систем с целью выявления средств и мер достижения наибольшего уровня защищенности при меньших финансовых затратах на создание системы.

Литература

1. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности // Геополитика и безопасность. 2014. № 1 (25). С. 69-77
2. Верзун Н.А., Колбанев М.О., Татарникова Т.М. Технологическая платформа четвертой промышленной революции // Геополитика и безопасность. 2016. № 2 (34). С. 73-77
3. Верзун Н.А., Колбанёв М.О., Татарникова Т.М. Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности Санкт-Петербург, 2016. С. 52-56
4. Колбанёв М.О., Коршунов И.Л., Левкин И.М., Микадзе С.Ю. К вопросу об информационно-экономической безопасности общества // Геополитика и безопасность. 2015. № 3 (31). С. 87-91.
5. Kolomoitcev V.S., Bogatyrev V.A. The fault-tolerant structure of multilevel secure access to the resources of the public network // Communications in Computer and Information Science - 2016, Vol. 678, pp. 302-313
6. Соколов Р.В., Андреевский И.Л. Проектирование и эксплуатация информационных систем // Санкт-Петербург, 2017
7. Bogatyrev V.A., Vinokurova M.S. Control and Safety of Operation of Duplicated Computer Systems // Communications in Computer and Information Science - 2017, Vol. 700, pp. 331-342
8. Богатырев В.А., Богатырев С.В. Надежность мультикластерных систем с перераспределением потоков запросов // Известия высших учебных заведений. Приборостроение - 2017. - Т. 60. - № 2. - С. 171-177
9. Коршунов И.Л., Пуха Г.П. Концепция построения защищенного комплекса для формирования и распределения нагрузки вуза // Информационная безопасность регионов России (ИБРР-2015) Материалы конференции. 2015. С. 219-220
10. Пуха Г.П., Драчёв Р.В., Попцова Н.А. Информационно-логическая модель базы данных для системы интеллектуальной поддержки принятия решений. Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 117-124
11. Емельянов А.А., Коршунов И.Л. Оценка затрат на системы информационно- экономической безопасности // Технологии информационно-экономической безопасности Санкт-Петербург, 2016. С. 63-69.
12. Татарникова Т.М. Задача синтеза комплексной системы защиты информации в ГИС // Ученые записки Российского государственного гидрометеорологического университета. 2013. № 30. С. 204-211.
13. Коломойцев В.С., Богатырев В.А. Вероятностно-временные показатели при поэтапном применении средств защиты информации // Вестник компьютерных и информационных технологий -2017. - № 11(161). - С. 37-43
14. Максимцев И.А., Колбанев М.О., Коршунов И.Л., Левкин И.М., Микадзе С.Ю. О технологических основаниях новой доктрины информационной безопасности российской федерации // Новые горизонты глобального мира. Санкт-Петербург, 2015. С. 270-281
15. Богатырев В.А., Богатырев С.В. Своевременность обслуживания в многоуровневых кластерных системах с поэтапным уничтожением просроченных запросов // Вестник компьютерных и информационных технологий - 2018. - № 2. - С. 28-35
16. Богатырев В.А., Кармановский Н.С., Попцова Н.А., Паршутина С.А., Богатырев С.В. Имитационная модель поддержки проектирования инфокоммуникационных резервированных систем // Научно-технический вестник информационных технологий, механики и оптики -2016. - Т. 16. - № 5(105). - С. 831-838
17. Bogatyrev V.A., Parshutina S.A. Redundant Distribution of Requests Through the Network by Transferring Them Over Multiple Paths//Communications in Computer and Information Science, IET - 2016, Vol. 601, pp. 199-207
18. Гатчин Ю.А., Жаринов И.О., Коробейников А.Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2 (78). С. 92-95
19. Богатырев В.А., Богатырев С.В. Многоэтапное обслуживание запросов, критичных к задержкам ожидания, в многоуровневых системах // Научно-технический вестник информационных технологий, механики и оптики -2017. - Т. 17. - № 5(111). - С. 872–878
20. Богатырев В.А., Богатырев С.В. Резервированное обслуживание в кластерах с уничтожением неактуальных запросов // Вестник компьютерных и информационных технологий - 2017. - № 1(151). - С. 21-28
21. Богатырев В.А., Паршутина С.А. Модели многопутевой отказоустойчивой маршрутизации при распределении запросов через сеть // Вестник компьютерных и информационных технологий - 2015. - № 12. - С. 23-28

УДК 004.02

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ОЦЕНКИ ПОКАЗАТЕЛЕЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАДАЧЕ ОЦЕНКИ НАДЕЖНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ

А.В.Струков[1], Н.А. Хоферихтер[2]

[1]*АО "Специализированная инжиниринговая компания севзапмонтажавтоматика"* (*СПИК СЗМА*),
199106, *г. Санкт-Петербург,* 26-*я линия В.О., д.*15*, корп.* 2*, лит. А, Бизнес центр «Биржа»;*
[2]*Международный банковский институт (МБИ), Санкт-Петербург,*
191023, *Санкт-Петербург, Невский пр*., 60

В статье рассматриваются подходы к оценке надежности автоматизированных систем управления (АСУ) с учетом надежности средств защиты информации (СЗИ). Подход учитывает надежность аппаратных средств как самой АСУ, так и СЗИ. В качестве показателя надежности средств защиты с точки зрения реализации их основных функций рассматриваются показатели функциональной безопасности.

Ключевые слова: надежность, вероятность отказа на запрос, схема функциональной целостности

SOFTWARE IMPLEMENTATION OF ALGORITHM FOR PERFORMANCE ASSESSMENT OF FUNCTIONAL SAFETY MEANS PROTECTION OF INFORMATION IN ASSESSING THE RELIABILITY OF TECHNICAL SYSTEMS

A.V. Strukov, N. A. Hoferichter

JSC "Specialized engineering company SZMA,
199106, *St. Petersburg*, 26*th line V. O.*, 15, *korp.* 2*, lit. A, business center "Exchange»;*
International banking Institute (IBI), Saint Petersburg, 191023, *St. Petersburg, Nevsky prospect*, 60

The article discusses approaches to assessing the reliability of automated control systems (ACS), taking into account the reliability of information security. The approach takes into account the reliability of the hardware as the ACS and szi. Functional safety indicators are considered as an indicator of safety equipment reliability from the point of view of realisation of their main functions.

Keywords: reliability, probability of failure on demand, scheme of functional integrity

Рассмотрим некоторую сложную техническую систему (СТС), важность выполнения задач которой позволяет отнести этот объект к объектам критической информационной инфраструктуры (КИИ). Согласно Федеральному закону №187-ФЗ [1] к таким объектам относятся информационные системы, информационно-телекоммутационные системы, автоматизированные системы управления, функционирующие в одной из следующих сфер: здравоохранение, наука, транспорт, связь, банковская сфера и иные сферы финансового рынка, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности, топливно-энергетический комплекс, в том числе атомная энергетика.

Реализация мероприятий по обеспечению информационной безопасности объектов КИИ, в частности АСУ, предполагает, в том числе, и использование программно-аппаратурных средств защиты информации. При этом следует говорить о комплексе средств, способных не только контролировать информацию, выявлять атаки и вредоносные программы, но и контролировать работу и целостность всех средств системы. Например, компания InfoWatch [2] предлагает к внедрению комплекс СЗИ, состоящий из 6 базовых модулей – четырех основных и двух вспомогательных. Среди них – модуль межсетевого экранирования и модуль обнаружения и предупреждения вторжений, которые предполагает подключение вразрез.

СЗИ имеют различные типовые схемы применения, которые выбираются по требованию заказчика с учетом особенностей конкретного объекта.

[1]*А.В.Струков – кандидат технических наук, доцент, ведущий специалист исследовательского отдела АО «СПИК СЗМА», тел.:* +79214021905*. e-mail: Alexander_Strukov@szma.com;*
[2]*Н.А. Хоферихтер – кандидат экономических наук, доцент кафедры международной экономики и менеджмента МБИ, тел.:* +79112509723*, e-mail: n-meiner@bk.ru*

В общем случае по аналогии с анализом надежности средств противоаварийной защиты (ПАЗ) будем рассматривать влияние средств защиты на надежность объекта защиты (объекта управления – ОУ) в двух его проявлениях:

- физическое, связанное с безотказностью СЗИ, которые могут иметь подключение вразрез;
- функциональное, связанное с выполнением функций безопасности, которое будем называть функциональной безопасностью.

Функциональная безопасность – это часть общей безопасности, обусловленная применением объекта управления (ОУ) и АСУ ОУ, зависящая от правильности функционирования средств защиты и других средств по снижению риска [3]. ОУ – оборудование, машины, аппараты или установки, используемые для производства, обработки, транспортирования, в медицине или в других процессах. Для ОУ безопасное состояние – это состояние, в котором достигается безопасность именно ОУ.

Система, связанная с безопасностью, реализует функции безопасности, требующиеся для достижения и поддержки безопасного состояния ОУ, и предназначена для достижения своими средствами или в сочетании с другими средствами снижения риска необходимого уровня безопасности для требуемых функций безопасности.

Функция безопасности реализуется в СЗИ и предназначается для достижения или поддержания безопасного состояния ОУ по отношению к конкретному опасному событию:

В общем случае инструментальные аппаратно-программные СЗИ, как приборные системы безопасности, состоят из трех подсистем:

- подсистемы обнаружения опасности (сенсорные подсистемы или подсистемы датчиков);
- подсистемы принятия решения на основе анализа сигналов, полученных от датчиков и сенсоров, и формирования запроса к подсистеме исполнительного управляющего воздействия для нейтрализации опасности;
- подсистема исполнительных (конечных) элементов, которые реализуют сигналы управляющего воздействия.

Каждая подсистема может обладать избыточностью (структурной, временной, функциональной и т.д.). Например, подсистема принятия решения может иметь мажоритарную структуры (структуру голосования) для корректной обработки информации в условиях неопределенности.

Зачастую СЗИ работают как пассивные системы наблюдения, ожидая запроса на некоторый сигнал опасности – угрозы. Учитывая конечную надежность инструментальных (приборных) средств, необходимо осуществлять контроль их состояния.

Особое внимание уделяется опасным отказам, то есть таким отказам, которые могут перевести СЗИ в опасное для объекта защиты состояние.

Отказ СЗИ может быть обнаружен либо средствами самодиагностики без прерывания функций безопасности, либо в режиме контрольной проверки с прерыванием выполнения функций безопасности СЗИ.

При диагностических проверках могут быть найдены опасные обнаруженные отказы (DD). Если такой отказ обнаружен, то СЗИ переходит в режим восстановления, и на это время применяются дополнительные меры по обеспечению безопасности.

Этот процесс характеризуется двумя основными показателями – интенсивностью опасных обнаруженных отказов λ_{DD}, и средним временем восстановления MTTR.

Опасные отказы, обнаруженные при контрольных проверках, называются опасными необнаруженными отказами (DU). Можно предположить, что при проведении контрольной проверки обнаруживаются и устраняются все скрытые отказы СЗИ.

Этот процесс характеризуется тремя основными показателями – интенсивностью опасных необнаруженных отказов λ_{DU}, средним временем ремонта MRT и интервалом между контрольными проверками T_1.

Рассмотрим три типичных вида функционирования СЗИ.

1. В межконтрольном периоде не было опасных отказов, запросы на формирование функций безопасности не было, СЗИ работоспособны ($X(t)$=1), контрольная проверка проведена на интервале $\{T_1,\ T_1+MRT\}$, СХИ после проверки возобновили работу. Условный график состояний СЗИ для этого режима представлен на рис.1.

2. В межконтрольном периоде произошел опасный обнаруженный отказ (DD), СЗИ переходят в состояния $X(t)$=0 и не способны выполнять функции безопасности (рис.2). После проведения восстановительных работ длительностью MTTR СЗИ переходит в работоспособное состояние до наступления времени контрольной проверки T_1.

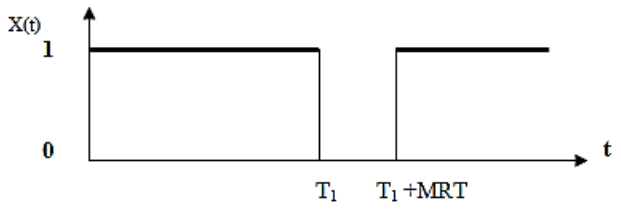


Рисунок 1 – **График состояний СЗИ при отсутствии запросов**

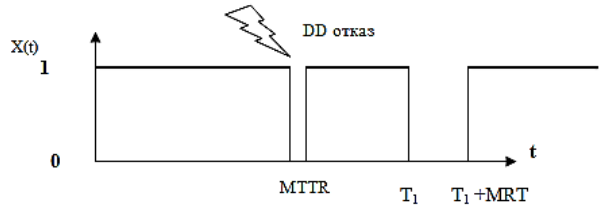


Рисунок 2 – **График состояний СЗИ при наличии обнаруженного отказа**

3. В межконтрольном периоде произошел опасный необнаруженный отказ (DU). СЗИ находятся в состоянии скрытого отказа и в случае прихода запроса не могут выполнять функции безопасности в течение интервала времени D_1 (рис.3).

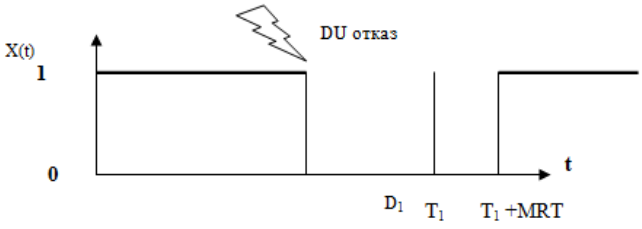


Рисунок 3 – **График состояний СЗИ при наличии необнаруженного отказа**

Основной характеристикой СЗИ является вероятность неготовности к выполнению функции безопасности – *PFD*.

При периодических контрольных проверках *PFD* как функция времени имеет вид, показанный на рис.4.

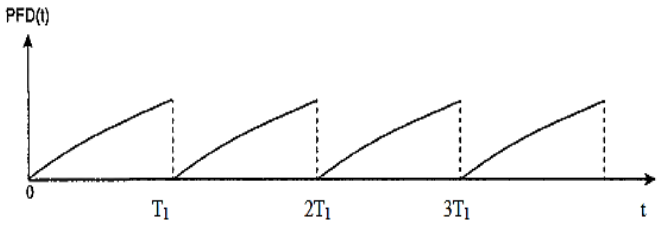


Рисунок 4 – **График изменения вероятности отказа на запрос (PFD)**

В этом случае среднее значение *PFD(t)* можно посчитать на первом интервале $(0,T_1)$:

$$PFDavg = \frac{1}{T_1}\int_0^{T_1} PFD(t)dt\,. \qquad (1)$$

Графическая иллюстрация соотношения значений *PFD(t)* и *PFDavg* приведена на рис.5.

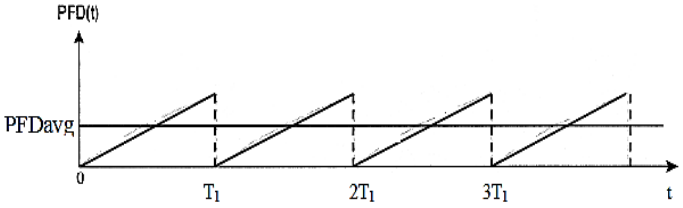


Рисунок 5 – **График изменения функции *PFD(t)* и значения *PFDavg***

В общем случае эта задача решается на основе анализа марковских процессов. При некоторых допущениях возможно использование более простых формул [4].

Обычно рассматривают два основных режима работы СЗИ – с низкой частотой запросов к исполнительным элементам (не чаще одного раза в год) и с высокой (непрерывной) – чаще одного раза в год вплоть до режима работы с непрерывным запросом. В первом случае корректно говорить о средней вероятности отказа на запрос *PFD*, во втором – о средней частоте отказов на запрос *PFH*, физический смысл при этом остается одним – оценка вероятности несрабатывания СЗИ при возникновении запроса (угрозы). Рассмотрим случай низкой частоты возникновения угроз.

Для структуры СЗИ 1oo1 («1oo1 – структура один из одного» – нерезервированный набор элементов) при экспоненциальном законе распределения времени до отказа вероятность безотказной работы $R(t)$ рассчитывается по известной формуле

$$R(t) = \exp(-\lambda_{DU} t)\,. \qquad (2)$$

Тогда при малых значениях интенсивности опасных необнаруженных отказов λ_{DU} можно пренебречь влиянием времени восстановления MTTR и ремонта MRT (несколько часов) по сравнению с межконтрольным периодом T_1 (несколько месяцев или даже лет). В этом случае с учетом (1) и (2) приближенные формулы для расчета средней вероятности отказа на запрос *PFD* и средней частоте отказов на запрос *PFH* имеют вид [4]

$$PFD_{avg} \approx \frac{\lambda_{DU} T_1}{2}\,, \qquad (3)$$

(4)

$$PGH \approx \lambda_{DU}.$$

Подсистемы датчиков, исполнительных механизмов и логики могут иметь сложные резервированные структуры, например, дублированные структуры 1oo2 (для работы СЗИ достаточно одного средства из двух), мажоритарные структуры *KofN* (для работы СЗИ достаточно *K* средств из общего числа *N*), а также их комбинации. В этом случае можно использовать программные средства, позволяющие строить деревья неисправностей и структурные схемы надежности [5].

В качестве примера рассмотрим решение задачи с использованием аттестованного в Ростехнадзоре РФ программного комплекса АРБИТР [6].

Структурные методы анализа надежности в ПК АРБИТР реализованы с помощью универсального графического инструмента – схем функциональной целостности (СФЦ). Универсальность СФЦ выражается в том, что одни и те же графические элементы могут быть использованы для построения структурных схем надежности (ССН), деревьев неисправностей (ДН) и деревьев событий (ДС). Математической основой ПК АРБИТР является общий логико-вероятностный метод.

На рис.6 показан фрагмент интерфейса решения задачи моделирования показателей функциональной безопасности СЗИ.

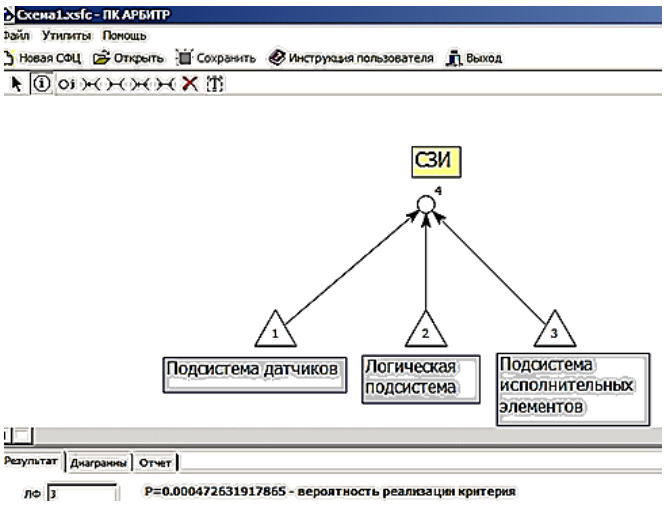


Рисунок 6 – **Экранный интерфейс моделирования показателей функциональной безопасности СЗИ**

СЗИ не выполнят свои функции безопасности в том случае, если не выполнят свои функции все подсистемы. Поэтому системный показатель (вершина *y4*) есть логическая сумма всех событий отказов подсистем.

На рис.6 треугольниками обозначены подсистемы СЗИ, которые имеют собственную внутреннюю структуру. Например, подсистема датчиков имеет структуру 2oo3. СФЦ подсистемы датчиков показана на рис.7.

Исходными данными для моделирования вероятности отказа на запрос подсистемы датчиков являются вероятности отказа на запрос датчиков. На СФЦ эти вероятности являются элементами 1, 2 и 3 дерева неисправностей. Системным критерием является вершина 4, реализация которой возможна при реализации любых двух инициирующих событий – отказов датчиков. Численные значения вероятностей отказов могут быть легко рассчитаны по формулам (3) или (4).

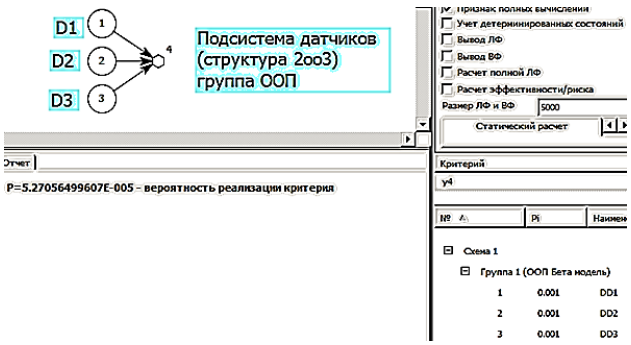


Рисунок 7 – **СФЦ подсистемы датчиков**

Согласно рекомендациям международных стандартов [3], анализ резервированных структур производится с учетом моделей отказов по общей причине (ООП). На рис.7 в нижнем правом углу показаны параметры Бета-модели учета ООП. Результатом моделирования является вероятность реализации критерия *y4*, который по физическому смыслу в данной задаче является вероятностью отказа на запрос подсистемы датчиков.

В соответствии с теорией информационной безопасности для систем, в которых не предусмотрено никаких мер по обеспечению информационной безопасности, вероятность реализации угрозы считается равной единице [7].

Учитывая такой подход, предлагается следующая методология анализа надежности АСУ с учетом надежности СЗИ.

В качестве логических условий работоспособности АСУ следует рассматривать следующие:

- условие безотказности аппаратных средства АСУ;
- условие безотказности аппаратных средств защиты информации;

- условие отсутствия отказов на запрос реализации функции безопасности в случае возникновения угрозы.

В этом случае логико-вероятностная модель в виде СФЦ может быть представлена как немонотонная схема, объединяющая структурные схемы надежности АСУ и СЗИ, а также дерево неисправностей для функции безопасности (рис.8).

В данном примере вероятность безотказной работы аппаратной части АСУ принята 0.95, аппаратной части СЗИ – 0.99, вероятность отказа на запрос СЗИ равна 5.27E-07 (рис.7).

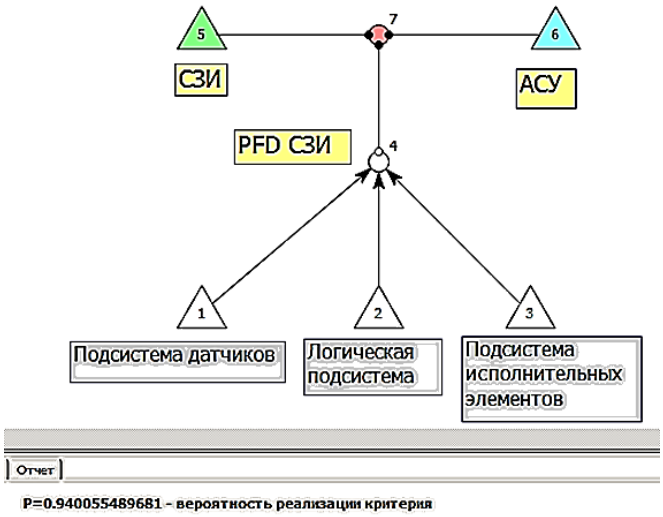
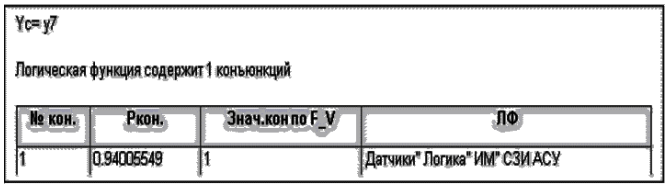


Рисунок 8– **СФЦ для моделирования надежности АСУ**

Результат моделирования с использованием СФЦ, показанной на рис.8, является формирование логической функции. Фрагмент отчета результатов моделирования приведен на рис.9.


Yc= y7

Логическая функция содержит 1 конъюнкций

№ кон.	Ркон.	Знач.кон по F_V	ЛФ
1	0.94005549	1	Датчики" Логика" ИМ" СЗИ АСУ

Рисунок 9 – **Фрагмент отчета результатов моделирования**

Логическая функция на рис.9 выражает условия для безотказности АСУ – отсутствие отказов в подсистеме датчиков (логическая переменная <Датчики">), в логической подсистеме (логическая переменная <Логика">), в подсистеме исполнительных механизмов (логическая переменная <ИМ">), а также безотказность аппаратных средства защиты информации (логическая переменная <СЗИ>) и безотказность аппаратных средств АСУ (логическая переменная <АСУ>). Знак <"> означает признак инверсного состояния логической переменной.

Как видно из рис.9, применение СЗИ снижает такой показатель надежности, как вероятность безотказной работы (с 0.95 до 0.94005549). И в то же время отсутствие СЗИ может, в случае кибератаки, привести к полной остановке АСУ.

Заключение

В промышленной безопасности, теории надежности и функциональной безопасности средств противоаварийной защиты накоплен значительный опыт решения риск ориентированных задач, который может быть использован для разработки методик оценки надежности различных объектов с учетом показателей информационной безопасности.

Литература

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года №187-ФЗ.

2. Специализированный программно-аппаратный комплекс InfoWatch ASAP [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/products/asap (дата обращения 22.03.2018).

3. ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1-7. 2012.

4. Rausand M. Reliability of Safety-Critical Systems: Theory and Applications. Willey. 2014. 448 p.

5. Можаева И.А., Нозик А.А., Струков А.В. Программная реализация методов количественного анализа риска аварий опасных производственных объектов на основе логико-вероятностного и логико-детерминированного подходов // Наука и безопасность. 2016. №2/20. С.26–36.

6. Можаев А.С. Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб.– М. : РНЦ «Курчатовский институт», 2008. – Вып. 2/2008. – С.105-116.

7. Рябинин И.А. Надежность и безопасность структурно-сложных систем. – СПб.: Изд-во С.-Петерб. ун-та, 2007. – 276с.

8. Корниенко А.А., Нозик А.А., Струков А.В. Моделирование и автоматизированный расчет надежности информационных систем и средств защиты информации. Учебное пособие. – СПб.: ПГУПС, 2014, 33с.

9. Беззатеев С.В., Волошина Н.В., Санкин П.С. Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности // Информационно-управляющие системы –2014. –№ 3(70). – С.78–83.

УДК 004.725.2

ПРОТОКОЛ ПАРНОЙ АУТЕНТИФИКАЦИИ УСТРОЙСТВ В СТАТИЧЕСКИХ СЕТЯХ БЕЗ ИНФРАСТРУКТУРЫ

С.В. Нестерук[1], С.В. Беззатеев[2]

Государственный университет аэрокосмического приборостроения (*ГУАП*),
190000, *Санкт-Петербург*, *ул. Большая Морская, д*. 67*, лит. А*

В работе рассматриваются вопросы безопасности беспроводных сетей без инфраструктуры, с быстро меняющимся составом элементов. Предлагается протокол аутентификации устройств, позволяющий противостоять атакам на радиоканал, физическим атакам, и являющийся энергоэффективным.

Ключевые слова: Интернет вещей, сенсорная сеть, аутентификация.

LOCATION-BASED PROTOCOL FOR THE PAIRWISE AUTHENTICATION IN THE NETWORKS WITHOUT INFRASTRUCTURE

S.V. Nesteruk, S.V. Bezzateev

State University of aerospace instrumentation,
190000, *St. Petersburg*, *Bolshaya Morskaya str*., 67, *lit. A*

This paper, we consider security issues of the wireless networks without infrastructure, with the rapidly changing composition. The device authentication protocol is proposed, which allows resisting attacks on the radio channel, physical attacks on the device, and is energy efficient.

Key words: Internet of Things, sensor network, authentication.

Введение. Со времён зарождения Интернета телекоммуникационные технологии сильно изменились и усовершенствовались [1]. Сейчас мы наблюдаем новый виток развития, на котором всё больше контента не создаётся людьми, а генерируется устройствами, что является логичным продолжением автоматизации всех сфер деятельности человека [2]. Такая парадигма называется Интернет вещей (IoT), и была впервые озвучена изобретателем Кевином Эштоном в 1999 г. [3].

Стремительный рост популярности Интернета вещей сегодня обусловлен резким падением цен на сенсоры и микроконтроллеры [4].

Технологии Интернета вещей используются повсеместно [5]. Ожидается, что в 2018 году мировые расходы на Интернет вещей достигнут 770 млрд. долларов. В первую очередь в таких технологиях заинтересованы промышленное производство (индустриальный Интернет), транспорт (Интернет машин) и коммунальные компании (системы мониторинга окружающей среды) [6].

Эти технологии породили множество небольших компаний, предлагающих свои решения, призванные помочь оставаться в безопасности в быстро меняющейся среде. Кроме того, многие крупные промышленные гиганты также выделяют свои ресурсы на исследования в этой области [7].

Проблемы безопасности являются основным препятствием на пути дальнейшего развития Интернета вещей. Если не решить задачи в сфере безопасности, пользователи потеряют доверие к подобным решениям [8]. При этом безопасность в сфере Интернета вещей имеет свою специфику:

- Устройства IoT очень разнообразны, а потому у них могут быть разные потенциальные уязвимостями.
- Устройства имеют ограниченный ресурс батареи.
- Большинство устройств должно работать в режиме реального времени.
- Устройства обычно рассчитываются на длительный жизненный цикл.
- Устройства часто расположены в незащищённой среде, что увеличивает риск физической атаки и усложняет диагностику [9].

Важным вопросом при разработке систем Интернета вещей является обеспечение безопасной передачи данных на уровне устройств. Мы можем рассматривать этот уровень как беспроводную сенсорную сеть. Беспроводная сенсорная

[1]*Сергей Валентинович Нестерук – студент 4 курса кафедры Технологий защиты информации, тел.:* +7 (911) 951 16 57, *e-mail: nesterus@protonmail.com;*
[1]*Сергей Валентинович Беззатеев – доктор технических наук, заведующий кафедры Технологий защиты информации, (научный руководитель) e-mail: bsv@aanet.ru*

сеть представляет собой самоорганизующуюся систему, состоящую из связанных радиоканалом маломощных узлов, которые могут выполнять роль пассивных датчиков для сбора данных или роль исполнительных устройств. В системе, построенной таким образом, устройства должны общаться между собой и реагировать на изменения в окружающей среде так, чтобы выполнялась поставленная задача [10].

Цель данной работы заключается в нахождении оптимального алгоритма аутентификации устройств в сетях с отсутствием инфраструктуры (типа Ad hoc).

Топологии сенсорных сетей. На сегодняшний день самой распространённой топологией, которую используют разработчики систем Интернета вещей, а также разработчики платформ такие как [11-15] является «звезда». Она подразумевает наличие одной базовой станции, с которой связываются все абоненты. Такой подход является самым простым в реализации, но часто не самым эффективным, поэтому большую популярность набирают различные типы самоорганизующихся сетей.

Самоорганизующаяся сеть представляет собой сеть с изменяемой децентрализованной инфраструктурой [16] или вообще с отсутствием какой-либо инфраструктуры. Среди плюсов таких сетей: самоорганизация, самовосстановление, малая потребная мощность передачи данных, масштабируемость и плотность покрытия. Среди недостатков: сложность сети, накладные расходы на поддержание сети задержка при ретрансляции данных, высокое энергопотребление ретрансляторов.

С развитием технологий самоорганизующихся сетей также появилась путаница в их классификации. Пользователи стали использовать термин «ad hoc» для обозначения прямого соединения двух компьютеров, один из которых был точкой доступа и обеспечивал выход в Интернет [17]. Рассмотрим некоторые виды самоорганизующихся сетей и их основные свойства в порядке возрастания предоставляемых возможностей и, соответственно, повышения сложности их проектирования.

Mesh сети. Mesh сети – радиосети ячеистой структуры, состоящие из беспроводных стационарных маршрутизаторов, которые создают беспроводную магистраль и зону обслуживания мобильных/стационарных абонентов, имеющих доступ к одному из маршрутизаторов. Mesh сети строятся по топологии «звезда звёзд», и имеют случайные соединения опорных узлов [18]. Из-за иерархической структуры такие сети просты в проектировании. Именно поэтому на сегодняшний день они наиболее распространены среди самоорганизующихся сетей, и успешно применяются в системах связи и сенсорных сетях. Но по той же причине они являются менее надёжными, поскольку при выходе из строя одного узла сети, все связанные с ним устройства более низкого уровня также будут недоступны [17].

Главные свойства mesh сетей заключаются в том, что они: беспроводные и динамические.

Под динамичностью сети здесь подразумевается то, что она настраивается сама, без участия человека. При этом она может требовать управляющей или статистической информации между узлами, участвующими в организации сети приёма и передачи данных [19].

Ad hoc сети. Выражение «ad hoc» пришло из латыни и переводится как «для данного случая». Ad hoc сети – радиосети со случайными стационарными абонентами, реализующие полностью децентрализованное управление при отсутствии базовых станций или опорных узлов. Топология таких сетей имеет случайное соединение узлов [18]. Важной особенностью таких сетей является то, что узлы такой сети независимы друг от друга и могут включаться или выключаться в любой момент, что предопределяет случайный характер структуры сети. В таких сетях узлы полностью или частично функционально идентичны. Одноранговый принцип организации динамических сетей обусловливает их высокую отказоустойчивость за счет исключения проблемы уязвимости центрального звена [16]. Таким образом, главные свойства ad hoc сетей заключаются в том, что они: беспроводные, динамические и децентрализованные. Децентрализованность сети заключается в отсутствии единого управляющего центра [19].

Отличительная особенность вышеперечисленных технологий от других динамических сетей является пространственная стационарность узлов сети. Это существенно упрощает решение задачи маршрутизации потоков данных и позволяет хранить на узлах полную топологию сети или ее отдельные фрагменты [16].

MANET сети. MANET (Mobile Ad hoc NETworks) сети – радиосети со случайными мобильными абонентами, реализующие полностью децентрализованное управление при отсутствии базовых станций или опорных узлов. Топология таких сетей – быстро меняющаяся со случайным соединением узлов [18]. Сеть MANET является частным случаем ad hoc сети. Главные свойства MANET сетей заключаются в том, что они: беспроводные, динамические, децентрализованные и мобильные. Мобильность сетей заключается в возможности перемещения узлов сети в пространстве [19].

VANET сети. VANET (Vehicle Ad hoc NETworks) – сети связи транспортных средств. Являются гибридами MANET сетей [18].

Отличительной особенностью таких сетей является то, что все узлы постоянно движутся и могут связываться друг с другом на очень непродолжительное время, что значительно усложняет маршрутизацию информации. В некоторых системах конечные устройства могут постоянно передвигаться, и должны быть обеспечены связью в любой точке. В данной работе мы рассмотрим протокол взаимной аутентификации устройств, который подразумевает статичность абонентов, и гарантирует невозможность работы устройства при его значительном отдалении от места его инициализации.

Существующие протоколы. За последние несколько десятилетий было предложено множество протоколов аутентификации устройств в сенсорных сетях. Большинство из них основаны на основных протоколах, которые мы коротко опишем далее.

EG Scheme. В схеме, предложенной Эшенауером и Глигором [20], перед установкой устройств сервер должен сгенерировать большой пул ключей и записать на каждое устройство случайно выбранное подмножество из этого пула. После установки устройств у любых двух соседних устройств сети с определённой вероятностью будет хотя бы один общий ключ. У данной базовой схеме есть ряд недостатков:

- Не используется идентификатор устройства, что не позволяет определить какое именно устройство аутентифицируется.
- При захвате одного устройства, компрометируются все устройства, имеющие с этим устройством хотя бы один общий ключ.
- При масштабировании сети на устройства должны быть записаны большие подмножества ключей, иначе вероятность совпадения хотя бы одного ключа на двух соседних устройствах будет очень мала.

Позже данная схема была улучшена. В PKS-Key [21] устройствам для аутентификации необходим не один, а несколько общих ключей, на основе которых считается парный ключ. Также в этой схеме предлагается помимо общих ключей использовать идентификаторы, что позволяет однозначно определить собеседника. Для обновления парного ключа предлагается передавать его частями по нескольким разным маршрутам, что не позволит злоумышленнику перехватить новый ключ, если у него нет доступа к достаточному количеству соседних устройств. Несмотря на увеличение криптостойкости такой схемы, в ней сохраняется ряд недостатков:

- Используется большой коммуникационный ресурс.
- С увеличением числа захваченных устройств увеличивается вероятность компрометации всей сети.
- Сохраняется ограничение на максимальное количество устройств в сети.

В PKS-MP схеме [22] было предложено при записи подмножества ключей на устройства основываться на вероятности того где устройство будет установлено. Если два устройства с большой вероятностью будут установлены рядом, то в их подмножества будет добавлен одинаковый общий ключ. Таким образом, на устройства можно записывать меньше ключей, что убирает ограничение на размер сети. Но на практике довольно сложно заранее определить, где будет установлено конкретное устройство.

TESLA. Для цифровой подписи необходима асинхронность. Но классические асинхронные алгоритмы требуют большого вычислительного ресурса. В [23] было предложено добиваться асинхронности с помощью времени, используя при этом синхронные криптографические примитивы. В данной схеме сообщение и подпись отправляются в разные временные интервалы. Подпись основывается на цепочке ключей, получив которую все могут вычислить любой предыдущий ключ, но следующий ключ может вычислить только устройство, обладающее секретом. В данной схеме:

- Для работы схемы необходима синхронизация устройств по времени.
- Существует большая задержка в определении ключа.
- Для больших сетей требуется очень большое количество пересылок.
- Каждое устройство во время начальной инициализации активируется отдельно.

На основе данной схемы были предложены μTESLA [24] и Multilevel μTESLA [25], оптимизированные для больших сетей с помощью использования широковещательной передачи ключей. Позже была предложена схема RPT [26], которая позволяет моментально аутентифицировать сообщение, но требует отправки сообщений в регулярные и предсказуемые промежутки времени.

BiBa. В схеме BiBa [27] для подписи сообщения отправитель сначала вычисляет хэш от сообщения и выбирает на его основе одну одностороннюю функцию из некоторого заранее определенного подмножества односторонних функций. С её помощью отправитель также считает хэши от заранее сгенерированных случайных чисел, и ищет коллизии среди получившихся значений. Найденные коллизии и будут подписью сообщения. Криптостойкость данного протокола обеспечивается тем, что отправитель найдёт коллизии с большей вероятностью, чем злоумышленник, который не знает всего множества случайных чисел сгенерированных отправителем даже, если он захватил несколько уст-

ройств. В данной схеме сообщения быстро верифицируются но очень долго подписываются.

В HORS [28] протокол позволяет подписывать сообщения быстрее благодаря тому, что оптимизирован выбор односторонней функции из заранее определенного подмножества.

LEAP. Базовый протокол LEAP [29] подразумевает использование в иерархической mesh-сети. При этом для разных типов сообщений выделяют несколько типов ключей. Индивидуальный ключ используется для шифрования сообщений между устройством и сервером. Парный ключ устройства вырабатывают со своими соседями на основе мастер-ключа и идентификаторов устройств. Мастер-ключ удаляется из памяти устройств после создания парных ключей. Кластерный ключ генерируется одним из устройств для всех соседних и передаётся им с помощью парных ключей. Групповой ключ единственный для всех сети. Одним из недостатков такой схемы является то, что, если злоумышленник успевает получить мастер-ключ из памяти устройства до его удаления, то он получает доступ ко всей сети.

В TB-LEAP [30] для каждого интервала времени используется свой мастер-ключ, что сужает область скомпрометированных устройств при захвате мастер-ключа от всей сети до одного кластера. Далее мы рассмотрим более подробно протокол LEAP, и предложим улучшение схемы, рассмотренной в [31].

Уязвимость LEAP к атаке на этапе инициализация устройств. В базовой схеме LEAP во время инициализации сети устройства отправляют широковещательные запросы со своими идентификаторами и ждут ответ от соседних устройств с их идентификаторами.

$$u \rightarrow *: IDu;$$

$$v \rightarrow u: IDu, H(H(IDv||MK), IDu||IDv),$$

где u – это новое устройство; v – одно из устройств, ответивших на запрос u; $H()$ – криптографическая хэш-функция.

В такой схеме возможна уязвимость, при помощи которой можно скомпрометировать всю сеть, захватив всего одно устройство. Далее рассмотрим более подробно вариант атаки и способы защиты от неё.

Алгоритм 1 Атака на протокол LEAP.

1: Устройство u во время инициализации отправляет широковещательный запрос:

$$u \rightarrow v: IDu.$$

2: Устройство v отвечает:

$$v \rightarrow u: ID_u, H(H(ID_v||MK)||ID_u||ID_v) \quad (1)$$

где ID_u это идентификатор устройства u, ID_v это идентификатор устройства v.

3: Злоумышленник E перехватывает (1).

4: Устройство u генерирует парный ключ

$$Ku, v = H(ID_u||ID_v||MK), ID_u < ID_v$$

5: В сеть добавляется новое устройство k, и отправляет широковещательный запрос:

$$k \rightarrow *: ID_k$$

6: Злоумышленник E отвечает перехваченным ранее ответом:

$$E \rightarrow k: ID_u, H(H(ID_v)|| ID_u||ID_v)$$

7: Устройство k на основе ответа E генерирует парный ключ:

$$Kk, v = H(ID_k||ID_v||MK), (ID_k < ID_v)$$

8: Злоумышленник захватывает устройство k, и получает ключ $K_{k,v}$.

9: Злоумышленник может общаться с устройством v представляясь устройством k.

Таким образом, злоумышленник может получить парные ключи для общения с нужными ему устройствами перехватив их ответы на запрос инициализации, и захватив одно устройство. Далее нами будут предложены и проанализированы возможные варианты защиты от описанной атаки.

В зависимости от конкретной реализации системы мы можем использовать устройства, затрачивающие разный энергоресурс на различные операции. Далее мы рассмотрим две схемы, причем при выборе оптимальной из этих двух схем следует учитывать какая из операций в конкретной системе требует меньше ресурса: беспроводная пересылка данных или проверка цифровой подписи.

Возможные схемы защиты от уязвимости LEAP на этапе инициализация устройств.

Симметричная схема. Схема включает фазу настройки устройств на сервере, развёртывание сети и фазу добавления новых устройств.

При инициализации сервер генерирует уникальный идентификатор для каждого устройства, мастер-ключ и записывает их на устройства. Далее идёт фаза развёртывания сети, во время которой все устройства новые т.е. ещё хранят мастер-ключ.

Алгоритм 2 Симметричное развёртывание.

1: Устройство u отправляет широковещательный запрос:

$$u \rightarrow *: ID_u, H(ID_u||R_u||MK), R_u, new$$

где R_u – это случайное число, сгенерированное u;

MK — это мастер-ключ;

new – это строка, которая позволяет понять, что устройство ещё хранит MK.

2: Устройство v считает $H(ID_u||R_u||MK)$, и

если оно совпадает с тем, что прислал u, *тогда* отправляет:

$$v \rightarrow u: ID_v, H(ID_v||R_v||MK), R_v, new$$

3: Устройство u проверяет подпись, и

если она верна **т***огда* вычисляет

$$K_{u,v} = H(ID_u||ID_v||MK), ID_u < ID_v \quad (2)$$

4: Устройство *v* вычисляет

$$K_{v,u} = H(ID_u||ID_v||MK), ID_u < ID_v \quad (3)$$

5: Устройство *u* генерирует ключ

$$K_{u,u} = H(ID_u||MK) \quad (4)$$

необходимый для дальнейшего масштабирования сети.

6: Устройство *v* генерирует ключ $K_{v,v}$ аналогично (4).

7: Устройство *u* удаляет *MK*.

8: Устройство *v* удаляет *MK*.

Как видно ключи (2) и (3) совпадают, и будут далее использоваться как парный ключ *u* и *v*.

Поскольку после начального развёртывания сети установленные устройства удаляют мастер-ключ, для добавления новых устройств в сеть нужна отдельная схема.

Алгоритм 3 Симметричное добавление нового устройства.

1: Новое устройство *u* отправляет широковещательный запрос со своим идентификатором и случайным числом:

$$u \rightarrow *: ID_u, H\big(ID_u||R_u||MK\big), R_u, new, \quad (5)$$

где R_u – это случайное число, сгенерированное *u*.

2: Устройство *v* отвечает своим идентификатором с подтверждением ACK_v:

$$v \rightarrow u: ID_v, ACK_v = H(ID_u||ID_v||R_v||K_{v,v}), old \quad (6)$$

где *old* – это строка, информирующая, что *v* больше не хранит *MK*.

3: Устройство *u* считает $K_{v,v}$ по формуле (4), и

если вычисленное им значение $H(ID_u||ID_v||R_u||K_{v,v}))$ совпадает с ACK_v *тогда* сохраняет $K_{v,v}$ *иначе* удаляет $K_{v,v}$ из памяти.

4: Устройство *u* удаляет *MK*.

При этом устройство *v* обязано реагировать на каждый запрос (5), и в ответ должно считать и пересылать (6).

Асимметричная схема.

Алгоритм 4 Ассиметричная настройка устройств.

1: Сервер генерирует ключи для цифровой подписи *(MK =* K_{priv} *,* K_{pub}*)* и записывает их на устройства. При этом мастер-ключом в такой схеме считается секретный ключ K_{priv}.

2: Сервер генерирует уникальный идентификатор для каждого устройства, и записывает их на устройства.

Алгоритм 5 Ассиметричное развёртывание.

1: Устройство *u* отправляет подписанный широковещательный запрос:

$$u \rightarrow *: ID_u, H_{MK}(ID_u)$$

где $H_{MK}()$ — это подпись мастер-ключом.

2: Устройство *v* проверяет подпись с помощью открытого ключа K_{pub}, и

если подпись верна, *тогда* отправляет:

$$v \rightarrow u: ID_v, H(ID_v||R_v||MK), R_v, new$$

3: Устройство *u* проверяет подпись, и

если она верна *тогда* вычисляет $K_{u,v}$ аналогично (2).

4: Устройство *v* вычисляет $K_{v,u}$ аналогично (3).

5: Устройство *u* генерирует ключ $K_{u,u}$ аналогично (4).

6: Устройство *v* генерирует ключ $K_{v,v}$ аналогично (4).

7: Устройство *u* удаляет *MK*.

8: Устройство *v* удаляет *MK*.

Алгоритм 6 Ассиметричное добавление нового устройства.

1: Устройство *u* отправляет подписанный широковещательный запрос со своим идентификатором:

$$u \rightarrow *: ID_u, R_u, H_{MK}(ID_u||R_u)$$

2: Устройство *v* проверяет подпись с помощью открытого ключа K_{pub}, и *если* подпись верна *тогда* отвечает своим идентификатором с подтверждением:

$$v \rightarrow u: ID_v, ACK_v = H(ID_u||ID_v||R_u||K_{v,v}), old$$

3: Устройство *u* считает $K_{v,v}$ по формуле (4), и

если $H(ID_u||ID_v||R_u||K_{v,v})$ совпадает с ACK_v, *тогда* сохраняет $K_{v,v}$ *иначе* удаляет $K_{v,v}$ из памяти.

4: Устройство *u* удаляет *MK*.

Ассиметричная схема отличается от симметричной тем, что первый широковещательный запрос тоже подписывается.

При этом важно отметить, что выполнение ассиметричной операции будет использовать намного больше энергоресурса. Но её применение позволит при DoS атаке не отвечать на сообщения злоумышленника. Таким образом, если при работе сети нет атак, устройства выполнят всего одну лишнюю асимметричную операцию, а при атаке не будут тратить ресурс на ответы, но будут вынуждены считать асимметричные операции.

Аутентификация устройств. При выборе протокола аутентификации для ad hoc сети важно понимать, что кроме таких угроз как не санкционируемый доступ и подмена данных существует также угроза разряда батареи устройства [9]. Для того, чтобы противостоять этой угрозе необходимо снизить вычислительные затраты устройства при аутентификации.

Предлагаемый протокол:

Алгоритм 7 Аутентификация устройства.

1: Устройство *u* отправляет запрос на аутентификацию:

$$u \rightarrow v: ID_u. \quad (7)$$

где *u* – устройство, которое хочет отправить сообщение, *v* – принимающее устройство.

2: Устройство v отправляет случайное число Rv и подтверждение:

$v \rightarrow u: R_v 3$: Устройство u считает сеансовый ключ:

$$K_{auth} = H(K_{u,v}||ID_u||R_v)\,. \qquad (8)$$

4: Устройство v считает сеансовый ключ аналогично (8).

Как видно из (7) аутентификацию всегда инициирует передающее устройство. Роль приёмного устройства сводится к генерированию и передаче случайного числа для каждого устройства, которое хочет пройти аутентификацию, и вычислению сеансового ключа на его основе и пассивному прослушиванию канала.

Важно отметить, что благодаря использованию криптографической хэш-функции, например, [32], нет необходимости менять сеансовый ключ при неудачной попытке устройства аутентифицироваться. Новый ключ будет сгенерирован только для нового сеанса.

Атаки на сенсорную сеть. Поскольку датчиков в сенсорной сети может быть много, и они могут быть распределены на большой площади, злоумышленник может получить непосредственный доступ к устройству [33]. Поэтому имеет смысл рассматривать отдельно те угрозы, в которых злоумышленник имеет доступ к устройству, и те, для которых используется только доступ к каналу связи. Далее рассмотрим распространённые атаки на сенсорные сети.

Атаки без доступа к устройству. Находясь в зоне работы радиоканала, злоумышленник может перехватывать легальный трафик и создавать вредоносный трафик.

При этом могут осуществляться следующие атаки:

1) **DoS (Denial-of-service).**

DoS атака является попыткой сделать устройство недоступным для своих реальных абонентов. Из-за очень ограниченных вычислительных ресурсов и заряда батареи IoT устройства особенно уязвимы перед этим типом атак.

Предлагаемый протокол аутентификации смягчает воздействие подобных атак благодаря тому, что освобождает устройство от необходимости вычислять новый сеансовый ключ при каждой попытке другого устройства пройти аутентификацию.

Когда устройство получает запрос на попытку аутентифицироваться оно должно посчитать сеансовый ключ (8). При этом, если запрашивающее устройство успешно проходит аутентификацию, то принимающее устройство выходит из энергосберегающего режима, и продолжает обслуживание проверенного абонента. Если запрашивающее устройство не проходит аутентификацию, то принимающее устройство не пересчитывает сеансовый ключ, и не выходит из энергосберегающего режима.

Также может быть предпринята попытка провести DoS атаку не сообщениями, а запросами на аутентификацию. Чтобы избежать такую атаку в данной работе предложены две схемы. Синхронная схема использует для проверки подлинности собеседника исключительно симметричные криптографические примитивы, но требует одной дополнительной пересылки. Асимметричная схема позволяет не отвечать на неподлинные запросы, но использует более затратные асимметричные примитивы.

2) **Прослушивание**

Прослушивание канала может позволить злоумышленнику получить конфиденциальные данные. Чтобы этого избежать, передаваемые сообщения необходимо шифровать. Для упрощения управления ключами при шифровании в некоторых случаях можно использовать сеансовый ключ (8). Но мы рекомендуем использовать уникальный ключ для шифрования передаваемых данных на каждом устройстве, и расшифровывать их не на каждом промежуточном узле сети, а на сервере. В таком случае ключи для дешифрования необходимо хранить на сервере.

3) **Подмена данных**

Для защиты данных от подмены недостаточно их шифровать. Необходимо использовать цифровую подпись для передаваемых сообщений. Для этой процедуры также возможно использовать сеансовый ключ (8).

Атаки с доступом к устройству. Получив доступ к устройству, злоумышленник может получить доступ к памяти устройства.

При этом могут осуществляться следующие атаки:

4) **Подделка (Spoofing)**

Если злоумышленник имеет доступ к памяти устройства, он может извлечь криптографический материал и частично или полностью подменить устройство [14].

При этом важно не позволить злоумышленнику, получив контроль над одним устройством, получить контроль над всей сенсорной сетью. Это требование обеспечивается тем, что для каждой пары устройств сеансовый ключ уникален. Если устройство добавлено в сеть после начальной инициализации сети, парный ключ (4) может оказаться не уникальным, но благодаря использованию идентификатора передающего устройства в формуле расчета сеансового ключа (8), сеансовый ключ будет уникальным. Таким образом, злоумышленник сможет подделать процедуру аутентификации только с захваченного устройства.

При этом подразумевается, что МК был удалён с устройства раньше, чем злоумышленник получил к нему доступ.

5) **Прослушивание**

Контролируя устройство, злоумышленник может сканировать проходящий через него трафик. Чтобы избежать прослушивания телеметрических данных на ретрансляторе, данные должны расшифровываться не на каждом узле, а на сервере.

6) **Перемещение устройства**

При доступе злоумышленника к устройству он может переместить его в место, из которого устройство будет присылать неверные телеметрические данные или же клонировать устройство. Предлагаемый протокол аутентификации позволяет переместить устройство только в рамках зоны действия устройства, с которым оно аутентифицируется. Если переместить устройство у другую часть сети, оно не сможет выработать парные ключи с новыми соседями. Таким образом несанкционированное перемещение устройства невозможно. Протокол предназначен для использования в ad hoc сетях, поскольку рассчитан на взаимодействие точка-к-точке узлов с симметричным функционалом. Но это не мешает использовать его в mesh сетях со сложной иерархией.

Несмотря на то, что протокол не пригоден для использования в MANET и VANET сетях, это не означает, что его абоненты не могут передвигаться. Возможны варианты архитектуры системы, в которых мобильные абоненты собирают информацию в течение некоторого времени, и передают её ретранслятору вернувшись на место инициализации устройства. Кроме аутентификации, протокол может предоставлять ключи, которые можно использовать для шифрования и цифровой подписи передаваемых сообщений. Поскольку алгоритм гарантирует невозможность использования устройства вне зоны его инициализации, его можно использовать для локального позиционирования. Такая система не будет точной, но не потребует дополнительного оборудования устройства.

В зависимости от характеристик конкретной системы оптимальным будет использование асимметричной схемы, если устройство тратит больше ресурса на пересылку данных, чем на вычисление цифровой подписи, и симметричной схемы в противном случае.

Поскольку для расчёта парных ключей на этапе инициализации сети для всех устройств используется общих мастер-ключ, важно не допустить получения этого ключа злоумышленником. Получив МК злоумышленник может подделать сообщения от любого устройства сети.

Важно понимать, что для масштабирования сети придётся хранить МК на сервере, чтобы записывать его не новые устройства. Поэтому, необходимо обеспечить защиту не только новых устройств от физических атак до момента их инициализации, но также защищать МК на сервере.

Также стоит отметить, что нельзя беспрекословно доверять данным, которые пришли из сенсорной сети. Их необходимо проверять и логировать не сервере.

выводы

В данной работе предложен простой и эффективный протокол аутентификации устройств в сенсорной сети, который гарантирует невозможность несанкционированного перемещения устройства в беспроводной сенсорной сети. Данный протокол подходит для использования в не мобильных ad hoc и mesh сетях, и обеспечивает простую масштабируемость системы. Предложенный протокол обеспечивает защиту от прослушивания и подмены данных, а также больших энергопотерь при атаках на систему. В дальнейшем предполагается смоделировать работу протокола, и определить оптимальный размер мастер-ключа и идентификаторов устройств, а также подобрать энергоэффективную хэш-функцию для использования в предложенном протоколе.

Литература

1. Сафонов А. В IoT вещи сами генерируют информацию. PostNauka [Электронный ресурс]. – Режим доступа: https://postnauka.ru/talks/30032, (дата обращения: 21.02.2018).
2. Хоров Е. От сенсорных сетей к Интернету вещей. PostNauka[Электронный ресурс]. – Режим доступа: https://postnauka.ru/faq/80050, (дата обращения: 21.02.2018).
3. Восков Л. Эволюция IoT. PostNauka [Электронный ресурс]. – Режим доступа: https://postnauka.ru/talks/80081, (дата обращения: 21.02.2018).
4. Step by step: collect and test the Internet of things based on the SAP Cloud Platform. SAP Cloud Platform official blog [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/sap/blog/326526/, (дата обращения: 21.02.2018).
5. DC Forecasts Worldwide Spending on the Internet of Things. Business Wire Inc. [Электронный ресурс]. – Режим доступа: https://www.businesswire.com/news/home/20171207005963/en/IDC-Forecasts-Worldwide-Spending-Internet-Things-Reach, (дата обращения: 21.02.2018).
6. The 10 Most Vulnerable IoT Security Targets. Internet of Things Institute [Электронный ресурс]. – Режим доступа: http://www.ioti.com/security/10-most-vulnerable-iot-security-targets, (дата обращения: 21.02.2018).

7. 25 leading IoT security companies. Internet of Things Institute [Электронный ресурс]. – Режим доступа: http://www.ioti.com/security/25-leading-iot-security-companies, (дата обращения: 21.02.2018).
8. How to Get One Trillion Devices Online. MIT Technology Review [Электронный ресурс]. – Режим доступа: https://www.technologyreview.com/s/608878/how-to-get-one-trillion-devices-online/, свободный (дата обращения: 26.02.2018).
9. What Makes IoT Security so Unique. ZingBox Inc. [Электронный ресурс]. – Режим доступа: https://www.zingbox.com/iot-security, (дата обращения: 26.02.2018).
10. Рагозин Д.В. Моделирование синхронизированных сенсорных сетей // Проблемы программирования. – 2008. – Т. 2-3. – С. 721-729.
11. От инновационной технологии LPWAN к первой IoT платформе. Strizh [Электронный ресурс]. – Режим доступа: http://www.embeddedday.ru/2016/presentations/1.5_%D0%A1%D0%A2%D0%A0%D0%98%D0%96_LPWAN.pdf, (дата обращения: 26.02.2018).
12. CENTRI Internet of Things Advanced Security. CENTRI Technology Inc. [Электронный ресурс]. – Режим доступа: https://www.centritechnology.com/wp-content/documents/CENTRI_datasheet_IoTAS.pdf, (дата обращения: 26.02.2018).
13. Going back to school on IoT security – personal reflections from a cybersecurity product marketeer [Электронный ресурс]. – Режим доступа: https://blogs.cisco.com/security/going-back-to-school-on-iot-security-personal-reflections-from-a-cybersecurity-product-marketeer, (дата обращения: 26.02.2018).
14. Internet of Things security architecture. Microsoft Inc. [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture, (дата обращения: 26.02.2018).
15. Device Security. Google Cloud Platform [Электронный ресурс]. – Режим доступа: https://cloud.google.com/iot/docs/concepts/device-security, (дата обращения: 26.02.2018).
16. Шишаев М. Г. Современные технологии сетей типа ad-hoc и возможные подходы к организации одноранговых телекоммуникационных сетей на базе мобильных устройств малого радиуса действия // Труды Кольского научного центра РАН. –2010. – С. 70-74.
17. Rohilla Y. A comparative study of wireless mesh and ad hoc / International Journal on Computer Science and Engineering (IJCSE). – 2012. – Vol. 4, No. 06. – pp. 1181-1184.
18. Воитенго Г. Что такое MANET или почему WiFi не решение всех телекоммуникационных проблем [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/197860/, (дата обращения: 26.02.2018).
19. Гусс С. В. Самоорганизующиеся mesh сети для частного использования / Математические структуры и моделирование. – 2016. – Том 4(40) . – С. 102-115.
20. Eschenauer L. A Key-management Scheme for Distributed Sensor Networks / L. Eschenauer, V. D. Gligor. – Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS'02). – 2002. – 41-47 pp.
21. Chan H. Random Key Predistribution Schemes for Sensor Networks / H. Chan, A. Perrig, D. Song // IEEE Symposium on Research in Security and Privacy. – 2003. – 197-213 pp.
22. A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge // IEEE Transactions on dependable and secure computing. – 2006. – vol. 3, No. 1. – 62-77 pp.
23. Perrig A. Efficient authentication and signing of multicast streams over lossy channels / A. Perrig, R. Canetti, D. Song, D. Tygar // Proceedings of the 2000 IEEE Symposium on Security and Privacy. – 2001.
24. SPINS: Security protocols for sensor networks / A. Perrig, R. Szewczyk, V. Wen, D. Culler, D. Tygar // Proceedings of Seventh Annual International Conference on Mobile Computing and Networks. – 2001.
25. Donggang L. Multilevel μTESLA: Broadcast Authentication for Distributed Sensor Networks / L. Donggang, N. Peng. – North Carolina State University. – ACM Transactions on Embedded Computing Systems. – 2004. – Vol. 3, No. 4. – 800–836 pp.
26. Luk M. Seven Cardinal Properties of Sensor Network Broadcast Authentication / M. Luk, A. Perrig, B. Whillock. – Electrical and Computer Engineering Carnegie Mellon University. – 147-156 pp.
27. Perrig A. The BiBa one-time signature and broadcast authentication protocol // Eighth ACM Conference on Computer and Communication Security. – 2001. – 28–37 pp.
28. Reyzin L. Better than BiBa: Short One-time Signatures with Fast Signing and Verifying / L. Reyzin, N. Reyzin // Boston University. – pp. 1-9.
29. Zhu S. LEAP: Efficient security mechanisms for largescale distributed sensor networks / S. Zhu, S. Setia, S. Jajodia. – Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS'03), 2003. – 62-72 pp.
30. Jang J. A time-based key management protocol for wireless sensor networks / J. Jang, T. Kwon, J. Song // Proceedings of ISPEC. – 2007. – LNCS 4464. – pp. 314-328.
31. Нестерук С. В. Аспекты безопасности беспроводных сенсорных сетей / С. В. Нестерук, А. В. Шишко, С. В. Беззатеев // Международная студенческая конференция ГУАП. – 2017. – Том. 1 Технические науки. – С. 282-285.
32. I. Anshel, D. Atkins, D. Goldfeld, P. Gunnells, "A class of hash functions based on the algebraic eraser", Groups Complex, Cryptol, 2016, vol:8(1), pp. 1–7.
33. Abomhara M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks / M. Abomhara, G. M. Koien // Journal of Cyber Security and Mobility. – 2015. – University of Agder. – pp. 65-88

УДК 004.056.053

ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АППАРТАНО-ПРОГРАММНОГО КОМПЛЕКСА «БЕЗОПАСНЫЙ ГОРОД»

А.А. Лосева[1], А.В. Андреев[2]

ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»
195251, *Санкт-Петербург, ул. Политехническая,* 29

В статье применяется теория множеств для построения модели угроз информационной безопасности аппаратно-программного комплекса «Безопасный город» с применением теории множеств, в которой учитываются внутрисегментные и межсегментные вторжения злоумышленников.

Ключевые слова: модель угроз, информационная безопасность, противодействие терроризму.

THE DEVELOPMENT OF THE MODEL OF INFORMATION SECURITY THREATS OF THE HARDWARE-SOFTWARE SYSTEM "SAFE CITY"

A.A. Loseva, A.V. Andreev

The article deals with description of the model of information security threats of the hardware-software system «safe city» from the position of set theory, given the inside-and inter-segment intrusion of attackers.

Keywords: model of the treats, information security, counteraction to terrorism.

В настоящее время одной из важнейших задач является повышение общего уровня общественной безопасности, правопорядка и безопасности среды обитания. Одним из направлений решения задачи может быть существенное улучшение координации деятельности соответствующих сил и служб, путем внедрения на базе муниципальных образований комплексной информационной системы, обеспечивающей мониторинг, прогнозирование, предупреждение и ликвидацию возможных угроз, а также контроль устранения последствий чрезвычайных ситуаций и правонарушений. Для решения данного комплекса задач разработан аппаратно-программный комплекс (АПК) «Безопасный город». Рассмотрим модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город» с позиции теории множеств, учитывая вторжения злоумышленников.

Аппаратно-программный комплекс (АПК) «Безопасный город» представляет собой территориально-распределенную систему безопасности, состоящую из множества необходимых подсистем функционирования. Некоторые подсистемы отличаются своей внутренней инфраструктурой, наличием собственных систем управления базами данных, интеллектуальными средствами поддержки и распознавания образов. Многие из них являются самостоятельными информационными системами, автоматизирующими процессы обработки, хранения и передачи данных как через открытые информационные сегменты единой информационно-телекоммуникационной системы, так и через сегменты ограниченного распространения, доступ к которым осуществляется посредством удаленного подключения субъектов к выделенным им информационным ресурсам.

Необходимость создания требуемой системы защиты информации обусловлена такими факторами, как разнородность программно-аппаратного обеспечения подсистем, большое количество неоднозначно классифицируемых данных (признаков атак), получаемых от сетевых и хостовых сенсоров, сложность оценки событий информационной безопасности, возможные реализации угроз безопасности информации через обнаруживаемые злоумышленником уязвимости. Описание угроз безопасности, построение их модели позволяет адекватно оценить уровень опасности и предложить необходимую архитектуру подсистемы защиты информации АПК «Безопасный город».

В данной статье для построения такой модели проведем анализ угроз, направленных на информационные ресурсы подсистем АПК, учитывая данные, получаемые сенсорами маршрутизаторов, коммутаторов и межсетевых экранов.

В настоящее время подавляющее число угроз информационной безопасности принципиально могут быть реализованы только в процессе функционирования информационных систем, при этом логическое вторжение является наиболее результативным для злоумышленника. Логическое вторжение обычно делится на внутрисистемное и удаленное. При внутрисистемном вторжении предполагается, что нарушитель уже

Лосева Анастасия Андреевна – студентка Санкт-Петербургского политехнического университета, тел: +7 952 369 88 79, *e-mail: losevanastasiia@gmail.com*
Андреев Андрей Викторович – кандидат военных наук, доцент высшей школы техносферной безопасности Санкт-Петербургского политехнического университета, тел.:+7 (812) 297 58 98, *e-mail:office@mes.spbstu.ru*

имеет учетную запись в системе как пользователь с невысокими привилегиями и совершает атаку на систему для получения дополнительных привилегий. Удаленное вторжение заключается в попытке проникновения в систему с удаленной машины (хоста) участников информационного обмена сети. Это атаки, выполняемые при постоянном участии человека, и атаки, выполняемые специальными программами: атаки на информацию, хранящуюся на внешних запоминающих устройствах, атаки на информацию, передаваемую по линиям связи, атаки на информацию, обрабатываемую в памяти компьютера.

Основной целью практически любой атаки при реализации угрозы является получение несанкционированного доступа к информации.

Для описания угрозы, представляющей собой канал несанкционированного доступа (реализация сетевой атаки, деструктивные воздействия вредоносных программ, инсайдерские атаки), необходимо указать субъект доступа, путь распространения угрозы и информационный объект, к которому осуществляется несанкционированный доступ, нарушающий правила разграничения. Такая угроза может быть описана кортежем:

$$U = \langle S, К, Б_с, Б_Х, П, ИО(С) \rangle, \quad (1)$$

где: S – источник угрозы, т.е. субъект доступа (пользователь (инсайдер), внешний злоумышленник или запущенные ими процессы);

К – оборудование в канале связи (коммутаторы, маршрутизаторы и др.);

Бс, Бх — сервисы безопасности на пути распространения угрозы, соответственно, сетевые и хостовые;

П – протоколы и пакеты;

ИО – информационный объект доступа (в конкретном сетевом сегменте ограничения С).

В соответствии с рекомендуемыми принципами построения архитектуры безопасности сети задается три категории ограничения информации: открытая, конфиденциальная и секретная. Тогда множество информационных объектов ИО (информационные ресурсы конфиденциального, секретного и открытого контуров) в сети представляет собой объединение множеств:

$$ИО = ИО^{о} \cup ИО^{к} \cup ИО^{с}, \quad (2)$$

где $ИО^{о}$ – множество информационных объектов категории «открыто»;

$ИО^{к}$ – множество информационных объектов категории «конфиденциально»;

$ИО^{с}$ – множество информационных объектов категории «секретно».

Множество сегментов сети С также представляет собой объединение множеств:

$$С = С^{о} \cup С^{к} \cup С^{с}, \quad (3)$$

где $С^{о}$, $С^{к}$, $С^{с}$ – подмножества сегментов, в которых хранится и обрабатывается информация, соответственно, с открытым, конфиденциальным и секретным уровнем ограничения;

$$Со = \{c_0 \in [1,К]\}, \quad (4)$$

где К – число сегментов, в которых хранится и обрабатывается информация категории «открыто»;

$$Ск = \{c_к \in [1,N]\}, \quad (5)$$

где: N – число сегментов, в которых хранится и обрабатывается информация категории «конфиденциально»;

$$Сс = \{c_{с\in}[1,M]\}, \quad (6)$$

где: М – число сегментов, в которых хранится и обрабатывается информация категории «секретно».

Множество субъектов доступа, внешних или внутренних, можно рассматривать как источники угроз, под которыми понимается атакующая программа или пользователь, непосредственно осуществляющий воздействие на сетевой сегмент информационной инфраструктуры АПК «Безопасный город». По расположению субъекта доступа относительно атакуемого объекта угрозы подразделяются на внешние и внутренние (внутрисегментные и межсегментные).

Внешние угрозы — это потенциально возможные действия, заключающиеся в поиске и использовании той или иной уязвимости, предпринимаемые: злоумышленником в целях проникновения с удаленного хоста в защищаемую систему, получения прав на удаленный доступ к ресурсам подсистем АПК и хищения данных; удаленным пользователем, имеющим легальные права, пытающимся превысить уровень своих полномочий.

Внутренние угрозы связаны с нарушением принятой политики безопасности: нелегальным поведением пользователя на хосте (ПК или сервере), попытками доступа пользователя к информационным ресурсам, уровень ограничения которых превышает его уровень доступа (попытки сетевых соединений, запуска приложений, реализации запросов к СУБД).

Множество угроз включает в себя подмножества внешних и внутренних угроз:

$$U = U_{вн} \cup U_{внеш} \quad (10)$$

В свою очередь, подмножество внутренних угроз включает в себя подмножества

$U_{m(l)}^{вн}$ и $U_{ml(k)}^{вн}$, где

$$U_{m(l)}^{вн} = \langle S^{k}, К, Б_с, Б_Х, П, ИО^{с}(С^{с}) \rangle \quad (11)$$

Здесь $U_{m(l)}^{вн}$ – угроза информационным объектам категории ограничения «секретно»

($ИО^{с}$) в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем ограничения «конфиденциально» (Бк), обрабатываемой в сегментах с ограничением «конфиденциально» или «открыто» и пытается превысить свои привилегии

$$U_{m(l)}^{вн} = \langle S^{o}, К, Б_с, Б_Х, П, ИО^{k}(С^{k}) \in ИО^{с}(С^{с}) \rangle \quad 12)$$

Угроза информационным объектам категории ограничения «секретно» (ИОс) и «конфиденциально» (ИОк) в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к «открытой» информации (Б0), обрабатываемой в сегментах сети с

«открытым» доступом и пытается превысить свои привилегии.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем:

$$U^{внш} = \langle S^{внш}, К, Б_с, Б_Х, П, ИО(С) \quad (13)$$

Таким образом, получено описание угроз безопасности исследуемого объекта, при этом источниками внутренних угроз являются субъекты и процессы, описываемые множествами S^k, S^0, источниками внешних угроз — субъекты и процессы, описываемые множеством $S^{внш}$.

Множество внешних субъектов доступа – это объединение множеств

$$S^{внш} = S_r^{n\ внш} \cup S_r^{внш} \in [1; R] \quad (14)$$

где $S_r^{n\ внш}$ – внешние пользователи, обладающие правами доступа (авторизованные удаленные участники информационного обмена);

$S_r^{внш}$ – внешние пользователи, обладающие возможностью несанкционированного доступа (неавторизованные участники информационного обмена других сегментов ЕИТКС ОВД);

R – число точек доступа через периметр сети АПК (совокупность инфокоммуникационного оборудования, заключенная в единое кольцо информационного обмена локальной сети и имеющая доступ во внешние сети к другим контурам ЕИТКС ОВД).

Введем множество функциональных индикаторов И – значений контролируемых параметров, с помощью которых фиксируются отдельные события информационной безопасности. Функциональные индикаторы отражают результаты контроля: изменений правил МСЭ; соответствия настроек других сервисов безопасности политике безопасности; изменений привилегий пользователей; системных вызовов; попыток доступа; состояния соединений.

Поскольку одним из эффективных способов идентифицировать угрозу (атаку) является анализ комбинаций поведений, предлагается сопоставить множеству возможных путей распространения атаки множество индикаторов. Тогда признак того, что подозрительная активность является угрозой, может быть оценен числом индикаторов на пути распространения атаки. Для идентификации внутренних атак предлагается использовать два типа индикаторов: системные и сетевые (хостовые), для идентификации внешних вторжений дополнительно использовать индикаторы, отображающие аномальные события на периметре сети АПК.

Зададим множество путей распространения атак :

$$I_p = Q^o + Q^k + Q^c$$

Где Q^o, Q^k, Q^c – число путей распространения атак к узлам в сегментах, в которых хранится и обрабатывается информация с уровнем ограничения, соответственно «открытая», «конфиденциальная», «секретная».

Множество индикаторов является объединением подмножеств:

$$И = И_o^к \cup И_o^c \cup И_к^c \cup И_{пер} \quad (17)$$

где $И_o^к$ – подмножество индикаторов, фиксирующих попытки доступа субъекта с «открытым» уровнем доступа к объекту с уровнем ограничения «конфиденциально»;

$И_o^c$ – подмножество индикаторов, фиксирующих попытку доступа субъекта с «открытым» уровнем доступа к объекту с уровнем ограничения «секретно»;

$И_{пер}$ – подмножество индикаторов, фиксирующих попытки проникновения на периметре.

Заданное множество индикаторов и путей распространения атак позволяет внести дополнительные экспертные знания о количестве событий информационной безопасности в систему построения нечетких продукционных правил.

Предложенное описание модели угроз показывает основные элементы канала несанкционированного доступа к информации, циркулирующей на разных уровнях сетевого инфокоммуникационного взаимодействия, учитывающего показания индикаторов событий информационной безопасности от маршрутизаторов, межсетевых экранов, систем обнаружения аномалий и вторжений. Обозначается подход для создания модели системы защиты информации АПК «Безопасный город».

Таким образом, приведено формализованное построение угроз безопасности АПК «Безопасный город» с позиции теории множеств с учетом сложности, неоднозначности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства. Такое описание является математической основой построения моделей трудно формализуемых процессов информационного противоборства.

Литература

1. Дунин Вадим Сергеевич, Хохлов Николай Степанович Модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город» // Вестник ВИ МВД России. 2011. №4. URL: https://cyberleninka.ru/article/n/model-ugroz-informatsionnoy-bezopasnosti-kompleksnoy-avtomatizirovannoy-intellektualnoy-sistemy-bezopasnyy-gorod (дата обращения: 18.03.2018).

2. Распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р

3. М.А. Шнепс-Шнеппе, С.П. Селезнев, Д.Е. Намиот, В.П. Куприяновский О телекоммуникационной инфраструктуре комплекса «Безопасный город» // International Journal of Open Information Technologies. 2016. №6. URL: https://cyberleninka.ru/article/n/o-telekommunikatsionnoy-infrastrukture-kompleksa-bezopasnyy-gorod (дата обращения: 18.03.2018).

4. Методические рекомендации по построению и развитию АПК "Безопасный город" в субъектах РФ

5. Единые требования к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город».

УДК 338.462, 339.543

РОЛЬ СИСТЕМЫ ЭКСПОРТНОГО КОНТРОЛЯ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ЭКСПОРТА ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ

А.Ю. Терешенкова[1], С.В. Щербич[2]

ЗАО «ЭксКонт», 197374, *Санкт-Петербург, Торфяная дорога, д.* 7*, лит. Ф, Бизнес-центр «Гулливер*-2*», оф*. 726

Раскрывается понятие и сущность экспортного контроля в Российской Федерации в отношении перемещения таких объектов как технологий. Анализируется нормативно-правовая база экспортного контроля в РФ, рассматривают особенности и сложности экспортного контроля при перемещении технологий и при оказании услуг во внешнеэкономической деятельности.

Ключевые слова: Экспортный контроль, лицензирование, внешнеэкономическая деятельность, экспорт технологий, трансфер технологии, ВЭД услуг, несырьевой экспорт.

ROLE OF THE EXPORT CONTROL SYSTEM IN THE SAFETY OF EXPORT OF INNOVATIVE TECHNOLOGIES

A.Yu. Tereshenkova, S.V. Shcherbich

CJSC «Excont», 197374*, St. Petersburg, Torfanaya road,* 7*, lit. F, Business Center "Gulliver*-2*", of.* 726

The article reveals the concept and essence of export control in the Russian Federation with respect to the movement of such objects as technologies. The regulatory and legal framework for export control in the Russian Federation is analyzed; peculiarities and difficulties of export control when moving technologies and when rendering services in foreign economic activity.

Keywords: Export control, licensing, and foreign economic activity, technology export, technology transfer, foreign economic activity services, non-primary exports.

Объём зарубежных продаж российского ПО и услуг по его разработке по данным некоммерческого партнерства «Руссофт», объединяющего отечественных компаний-разработчиков программного обеспечения, ежегодно растет на 10-15 %, в 2017 г. составил примерно $8,5 млрд.; в 2015г. – 7 млрд. долл. [1] В целях обеспечения развития экспорта технологий Президентом РФ было дано поручение сохранить текущие налоговые льготы для IT-компаний, а Федеральным Собранием был принят закон о преференциях отечественного софта, защищающий интересы россиян-разработчиков ПО, ведущими экспортерами из числа которых являются Kaspersky Lab, ABBYY, Parallels, Acronis и пр.

Президент России Владимир Путин в статье от 08.11.2017 «XXV саммит АТЭС в Дананге: вместе к процветанию и гармоничному развитию» назвал основной задачей Азиатско-тихоокеанского экономического сотрудничества «налаживание эффективного сотрудничества по поддержке инноваций».

На встрече в Самаре 7 марта 2018 г. Президент России Владимир Путин заявил, что финансирование программ поддержки инновационного, высокотехнологического экспорта будет увеличено, а также отметил, что у Минпромторга есть программа, которая посвящена поддержке инновационного экспорта.

Инновационный экспорт, передача знаний, включая передачу и распространение технологии от изобретателей к пользователям, является критическим компонент инновационной системы. Международные транзакции позволяют отслеживать рыночную диффузию технологий и инновации через международные границы.

Одним из видов таких международных сделок являются экспортные потоки интеллектуальной собственности, измеряемые по сборам за использование прав интеллектуальной собственности, включая трансграничные роялти и сборы собранных для лицензирования патентованных технологий. Хотя различные налоговые процедуры влияют на лицензионные сборы и модели торговли роялти, доходы от интеллектуальной собственности в целом указывают на то, какие страны производят продукты интеллектуальной собственности с коммерческой стоимостью. Обычно это также соответствует странам и экономикам, имеющим патенты. Не удивительно,

[1]*Терешенкова Анна Юрьевна – кандидат экономических наук, ЗАО «ЭксКонт», Северо-Западный институт управления РАНХиГС, тел.:+7 921 383 4565, e-mail: Atereshenkova@gmail.com;*

[2]*Щербич Сергей Васильевич – кандидат технических наук, ЗАО «ЭксКонт», тел.:+7 800 555 4420, e-mail: scherbich@gmail.com*

что экспортные доходы от использования интеллектуальной собственности по-прежнему сосредоточены в странах - ведущих получателях патентов: США, ЕС и Япония (по данным Управления патентов и товарных знаков США, United States Patent and Trademark Office). В 2016 г. выручка от экспорта за использование интеллектуальной собственности в США составляла 122 млрд. долл.; в ЕС в том же году – 66 млрд. долл., в Японии – 39 млрд. долл. США. Однако, если проанализировать период с 2008 по 2016 гг., то доля США снизилась, а остальная часть мировой доли (за исключением ЕС и Японии) увеличилась более чем в два раза с 6% до 16%. (рис. 1) [2] Таким образом, за последние несколько лет доходы от экспорта интеллектуальной собственности в ЕС и Японии выровнялись, в США рост остановился, а в других странах и регионах эти доходы продолжают расти.

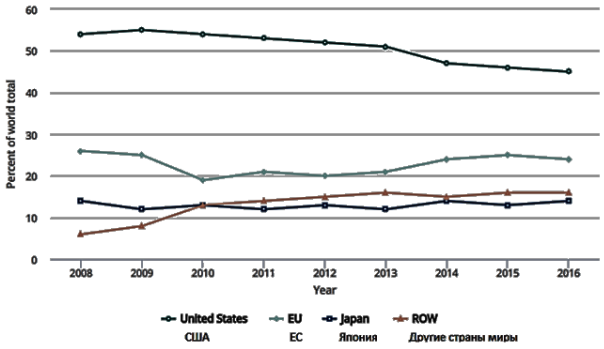


Рисунок 1 – **Экспорт интеллектуальной собственности (сборы за использование) по выбранному региону, стране или экономике:** 2008- 2016 годы, в процентах от общего объема торговли ИС. Источник: Всемирная торговая организация, данные о торговле и тарифах. [6]

Ниже представлены индикаторы международной торговли технологиями характеризующие позицию Российской Федерации на глобальных рынках, отражая конкурентоспособность и технологический уровень российских организаций и технологий, а также масштабы и степень участия страны в глобальных цепочках создания стоимости.

Объемы российского экспорта и импорта технологий по данным Всемирной торговой организации (ВТО) за период 2001– 2015 гг. выросли в 6.9 и в 5.6 раза соответственно, достигнув значений в 2015 г. по объему экспорта 1,7 млрд. долл. и по импорту - 2,2 млрд долл.США (рис. 2). [3] Суммарный оборот экспорта и импорта технологий в России в 2015 г. составил 3.9 млрд долл., увеличившись по сравнению с 2001 г. в 6.1 раза и с 2014 г. — на 3.3%.

Рисунок 2 – **Динамика экспорта и импорта технологий России, по годам, в млн. долл. США** [7]

По сравнению с 2014 г. в 2015 г. поступления от экспорта выросли на 29.4% при одновременном снижении выплат по импорту на 10.2%. Это сократило разрыв, однако не настолько, чтобы изменился характер сальдо: дефицит баланса платежей за технологии в 2015 г., снизившись вдвое, составил 0,6 млрд долл. В экспорте и импорте услуг технологического характера России в 2015 г., как и в предыдущие годы, доминировали инжиниринговые услуги (соответственно 67,2 и 57,9%). Удельный вес соглашений, предметами которых являлись охраняемые объекты промышленной собственности, составил лишь 5,4% экспорта, тогда как в структуре импорта технологий аналогичная величина достигала 19,1%. Следует отметить, что суммарные удельные веса сделок по патентам на изобретения, полезные модели и патентным лицензиям минимальны: соответственно 5% по экспорту и 3,6% по импорту (рис. 3) [3]. Подобные соотношения свидетельствуют о преобладании в торговле технологиями с зарубежными партнерами неохраноспособных объектов (например, промышленные образцы, фирменные наименования или их части, доменные имена и др.).

По данным Росстата за 2016 г. сальдо внешнеторгового баланса по технологиям выросло, сохранив отрицательное значение, наблюдался дефицит равный 1,22 млрд. долл. США (рис. 4).[4, с.58]

[6] Exports of intellectual property (charges for their use), by selected region, country, or economy: 2008–16. Source(s) World Trade Organization, Trade and tariff data. 15 August 2017. See Appendix Table 8-29. Science and Engineering Indicators 2018. Режим доступа: https://www.wto.org/english/res_e/statis_e/statis_e.htm

[7] Расчеты ИСИЭЗ на основе данных федерального статистического наблюдения по форме № 1-лицензия. // Экспресс-информация. Наука. Технологии. Инновация. Краткий статистический сборник. Институт экономики знаний Высшей школы экономики. Выпуск от 07.07.2016. – М.: НИУ ВШЭ, 2016. – 2 с.

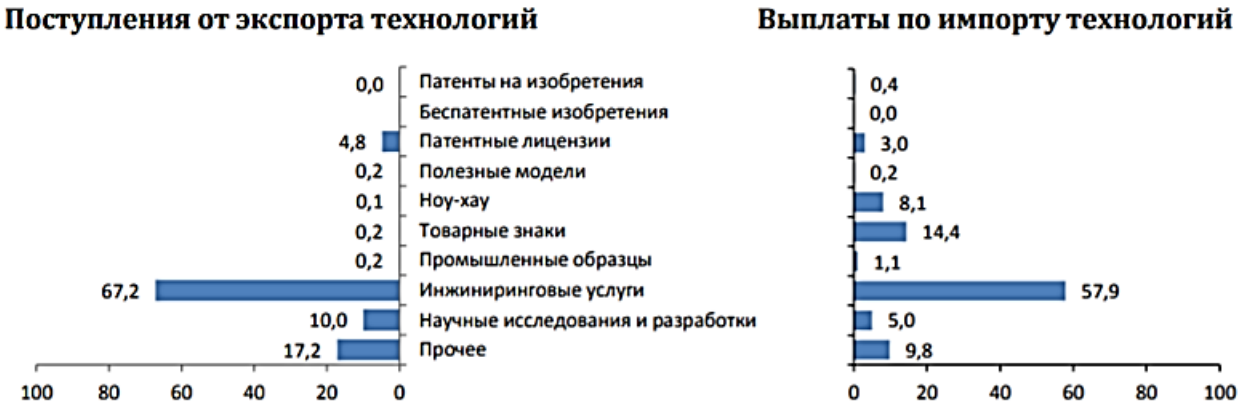


Рисунок 3 – **Структура экспорта и импорта технологий России по категориям соглашений: 2015 (%)**

	Поступления от экспорта технологий	Выплаты по импорту технологий	Сальдо платежей за технологии
Всего по категориям соглашений	**1277.0**	**2498.7**	**-1221.7**
Патенты на изобретения	0.0	5.4	-5.4
Беспатентные изобретения	–	0.1	-0.1
Патентные лицензии	83.1	80.6	2.5
Полезные модели	2.0	1.1	0.9
Ноу-хау	28.7	104.9	-76.2
Товарные знаки	0.9	444.8	-443.9
Промышленные образцы	50.1	10.5	39.6
Инжиниринговые услуги	819.0	1547.9	-728.9
Научные исследования и разработки	140.7	149.1	-8.4
Прочее	152.4	154.5	-2.1

Рисунок 4 – **Баланс платежей за технологии по категориям соглашений: 2016 (миллионы долларов США)**[8].

В течение 2000-х годов (вплоть до 2013 г.) география российского технологического экспорта характеризовалась преимущественной ориентацией на рынки развивающихся стран. При этом доля государств ОЭСР в структуре экспорта технологий устойчиво варьировала на уровне, превышающем 40%. В 2014 г. удельный вес государств ОЭСР достиг 71.0%, в 2015 г. — вновь снизился до 37.5% (рис. 4). [4, с.58] Наиболее значительные объемы российского экспорта приходились на такие государства ОЭСР, как США (319,1 млн. долл.США), Германия (47,2), Нидерланды (32,3) и Франция (20,6 млн.долл.США). Доля стран СНГ в 2015 г. составила 8.1%. [4, с.59] В их числе следует выделить Беларусь и Казахстан (соответственно 79,4 и 27,4 млн.долл.США), наиболее активно приобретавших российские технологии. Среди стран азиатского региона значительные суммы поступлений перечислялись из Китая, Бангладеш и Индии (соответственно 460,3; 207,0 и 85,9 млн.долл.). [4, с.59]

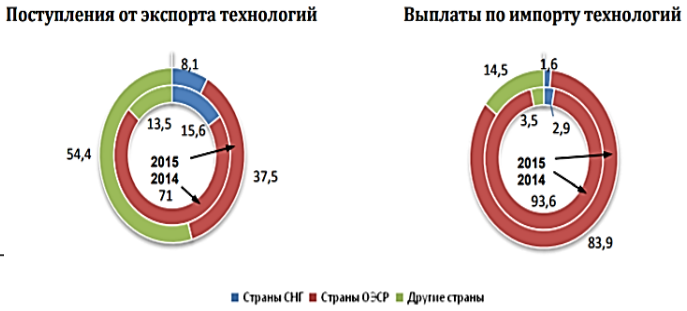


Рисунок 5 – **Структура экспорта и импорта технологий России по группам стран (%).**

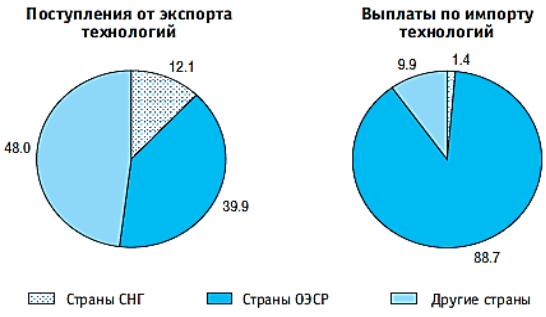


Рисунок 6 – **Структура экспорта и импорта технологий в России по группам стран: 2016 (проценты, %)**[9] [4, с.59]

Государства ОЭСР остаются крупнейшими партнерами России по импорту технологий:

[8] Наука. Технологии.Инновации: 2017: краткий статистический сборник / Н.В. Городникова, Л.М. Гохберг и др.; Нац. Исслед. Ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2017. - С. 58.

[9] Наука. Технологии. Инновации: 2017: краткий статистический сборник / Н.В. Городникова, Л.М. Гохберг и др.; Нац. Исслед. Ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2017. - 59 с.

их доля в 2015 г. достигла 83.9% объема выплат. Значительные суммы транзакций российскими лицензиатами направлялись в Германию (392.6 млн. долл.), США (254.1), Финляндию (196.1), Францию (174.9), Швейцарию (166.5) и Великобританию (138.6 млн долл.).

	Поступления от экспорта технологий	Выплаты по импорту технологий	Сальдо платежей за технологии
Россия	1277.0	2498.7	-1221.7
Великобритания	41060.6	21280.4	19780.1
Германия	71836.5	53734.3	18102.2
Италия	13239.9	12015.7	1224.2
Канада	2620.9	1227.4	1393.5
Республика Корея	10407.9	16409.0	-6001.1
США	130834.0	88891.0	41943.0
Франция	5188.3	3233.5	1954.8
Япония	32631.4	4978.7	27652.6

* Или ближайшие годы, по которым имеются данные.

Рисунок 7 – **Структура платежей за технологии в России по стран: 2016 (миллионы долларов США)10.** [4, с.60]

Т.о. с точки зрения организации внешнеэкономической деятельности все сделки с технологиями и инновациями можно условно классифицировать следующим образом: технологии и инновации в сфере промышленности; технологии и инновации в сфере услуг. Каждую группу которых можно в свою очередь разделить на два раздела, это внешнеэкономические сделки, где есть передача материального предмета (товара, как категории для таможенных целей) и, где нет передачи осязаемого «материального» предмета или носителя информации, т.е. эти сделки имеют «неосязаемый предмет сделки». (см. Табл. 1)

Внешнеэкономические операции (экспортные и импортные), в т.ч. связанные с трансфером технологий или оказанием услуг подлежат экспортному контролю согласно национальному законодательству, принятому на основе международных нормативно-правовых актов и соглашений, таких как Договор о нераспространении ядерного оружия (ДНЯО)[11], Соглашения, принятые в рамках Комитета Цангера [12] и Группы ядерных поставщиков (ГЯП) [13] в отношении установления списка подпадающих под экспортный контроль материалов и оборудования, Режим контроля за ракетными технологиями (РКРТ)[14], Вассенаарские договоренности по контролю за экспортом обычных вооружений и технологий «двойного применения» и др.

	Миллионы рублей	В процентах от общего объема экспорта товаров, работ, услуг
Всего по промышленному производству	863331.5	8.4
Добыча полезных ископаемых	133073.7	4.4
Обрабатывающие производства	730257.7	10.0
Высокотехнологичные	90138.9	28.9
Среднетехнологичные высокого уровня	106572.4	11.6
Среднетехнологичные низкого уровня	421543.8	8.2
Низкотехнологичные	54151.3	9.4
Производство и распределение электроэнергии, газа и воды	–	–
Всего по сфере услуг	55079.2	22.3
Всего по строительству	–	–
Всего по сельскому хозяйству	130.3	0.7

Рисунок 8 – **Экспорт инновационных товаров, работ, услуг в России по видам отраслей:** 2016 (миллионы рублей)[15]. [4, с.71]

[10] Наука. Технологии.Инновации: 2017: краткий статистический сборник / Н.В. Городникова, Л.М. Гохберг и др.; Нац. Исслед. Ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2017. - 60 с.

[11] Российская Федерация является правопреемницей Советского Союза, который подписал ДНЯО в 1968 году. Источник: TREATY ON THE NON-PROLIFERATION OF NUCLEAR WEAPONS (NPT) [Электронный ресурс]. Электрон. дан. URL: http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml. Загл. с экрана (дата обращения 07.11.2013).

[12] Российская Федерация входит в состав Комитета Цангера как правопреемница Советского Союза, который был одним из пятнадцати государств, создавших данную организацию в период 1971 - 1974 годов. Источник: Zangger Committee. History [Электронный ресурс]. Электрон. дан. URL: http://www.zanggercommittee.org/History/Seiten/default.aspx. Загл. с экрана (дата обращения 07.11.2013).

[13] Российская Федерация входит в состав Группы ядерных поставщиков как правопреемница Советского Союза, который стал членом этой организации в 1975 году. Источник: NUCLEAR SUPPLIERS GROUP (NSG). Home [Электронный ресурс]. Электрон. дан. URL: http://www.nuclearsuppliersgroup.org/A_test/01-eng/index.php?%20button=1. Загл. с экрана (дата обращения 07.11.2013).

[14] Российская Федерация присоединилась к Режиму контроля за ракетными технологиями в 1995 году. Источник: Missile Technology Control Regime. MTCR Partners [Электронный ресурс]. Электрон. дан. URL: http://www.mtcr.info/english/partners.html. Загл. с экрана (дата обращения 07.11.2013).

[15] Наука. Технологии.Инновации: 2017: краткий статистический сборник / Н.В. Городникова, Л.М. Гохберг и др.; Нац. Исслед. Ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2017. -71с.

Таблица 1 – **Классификация внешнеэкономических сделок с технологиями и инновациями**

Группы	Виды сделок	Виды государственного контроля при осуществлении ВЭД
1. Технологии и инновации в сфере промышленности		
1.1 Объекты интеллектуальной собственности (могут быть в материальной и «неосязаемой форме»)	1.1.1 Патенты и изобретения	Экспортный контроль, Валютный, Налоговый, Радиационный, Таможенный контроль (последние два применяются, только если ОИС перемещаются на материальном носителе, т.е. имеют материальную форму)
	1.1.2 Беспатентные изобретения	
	1.1.3 Патентные лицензии	
	1.1.4 Полезные модели	
	1.1.5 Ноу-хау	
	1.1.6 Товарные знаки	
	1.1.7 Промышленные образцы	
1.2 Материальные объекты (в материальной форме)	1.2.1 Промышленные образцы	
		Экспортный контроль, Валютный, Налоговый, Радиационный, Таможенный контроль
2.Технологии и инновации в сфере услуг		
Предметы сделки могут быть в материальной и «неосязаемой форме»	2.1.1 Инжиниринговые услуги	Экспортный контроль, Валютный, Налоговый, Радиационный, Таможенный контроль (только если при оказании услуг или выполнении работ есть товары, перемещаемые через таможенную границу)
	2.1.2 Научные исследования и разработки	
	2.1.3 Образовательные услуги и консультирование	

Кроме того, документы для экспорта технологий из России оформляются в соответствии с российскими актами о защите объектов авторского права. Передаваемые ноу-хау, результаты интеллектуальной деятельности, программы, базы данных должны быть защищены международным патентным законодательством, чтобы исключить их незаконное использование. На текущий момент патентование технологических цепочек и решений может производиться либо отдельно для каждого государства расположения контрагентов, либо с регистрацией товарного знака согласно Мадридской системе 1891 г.

В исключительных случаях, когда вывоз продаваемых технологий, образцов, программ, разработок или информации происходит на физическом носителе, подлежащем декларированию, уплате подлежат незначительные сборы за совершение таможенных операций и необходимо подать электронную таможенную декларацию на экспорт. Кроме того, для продажи ПО и др. разработок – компания должна быть зарегистрирована Министерством связи РФ, а продукт – внесен в официальный реестр национального софта, который ведется с 01.01.2016 г. По состоянию на март 2018г. там зарегистрировано 4205 позиций программ и баз данных[16]. [5]

В случаях, если среди предметов сделки нет информации или технологии, передаваемых на материальных носителях информации (бумажные документы, инструкции, отчеты, брошюры, диски, цифровые накопители информации и пр.), то «неосязаемый» экспорт технологий из России не подпадает под таможенное оформление и таможенный контроль. Соответственно, и не возникает обязанность по таможенному декларированию и уплате таможенные платежей. Однако, другие меры государственного регулирования и контроля применяются при совершении внешнеэкономических сделок с «неосязаемой передачей технологий», а именно, меры экспортного, валютного и налогового контроля. Эти же меры применяются при выполнение работ и предоставление услуг российскими компаниями, т.к. данные услуги несут в себе *информационную составляющую*, имеющую нередко ключевое значение.

16 Единый реестр российских программ для электронных вычислительных машин и баз данных. [Электронный ресурс]. Режим доступа: https://reestr.minsvyaz.ru/reestr/?PAGEN_1=209 Дата обращения: 15.03.2018г.

Следует отметить, что при «неосязаемой передачей технологий» за участниками ВЭД сохраняется обязанность по ведению учёта таких внешнеэкономических сделок, согласно Постановлению Правительства РФ от 13.06.2012 г. N 583 «О порядке учёта внешнеэкономических сделок для целей экспортного контроля». В этом Постановлении установлен перечень товаров (вкл. интегральные микросхемы), работ, услуг, сделки с которыми подлежат учету в целях экспортного контроля и за неисполнение этого требования, участники ВЭД подлежат административной ответственности. Также учитываются сделки с работами, услугами и результатами интеллектуальной деятельности, имеющими отношение к перечисленным в Постановлении товарам. Идентификацию передаваемых технологий на предмет отнесения передаваемых технологий к перечню, указанному в Постановлении Правительства РФ от 13.06.2012 г. N 583, должны проводить сами участники ВЭД или уполномоченные идентификационные центры по их обращению.

К сожалению, правила экспорта технологий из России не сформулированы в одном нормативном акте, нормы разбросаны в актах разных ведомств (ФСТЭК, ФТС, Минсвязь, ФС ВТС, Минобороны, ФСБ, Роспатент, ФГБУ «ФАПРИД», ФГБУ ВО «РГАИС»- национального центра медиации).

При этом, запрещены:

- реализация сведений, составляющих государственную тайну;
- поставка нелицензионной продукции с нарушением интеллектуальной собственности правообладателя;
- поставка продукции (технологий) с нарушением требований законодательства об экспортном контроле;
- поставка продукции (технологий) с нарушением законодательства о запретах и ограничений ЕАЭС.

В случаях, если поставка технологий будет проходить таможенное оформления и контроль, то на перемещаемые товары распространяется система запретов и ограничений ВЭД. Сведения, заявляемые декларантом в электронной декларации на товары и прилагаемых к ней документах, подтверждаются особым списком разрешительных документов или лицензий.

При проведении документального таможенного контроля сотрудник таможенного органа обязан, в том числе, убедиться в их подлинности, и в соблюдении, участником ВЭД законодательства об экспортном контроле и мер нетарифного регулирования. В частности, среди таких документов, подтверждающих соблюдение запретов и ограничений, указываемые в графе 44 декларации на товары (ДТ), в целях выполнения требований экспортного контроля и мер нетарифного регулирования, по классификатору выделим [5, с. 16]:

01091 – заключение органа, уполномоченного на ввоз/вывоз шифровальной техники;

01092 – нотификация;

01151 – лицензия на ввоз/вывоз, подлежащих ЭК (ФСТЭК), с передачей права собственности;

01152 – разрешение на транзит товаров, подлежащих ЭК;

01153 – разрешение (подтверждение) на ввоз/вывоз т., подлежащих ЭК (КЭК) – без передачи права собственности;

01154 – заключение идентификационного центра о непринадлежности товара к списку контролируемых товаров (например, Заключение Экс-Конт, ФСТЭК России);

01161 – лицензии на ввоз/вывоз продукции военного назначения (ФС ВТС);

01163 – заключение идентификации о непринадлежности товара к продукции военного назначения (ФС ВТС).

При наличии таможенного контроля уполномоченные должностные лица таможенных органов проводят документальный контроль, в рамках которого осуществляют в числе других операций, предусмотренных ТК ЕАЭС, выявление рисков, содержащихся в профилях риска, доведенных до таможенных органов в бумажном и (или) в электронном виде.

Существующая система таможенного контроля таможенным органом требует обязательного наличия одного из следующих документов:

– идентификационного заключения, составленного российским участником внешнеэкономической деятельности;

– лицензии, разрешения или иного документа, выданных уполномоченным федеральным органом исполнительной власти;

– заключения экспертной организации (требование статьи 24 Закона «Об экспортном контроле» и Пост. Правительства РФ от 13.06.2012 г. № 583 «О порядке учета внешнеэкономических сделок для целей экспортного контроля»).

Автоматизация процедуры проверки подлинности разрешительных документов проводится с применением межведомственных информационных ресурсов, предоставляющих заинтересованному должностному лицу информацию о выданных документах и их содержания. Доступ к такой информации осуществляется с автоматизированного рабочего места должностного лица таможенного органа, осуществляющего таможенное оформление товаров.

Лишь малая доля российских участников ВЭД осведомлена о необходимости идентифика-

ции продуктов интеллектуальной деятельности при перемещении через границу. За идентификацией поставляемых технологий обращаются, по информации независимого идентификационного центра в области экспортного контроля ЗАО «Центра проектов развития промышленности» и ЗАО «ЭксКонт», в основном обращаются, ФГУП, НИИ, крупные корпорации, получившие соответствующие уведомления от специально уполномоченного органа исполнительной власти в области экспортного контроля – ФСТЭК России.

Остальные же участники ВЭД могут столкнуться с предписаниями во время проверок их внешнеэкономической деятельности федеральными службами уже после состоявшегося факта поставки. Несоблюдение закона об экспортном контроле может повлечь за собой как административную, так и уголовную ответственность, а также запрет заниматься внешнеэкономической деятельностью определенный период времени, что негативно скажется на репутации и/или вообще существовании организации. Частично ликвидацию пробелов в знаниях в области экспортного контроля стараются устранить учебные центры, имеющие соответствующие программы.

Т.о. большое число проблем, тормозящих развитие инновационных технологий, и даже отраслей, сконцентрировано в сфере технологий, имеющих двойное применение, а также в области создания интеллектуальной собственности за счет федерального бюджета.

С одной стороны, государство заинтересовано и развивает поддержку высокотехнологичного экспорта, с другой, очень усложнены механизмы государственного контроля внешнеэкономической деятельности с технологиями и инновациями. Наблюдаются внутренние и внешние противоречия нормативной базы потребностям общества и предпринимателей.

Сложность текущей ситуации развития несырьевого экспорта, увеличения объёмов перемещения технологий в различных формах (ПО, обучение, услуги и т.п.) связана с низким уровнем информирования российских участников относительно их прав и обязанностей при перемещении через границу их продукции, которая при работе в сети интернет абсолютно размыта. Особенно при «неосязаемой» передаче информации, которая может происходить как по итогам каких-либо разработок, работ, услуг, так и в процессе, на разных стадиях их выполнения.

Перспектива развития экспорта технологий и высокотехнологичных продуктов заключается в одновременном движении органов власти к снижению бюрократических издержек и повышению информированности и вовлеченности самих участников в процедуры соблюдения законодательства, в том числе, в области экспортного контроля. Постановлением правительства и законом «Об экспортном контроле» установлена возможность участникам самостоятельно выполнять идентификацию своей продукции и технологий, либо обращаться в независимые идентификационные центры, имеющие большой опыт и знания в вопросах проведения идентификации в том числе технологий в самых различных формах – от этапов предварительных разработок проектов, выполнения работ, создания ПО и т.п., до обучения иностранных специалистов работе с экспортируемыми высокотехнологичными продуктами.

Литература

1. Экспорт ПО из России. Материал от 2017.10.04 [Электронный ресурс]. Загл. с экрана. Режим доступа: http://www.tadviser.ru/index.php Дата обращения: 15.03.2018.
2. Exports of intellectual property (charges for their use), by selected region, country, or economy: 2008–16. Source(s) World Trade Organization, Trade and tariff data. 15 August 2017. See Appendix Table 8-29. Science and Engineering Indicators 2018. Режим доступа: https://www.wto.org/english/res_e/statis_e/statis_e.htm
3. Экспресс-информация. Наука. Технологии. Инновация. Краткий статистический сборник. Институт экономики знаний Высшей школы экономики. Выпуск от 07.07.2016. – М.: НИУ ВШЭ, 2016. – 2 с.
4. Наука. Технологии.Инновации: 2017: краткий статистический сборник / Н.В. Городникова, Л.М. Гохберг и др.; Нац. Исслед. Ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2017. – 80 с.
5. Единый реестр российских программ для электронных вычислительных машин и баз данных. [Электронный ресурс]. Режим доступа: https://reestr.minsvyaz.ru/reestr/?PAGEN_1=209 Дата обращения: 15.03.2018г.
6. Терешенкова А.Ю. Актуальные вопросы таможенного контроля при декларировании и выпуске товаров отдельной категории // Научно-образовательный центр «Технологии товароведческой, таможенной и криминалистической экспертизы» Сборник научных работ. Под редакцией Г.Д. Дроздова. Санкт-Петербург, – 2015, - №6. – С. 16-24.
7. Терешенкова А.Ю. Анализ рисков и практика осуществления внешнеэкономической деятельности российскими компаниями // Научное издание «Экономическая наука сегодня». Сборник научных статей/ выпуск № 2: научный журнал. - Минск: БГТУ, – 2014. – С. 256-267.
8. Overview of the State of the U.S. S&E Enterprise in a Global Context // National Science Board/ Science & Engineering Indicators 2018. Режим доступа: https://www.nsf.gov/statistics/2018/nsb20181/assets/1387/overview.pdf Дата обращения: 15.03.2018.
9.

УДК 34.009(100)

ОСОБЕННОСТИ ЗАЩИТЫ НАСЕЛЕНИЯ ПРИГРАНИЧНЫХ ТЕРРИТОРИЙ ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Г.В. Лепеш[1]

Санкт-Петербургский государственный экономический университет (*СПбГЭУ*),
191023, *Санкт-Петербург, ул. Садовая*, 21

В статье рассматриваются перспективы сотрудничества по предупреждение чрезвычайных ситуаций и ликвидация их последствий в приграничных районах РФ, а также проблемы, связанные с необходимостью заключения соответствующих соглашений о пересечении границы и временном нахождении российских и иностранных граждан как на своей, так и на чужой приграничной территории.

Ключевые слова: чрезвычайная ситуация, приграничные территории, сотрудничество, региональные условия, международная ситуация.

FEATURES OF PROTECTION OF THE POPULATION OF BORDER TERRITORIES AGAINST EMERGENCY SITUATIONS

G.V. Lepesh

St. Petersburg state economic university (*СПбГЭУ*),
191023, *St. Petersburg, Sadovaya St.*, 21

В статье рассматриваются перспективы сотрудничества по предупреждение чрезвычайных ситуаций и ликвидация их последствий в приграничных районах РФ, а также проблемы, связанные с необходимостью заключения соответствующих соглашений о пересечении границы и временном нахождении российских и иностранных граждан как на своей, так и на чужой приграничной территории.

Ключевые слова: чрезвычайная ситуация, приграничные территории, сотрудничество, региональные условия, международная ситуация.

В соответствии с Федеральным законом N 68-ФЗ от 21.12.94 г. [1] чрезвычайной ситуацией (ЧС) является "обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей". При этом территорией, на которой складывается ЧС может быть регион, включающий практически любую часть суши, водного или воздушного пространства, расположенных в независимости от административной или государственной принадлежности данного региона.

Так как чрезвычайная ситуация складывается независимо от административной и территориальной принадлежности, то в современном обществе должны быть субъекты, в обязанности которых входит её предупреждение и ликвидация.

В соответствии с Федеральным законом от 30.12.2008 года № 309-ФЗ [2] "*Предупреждение чрезвычайной ситуации* – это комплекс мероприятий, проводимых заблаговременно и направленных на максимально возможное уменьшение риска возникновения чрезвычайных ситуаций, а также на сохранение здоровья людей, снижение размеров ущерба окружающей среде и материальных потерь в случае их возникновения" в том же законе [2] приводится определение *ликвидации чрезвычайно ситуации* –"это аварийно-спасательные и другие неотложные работы, проводимые при возникновении чрезвычайных ситуаций и направленные на спасение жизни и сохранение здоровья людей, снижение размеров ущерба окружающей среде и материальных потерь, а также на локализацию зон чрезвычайных ситуаций, прекращение действия характерных для них опасных факторов.

Осуществление функций в области предупреждения ЧС природного и техногенного характера и гражданской обороны на местах производится управлениями гражданской защиты, которые являются структурными подразделениями Главного управления Министерства РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС России). В общем термин «гражданская защита» включает в себя систему мероприятий, осуществляемых всеми органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и

[1]*Лепеш Григорий Васильевич – доктор технических наук, профессор, зав. кафедрой Безопасность населения и территорий от чрезвычайных ситуаций, СПбГЭУ, тел.:* +7 921 751 28 29, *e-mail*: *GregoryL@ Yandex.ru*

организациями независимо от их организационно-правовой формы, направленных на обеспечение защиты населения и территорий (ЗНиТ) от ЧС природного и техногенного характера, а также от опасностей, возникающих при военных действиях или вследствие этих действий.

Государственная политика в области ГЗ включает совокупность целей, задач, научно обоснованных теоретических положений, правовых, экономических норм и организационных мер, предпринимаемых органами государственного управления всех уровней в области ЗНиТ, предупреждения и ликвидации ЧС в мирное и военное время, а также механизмы по их реализации при природно-техногенной безопасности, причем на всей территории РФ, включая приграничные районы. В приграничных регионах РФ и сопредельных государствах проживают представители почти 50 национальностей. Из 89-ти субъектов РФ 45 представляют приграничные регионы страны. Они занимают 76,6 процента всей территории страны. В них проживает 31,6 процента населения России. Население приграничных районов – 100 тысяч человек.

Как правило любая ЧС имеет свои определенные территориальные границы, не связанные с государственной границей РФ. Очевидно, что проблема предупреждения и ликвидации чрезвычайных ситуаций в приграничных районах РФ связана с необходимостью охраны границы и согласованного действия приграничных субъектов с обоих сторон границы. При этом возникают трудности, обусловленные правилами пограничного режима, установленными с обеих сторон границы.

Главным фактором, обусловливающим специфику приграничья, является его географическое положение. Особую роль проблематика приграничных районов играет для России, имеющей громадный пограничный периметр, который составляют весьма различные по природным, демографическим, экономическим и т.д. характеристикам территории. На сегодняшний день границы, определяющие пределы государственной территории РФ (суши, вод, недр и воздушного пространства), неоднородны. Россия признаёт наличие границ с 18 государствами: Норвегией, Финляндией, Эстонией, Латвией, Литвой, Польшей, Белоруссией, Украиной, Грузией, Азербайджаном, Казахстаном, КНР, Монголией, КНДР, Японией и США, а также частично признанными Республикой Абхазией и Южной Осетией. По текущим данным Россия имеет наибольшее количество стран-соседей в мире. Протяжённость российской границы (без учёта присоединенного в 2014 г. Крыма) составляет 60 932 км[17], в том числе 38 тысяч км морских границ; среди сухопутных границ выделяются 7 тысяч км границ по рекам и 475 км по озёрам.

Основная территория РФ граничит по суше (см. рис.1) с 14 государствами-членами ООН и двумя частично признанными государствами (Республикой Абхазией и Южной Осетией). С Польшей и Литвой граничит только Калининградская область. Небольшой анклав, входящий в состав Брянской области, со всех сторон окружён территорией Белоруссии. На границе с Эстонией существует анклав Дубки.

Рисунок 1 – **Границы России** (общие/сухопутные)

Свободное пересечение границ для граждан РФ (при наличии внутреннего паспорта) предусмотрено со странами Белоруссия, Казахстан и Южная Осетия. За исключением Белоруссии все участки границы разрешается пересекать только на установленных пунктах пропуска с соблюдением всех предусмотренных законом процедур.

Охрана государственной границы производится Пограничной службой ФСБ России в пределах приграничной территории, а также Вооружёнными Силами РФ (войсками ПВО и ВМФ) – в воздушном пространстве и подводной среде. Обустройством пограничных пунктов ведает Министерство транспорта РФ. Однако далеко не все сухопутные границы являются охраняемыми.

[17] Данные Пограничной службы ФСБ РФ

С 1 января 2018 года вступил в законную силу приказ ФСБ России от 7 августа 2017 года № 454 «Об утверждении Правил пограничного режима» [3]. Новые Правила предусматривают въезд (проход) в пограничную зону, временное пребывание и передвижение в ней по документам, удостоверяющим личность, для граждан РФ, причем имеющим при себе документы, подтверждающие такую необходимость. Перечень этих документов установлен Правилами [3]. При пересечении границы с целью предупреждения или ликвидации последствий ЧС как российские, так и иностранные граждане должны иметь при себе документы, предусмотренные международными договорами РФ, регулирующими вопросы упрощенного порядка пропуска (пересечения) государственной границы, сотрудничества в области предупреждения и ликвидации ЧС, определяющие порядок и время нахождения их в пограничной зоне, которая находится на территории, где сложилась ЧС. В частности, правилами пограничного режима [3] предусмотрено пребывание в приграничной зоне РФ «при невозможности своевременно покинуть пределы пограничной зоны вследствие обстоятельств непреодолимой силы… до окончания действия соответствующих обстоятельств при условии уведомления о таких обстоятельствах пограничного органа или ближайшего подразделения пограничного органа, документального и иного достоверного их подтверждения».

Таким образом, предупреждение ЧС и ликвидация их последствий в приграничных районах РФ связана с необходимостью заключения соответствующих соглашений о пересечении границы и временном нахождении российских и иностранных граждан как на своей, так и на чужой приграничной территории.

Распоряжением Правительства РФ от 09.02.2001 N 196-р была утверждении Концепция приграничного сотрудничества в РФ [4], которая направлена на укрепление взаимодействия РФ и сопредельных государств в решении вопросов устойчивого развития приграничных территорий РФ и сопредельных государств, повышения благосостояния населения приграничных территорий РФ и сопредельных государств, укрепления дружбы и добрососедства с этими государствами. Концепцией [4], наряду с другими, поставлена задача создания условий для интеграции систем предупреждения и ликвидации чрезвычайных ситуаций сопредельных государств с целью повышения эффективности реагирования на чрезвычайные ситуации, имеющие трансграничные последствия. Для решения поставленных задач предусмотрено сотрудничество, в том числе, при совместном решении вопросов:

- оказания взаимной помощи в ЧС приграничных территорий РФ и сопредельных государств;
- своевременного взаимного информирования и оказания помощи в предупреждении и ликвидации на приграничных территориях чрезвычайных происшествий природного и техногенного характера;
- содействия в пересечении государственной границы группами специалистов и транспортными средствами для ликвидации последствий чрезвычайных ситуаций природного и техногенного характера.

В концепциях, принятых на региональных уровнях РФ эти задачи реализуются путем:

- создания систем оповещения об угрозе возникновения или о возникновении чрезвычайных ситуаций трансграничного характера;
- проведения совместных учений и других мероприятий, направленных на подготовку к действиям в условиях чрезвычайных ситуаций.

При этом речь идет о сопредельных странах Содружества Независимых Государств (СНГ). В Бишкекской конвенции о приграничном сотрудничестве государств – участников СНГ от 10.10.2008 г. [5] определяется, что приграничное сотрудничество осуществляется преимущественно на основе соглашений между компетентными органами, заключенных в пределах их полномочий с соблюдением законодательства Сторон и норм международного права. Примерно такое же утверждение содержится в ст. 2 Европейской рамочной конвенции о приграничном сотрудничестве территориальных сообществ и властей от 21.05.1980 г. [6]. Этому соответствует и определение, данное в Федеральном законе «Об основах приграничного сотрудничества в РФ» [7], «Соглашения о приграничном сотрудничестве независимо от их формы, наименования и содержания не являются международными договорами РФ». Они могут заключаться приграничным субъектом РФ или несколькими приграничными субъектами РФ. Закон устанавливает три группы субъектов приграничного сотрудничества: 1) РФ в целом; 2) приграничные субъекты РФ, территории которых прилегают к государственной границе России; 3) приграничные муниципальные образования, которые расположены в приграничных субъектах РФ и территории, которые прилегают к российской государственной границе. От имени субъектов приграничного сотрудничества выступают компетентные органы государственной власти и органы местного самоуправления. Концепция делает упор в первую очередь на органах исполнительной власти всех уровней, а также к участникам приграничного сотрудничества добавляет физических и юридических лиц.

Таким образом, приграничное сотрудни-

чество осуществляется в рамках полномочий территориальных сообществ или властей, определяемых внутренним правом каждой из Сторон. Несмотря на кажущуюся законодательную "простоту" на сегодняшний день соглашений между приграничными субъектами в области оказания взаимной помощи в ЧС существует лишь несколько.

Из существующих на сегодняшний день механизмов приграничного взаимодействия наиболее эффективным признается деятельность по типу «еврорегионов». Еврорегионы представляют собой европейскую форму международной интеграции, основанную на тесном сотрудничестве двух или нескольких территориальных образований, расположенных в приграничных районах соседствующих государств Европы, характерной чертой которых является наличие постоянно действующих общих рабочих органов. Ещё одной отличительной чертой еврорегионов является то, что в их пределах фактически устраняются таможенные барьеры и препятствия для перемещения рабочей силы. Подобная форма взаимодействия приграничных территорий становится популярной и в рамках СНГ.

Основной целью создания еврорегионов является объединение усилий приграничных территорий (местных органов власти) для преодоления их относительной отсталости в социально-экономической сфере из-за отдаленности (изолированности) от центра для решения вопросов, направленных на улучшение жизни населения этих территорий.

Концепция межрегионального и приграничного сотрудничества государств – участников Содружества Независимых Государств утверждена Решением Совета глав правительств СНГ от 15 сентября 2004 года, подписанным Азербайджанской Республикой, Республикой Армения, Республикой Беларусь, Республикой Казахстан, Кыргызской Республикой, Республикой Молдова, Российской Федерацией, Республикой Таджикистан и Украиной. Решение вступило в силу для Армении (15.09.04), Беларуси (15.09.04), Казахстана (15.09.04), России (15.09.04), Таджикистана (22.03.05) и Кыргызстана (18.04.05). Республика Молдова заявила о том, что не намерена в дальнейшем участвовать в реализации Концепции[18].

Наряду с вопросами социально-экономического сотрудничества данная концепция предусматривает взаимодействие стран в области предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера.

В соответствии с Соглашением между Правительством Азербайджанской Республики и Правительством РФ о сотрудничестве в области предупреждения и ликвидации чрезвычайных ситуаций от 9 января 2001 года Министерство по чрезвычайным ситуациям Азербайджанской Республики осуществляет тесное сотрудничество с Министерством РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

В целях дальнейшего укрепления и развития сотрудничества, руководствуясь данным Соглашением и Протоколом об активизации сотрудничества между МЧС Азербайджана и МЧС России от 28 марта 2006 года, 28 ноября 2008 года сторонами разработан и утвержден Комплексный план сотрудничества на период 2009 – 2011 годы по основным направлениям деятельности в области предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера, предусматривающий:

– обмен опытом и научно-техническое сотрудничество;

– сотрудничество между подразделениями сторон;

– сотрудничество в рамках международных организаций.

На регулярной основе осуществлялся обмен радиационно-экологической информацией на приграничных территориях **Беларуси** и Россией (ранее и с Украиной).

Областными управлениями МЧС Беларуси разработаны планы взаимодействия при ликвидации возможных трансграничных чрезвычайных ситуаций с Черниговской, Киевской, Житомирской и Ровенской областями Украины, а также Брянской и Смоленской областями России. В них определен порядок оповещения органов исполнительной и распорядительной власти областей и организаций, которые привлекаются для взаимодействия при угрозе или возникновении чрезвычайных ситуаций трансграничного характера, в том числе в период весеннего паводка и пропуска ледохода, связанных с возникновением эпидемий, эпизоотии, крупных аварий (катастроф) на промышленных предприятиях, продуктопроводах, аварий на железнодорожном, автомобильном и водном транспорте с выбросом сильнодействующих отравляющих веществ, а также указаны силы и средства, привлекаемые для ликвидации этих чрезвычайных ситуаций.

Решение о базовой организации в области предупреждения и ликвидации ЧС, было принято главами правительств на встрече в Ялте в мае 2007 года. В 2008 году в Институте переподготовки и повышения квалификации МЧС Беларуси, имеющем статус базовой организации государств – участников СНГ по подготовке кадров в области предупреждения и ликвидации чрезвычайных ситуаций, прошли подготовку 42 специалиста из государств – участников СНГ. В сентябре 2008 года в Национальном детском оз-

[18] нота Посольства Республики Молдова в Республике Беларусь № 476/227 от 18 марта 2008 года

доровительном лагере «Зубренок» (Республика Беларусь) проведен VI Международный слет юных спасателей-пожарных, в котором приняли участие детские команды из 12 стран, в том числе России, **Украины и Азербайджана.** В 2009 году был организован обмен гидрометеорологической и радиационно-экологической информацией между управлениями МЧС России и Украины. Осуществлялось еженедельное взаимное информирование об угрозе возникновения опасных метеорологических явлений, других ЧС между некоторыми областями России и **Кыргызской** республики. В 2010 году были проведены совместные учения МЧС России и Белоруссии.

В 2016 году МЧС **Республики Беларусь** провело реорганизацию ведомственных учреждений образования, в результате чего в Минске путем слияния трех вузов (Командно-инженерного института, Гомельского инженерного института и Института переподготовки и повышения квалификации МЧС РБ) был создан Университет гражданской защиты Министерства по чрезвычайным ситуациям Республики Беларусь, к которому и перешли фактически все обязательства и функции базовой структуры в области организации и проведения научно-исследовательских работ, совместных тренировок и учений Корпуса сил Содружества Независимых Государств для ликвидации последствий ЧС природного и техногенного характера, а также международных конференций.

Основными направлениями деятельности базовой организации по обучению кадров в области предупреждения и ликвидации ЧС являются обучение, подготовка, переподготовка и повышение квалификации кадров по специальности «Предупреждение и ликвидация чрезвычайных ситуаций», разработка, апробация и распространение учебно-методических и научно-исследовательских материалов в данной области, развитие сотрудничества отраслевых учреждений образования и научно-исследовательских организаций, организация инновационной деятельности по наиболее актуальным проблемам обучения кадров, подготовки, переподготовки и повышения квалификации специалистов в области защиты населения и территорий от чрезвычайных ситуаций.

Граница между Россией и **Украиной** была сформирована в советское время, в составе единой державы в 1928 году. В частности, с российской стороны к украинскому государству примыкают Брянская, Курская, Ростовская, Воронежская и Белгородская области. Данное разделение принято обоими субъектами и не вызывает каких-либо дополнительных вопросов уже длительное время. Граница Украины и России долгое время оставалась в неизменном состоянии. Однако в 1954 году по инициативе советских властей в честь памятной даты 300-летия воссоединения братских народов Автономная Республика Крым перешла под управление Украинской ССР. С точки зрения территориального расположения такая передача казалась вполне адекватной и обоснованной. В следующий раз граница Украины и России претерпела изменения в 2014 г, по народной, а не правительственной инициативе.

Ситуация резко изменилась в 2014 году в связи с внутренним конфликтом в Украине на территории Луганской и Донецкой областей. Сложившаяся на территории ситуация сегодня характеризуется как чрезвычайная. Так ее охарактеризовал Кабинет министров Украины в январе 2015 года. В рамках ЧС предусмотрены мероприятия по эвакуации населения. Решение о проведении эвакуации принимают: на государственном уровне – Кабмин, на региональном уровне – областные, городские государственные администрации. В режиме ЧС предусмотрено формирование гражданской защиты, в том числе и на добровольной основе, для проведения больших объемов работ по ликвидации последствий чрезвычайных ситуаций, военных (боевых) действий или террористических актов, а также для проведения восстановительных работ, требующих привлечения большого количества населения и техники. Кроме того, для ликвидации последствий ЧС в соответствии с законом могут привлекаться Вооруженные Силы Украины, другие военные формирования и правоохранительные органы специального назначения, образованные в соответствии с законами Украины. Этим правительство Украины пыталось воспользоваться для решения возникшего политического кризиса, приведшего по факту к самоопределению территорий и образованию пока непризнанных народных республик Донецкой (ДНР) и Луганской (ЛНР). Ситуация до сегодняшнего для остается чрезвычайной, носящей характер военного конфликта между Украиной и самопровозглашенными республиками. На фоне конфликта практически все пограничные взаимоотношения и соглашения по проблемам предупреждения и ликвидации ЧС между Россией и Украиной оказались «заморожены».

Пересечение границы Украины и России происходит через специальные пропускные пункты. Наиболее крупные железнодорожные посты оборудованы в городах Казачья Лопань, Бачевск, Квашино, Тополи и другие. Свои пограничные пункты есть и для автомобильного транспорта. Любые виды контроля на границе регулируются законодательствами двух государств, а также международными нормами. Для обеспечения надлежащей пропускной способности каждая из сторон обязана организовать всю необходимую инфраструктуру и двустороннее сообщение различных видов.

Отношения между Украиной и Россией на политическом уровне с 2014 года сложные, однако на сегодняшний день официальных изменений о правилах въезда на территорию страны озвучено не было, хотя по факту они имеются. По-прежнему, граница Украины и России доступна для пересечения на безвизовой основе. Соглашение о таком режиме было заключено еще в 1997 году. Гражданам РФ на пропускном пункте потребуется российский или заграничный паспорт, а для детей до 16 лет – свидетельство о рождении и при необходимости нотариально заверенная доверенность на выезд. Независимо от способа передвижения все лица, пересекающие границу, заполняют специальные иммиграционные карточки, состоящие из двух частей. Указанная в бланках информация вносится украинскими пограничниками в соответствующую картотеку. При въезде в Украину первая часть карточки передается погранслужбам, а вторая возвращается им же при выезде. Утеря данного бланка является нарушением режима пересечения территории страны.

Фактически, так как карта границы России и Украины существенно изменилась, перед жителями РФ образовались определенные сложности при необходимости поездки в соседнюю страну. Еще в марте 2014 года, когда Украина фактически перекрыла границу, ссылаясь на агрессивную политику РФ, попытки захвата чужой территории и пособничество терроризму. Дополнительное усиление было проведено на границе Луганской и Харьковской областей, то есть в тех регионах, где фактическая ситуация находится на грани гражданской войны.

Граждане России могут находиться на территории Украины в течение 90 дней. При необходимости продления указанного срока придется позаботиться о временной регистрации. Граждане других стран СНГ не имеют возможности въезжать в Украину без загранпаспорта, а жители Туркменистана даже обязаны получить визу. В связи с усложнением политических отношений России и Украины все взаимодействия между ними, в том числе и в отношении ЧС прекращены.

В Республике **Казахстан** разработан и принят План мероприятий по повышению эффективной защиты населения, экономического потенциала общества от воздействия чрезвычайных ситуаций природного и техногенного характера, развитию сил и средств для предупреждения, снижения ущерба и ликвидации их последствий. В соответствии с Законом Республики Казахстан от 5 июля 1996 года № 19-1 «О чрезвычайных ситуациях природного и техногенного характера» страна участвует в международном сотрудничестве в области ЧС природного и техногенного характера.

В соответствии с Соглашением между Правительством Республики Казахстан и Правительством РФ о совместном использовании и охране трансграничных водных объектов от 27 августа 1992 года ежегодно проводится заседание Казахстанско-Российской комиссии по совместному использованию и охране трансграничных водных объектов.

В целях дальнейшего взаимодействия по недопущению чрезвычайных ситуаций в период весеннего паводка происходит взаимообмен информацией прогнозов весеннего половодья. Для этого осуществляются системный сбор и обмен информацией о средней величине снежного покрова, осеннем увлажнении почвы, толщине льда на реках и водохранилищах, а также ежедневного сброса на них, ожидаемых уровнях весеннего половодья на реках и дате очищения ото льда рек и водохранилищ и т. д. Информация прогноза, времени начала и максимума половодья, водности, включая бюллетень постов наблюдения на реках, предоставляется в Оренбургскую область. Аналогичная информация из Оренбургской области России поступает в Актюбинскую область Казахстана.

Акиматом Атырауской области Республики Казахстан и правительством Астраханской области РФ подписан Меморандум о взаимопонимании относительно взаимодействия при оказании помощи людям, морским и воздушным судам, терпящим бедствие на Каспийском море. Для организации взаимодействия по проведению совместных мероприятий и оказанию взаимопомощи пострадавшим на море разработана схема управления взаимодействия с федеральным государственным учреждением администрации морского порта «Астрахань» Морского спасательно-координационного центра РФ и силовыми подразделениями Республики Казахстан.

МЧС **Кыргызстана** также активно сотрудничает с государствами – участниками СНГ в рамках Межгосударственного совета по чрезвычайным ситуациям природного и техногенного характера, Межгосударственного совета по гидрометеорологии и промышленной безопасности.

Необходимо отметить, что вопросы приграничного и межрегионального сотрудничества стоят очень актуально в части экологической безопасности.

В 2015 г Совет Федерации ратифицировал соглашение о сотрудничестве государств-участников СНГ в области предупреждения и ликвидации чрезвычайных ситуаций. Документ был подписан 16 октября 2015 года президентами России, Белоруссии, Казахстана, Армении, Киргизии и Таджикистана. Ранее действовал аналогичный договор от 1993 года. Соглашение предусматривает такие формы сотрудничества как предупреждение и мониторинг ЧС, инфор-

мирование о ЧС, угрожающих соседнему государству.

Кроме того, документ закрепляет упрощенный порядок транзита для спасателей, работающих на ликвидации ЧС в странах-участницах соглашения, в части таможенных и пограничных процедур. Данное соглашение ускоряет и снижает затраты при предоставлении помощи в ЧС на пространстве СНГ.

Соглашение открыто для подписания другими государствами СНГ, которые еще этого не сделали (Молдавия, Азербайджан, Узбекистан, Украина), пока для них действуют положения старого соглашения от 1993 года.

С **Абхазией и Южной Осетией** российские спасатели сотрудничают на основании постановления правительства, которое принимается после запроса о предоставлении помощи от иностранного государства.

Российско-**монгольское** сотрудничество осуществлялось в основном на уровне приграничных контактов по вопросам противодействия трансграничным лесным и степным пожарам. Главным управлением МЧС России по Забайкальскому краю совместно с Государственным агентством по ЧС Республики Монголия проводятся совместные тренировки по упрощённому пересечению государственной границы приграничными противопожарными формированиями двух стран.

Приграничное сотрудничество на **российско-китайском** участке границы имеет многовековую историю. Юридической базой для межрегиональных связей является подписанное10 ноября 1997 года Соглашение между правительствами РФ и КНР о принципах сотрудничества между субъектами России и провинциями, автономными районами и городами центрального подчинения КНР. В 1992 году Госсовет КНР объявил четыре сопредельных с Россией города (Маньчжурия, Хэйхэ, Суйфэньхэ и Хуньчунь) «городами приграничного сотрудничества». С этого времени китайская сторона активно ставит вопрос о совместных «зонах свободной торговли» на границе в районе основных пунктов пропуска. В 1992 году был введен упрощенный порядок пересечения китайско-российской границы. Для облегчения индивидуальной коммерческой деятельности жителей приграничных районов России в феврале1998 года путем обмена нотами заключено российско-китайское Соглашение об организации упрощенного пропуска российских граждан в китайские части торговых комплексов.

Россия и Китай тесно сотрудничают по вопросам предупреждения ЧС и ликвидации их последствий на основании Соглашения между Правительством РФ и Правительством КНР о сотрудничестве в области предупреждения и ликвидации чрезвычайных ситуаций. С 2012 года представители китайского министерства принимают участие в мероприятиях, проводимых МЧС России. В 2015 г. МЧС России и Министерство водного хозяйства Китая заключили соглашение о двухстороннем сотрудничестве в области помощи пострадавшим, действиях при чрезвычайных ситуациях, подготовке сотрудников. В ноябре 2017 г. делегация китайского правительства, провела переговоры с российской стороной о стратегическом партнерстве по линии МЧС. При этом стороны заключили партнерское соглашение сразу в нескольких сферах, так с февраля 2017 года в Китай направляются специалисты МЧС РФ для обмена опытом со своими китайскими коллегами. Также с 2018 года КНР начнет закупку специализированного оборудования, использующегося при тушении пожаров и устранении последствий ЧС. Китайская сторона подтвердила достигнутые 2 ноября договоренности на покупку у России многоцелевых самолетов БЕ-200, при этом расширив контракт на еще четыре авиационные единицы.

Особого внимания заслуживает партнерский договор о производственном содействии, которое предусматривает привлечение оборудования из Китая для малого бизнеса России, осуществляющего деятельность по созданию различной продукции в противопожарной сфере. Так на поставленном китайском оборудовании планируется производить такие экспортные товары, как огнетушители, пожарные щиты, напорные рукава, элементы оснащения спасателей и другие сопутствующие предметы и материалы. В свою очередь Китай на своих территориях начнет производство противопожарной химии, которая будет обслуживать потребности российского МЧС. Обсуждалось также создание объединенного отряда по борьбе с лесными пожарами в приграничной зоне, такое соглашение поможет эффективно бороться с огнем на граничащих территориях России и Китая, а также поспособствует сохранению уникальной фауны Приамурья.

Всего на двухдневной встрече было рассмотрены 42 проекта, связанных с ликвидацией ЧС, из которых только три инициативы обоюдным решением были оставлены для дальнейшей проработки деталей, остальной пакет соглашений был принят в полном объеме.

Среди стран, расположенных у северо-западных границ Россия наиболее активно взаимодействует по вопросам предупреждения ЧС и ликвидации их последствий с **Финляндией и Норвегией.** Сотрудничество осуществляется на площадке ООН, в других международных структурах, а также в региональных форматах на севере Европы и в Арктике, таких, как Совет государств Балтийского моря, Совет Баренцева/Евроарктического региона, Арктический совет, "Северное измерение".

Сотрудничество приграничных регионов является одним из традиционных приоритетов взаимодействия. Так в 1992 году было заключено Соглашение между правительством Российской Федерации и правительством Финляндской Республики о сотрудничестве в Мурманской области, Республике Карелии, Санкт-Петербурге и Ленинградской области. В 2012 году этот документ был заменен на Соглашение между правительством Российской Федерации и правительством Финляндской Республики о содействии приграничному сотрудничеству. На основании договоренностей в целях оперативного реагирования, сотрудничества и оказания взаимной помощи при возникновении лесных пожаров и чрезвычайных ситуаций трансграничного характера Стороны способствуют взаимодействию компетентных органов Сторон при осуществлении совместных мер, направленных на предупреждение стихийных бедствий и техногенных аварий и ликвидацию их последствий на территории приграничных регионов. В соответствии с данным Соглашением учреждена российско-финляндская Межправительственная комиссия по приграничному сотрудничеству.

Сотрудничество с Норвегией затруднялось тем, что с 1970 года существовал территориальный спор о границе между государствами в Баренцевом море. Суть его сводится к тому, что Россия проводила границу вдоль побережья острова Шпицберген, Норвегия полагала, что граница должна находиться равноудалённо от Шпицбергена с одной стороны и Земли Франца-Иосифа и острова Новая Земля с другой. Спор обострился, когда в акватории Баренцевого моря были обнаружены запасы углеводородов. Однако в 2010 г стороны пришли к соглашению, что новая делимитационная линия разделит спорную акваторию на две равные части, в связи с чем был подписали договор «О разграничении морских пространств и сотрудничестве в Баренцевом море и Северном Ледовитом океане»[19]. В настоящее время здесь действует «Соглашение между правительствами государств – членов Совета Баренцева/Евроарктического региона о сотрудничестве в области предупреждения, готовности и реагирования на чрезвычайные ситуации» [8].

На основании данного [8] соглашения «Правительства Королевства Норвегия, РФ, Финляндской Республики и Королевства Швеция, отмечая хорошо налаженное международное взаимодействие в области предупреждения, готовности и реагирования на ЧС договорились развивать данное сотрудничество в целях облегчения оказания взаимной помощи в случае природных или техногенных катастроф в Баренцевом/Евроарктическом регионе, включая предоставление помощи лицам, терпящим бедствие в морском и воздушном пространстве, а также в ЧС, вызываемых воздействием климата в северных регионов, включая прямое приграничное сотрудничество на местном и региональном уровнях в Баренцевом/Евроарктическом регионе в случае возникновения ЧС. В рамках соглашения предусмотрен также обмен информацией и опытом в области предупреждения и управления в ЧС, минимизации и ликвидации их последствий, а также проведения совместных тренировок и учений.

Компетентными органами, ответственными за реализацию соглашения [8] в своих странах определены:

- Министерство юстиции и полиции Королевства Норвегия;
- Министерство РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;
- Министерство внутренних дел Финляндской Республики;
- Министерство обороны Королевства Швеция.

Региональными и местными компетентными органами определены органы управления муниципалитетов, объединенных муниципалитетов и местные правительства, а также административные органы округов и соответствующие государственные органы в составе местных администраций в Баренцевом/Евроарктическом регионе, относящиеся к географическому району, занимаемому следующими политико-административными образованиями:

- в Королевстве Норвегия – губернии Нордланд, Тромс и Финнмарк;
- в РФ – Республика Карелия, Республика Коми, Архангельская область, Мурманская область и Ненецкий автономный округ;
- в Финляндской Республике – провинции Лапландия и Оулу;
- в Королевстве Швеция – губернии Норрботтен и Вестерботтен.

Переход границы в связи с ЧС не может быть осуществлен до получения специального разрешения. В соглашении определены условия пересечения границы группами реагирования, пункты пропуска, действительные документы, удостоверяющие личность гражданина и признаваемые в этом качестве запрашивающей стороной, документы, выдаваемые компетентным органом предоставляющей стороны, подтверждающий полномочия руководителя группы и перечень ресурсов помощи. Членам групп реагирования разрешается носить свою униформу на территории государства запрашивающей стороны.

Договаривающиеся стороны применяют соответствующее национальное законодатель-

[19] Ратифицирован Государственной Думой в 2011 г.

ство и международные обязательства относительно освобождения от таможенных пошлин, других платежей и сборов при ввозе, транзите и вывозе ресурсов для чрезвычайного реагирования с территории договаривающихся сторон. После окончания операции по чрезвычайному реагированию группы реагирования предоставляющей стороны обязаны вывезти с территории государства запрашивающей стороны ввезенные ресурсы помощи, за исключением израсходованных, утраченных или распределенных среди населения, если запрашивающая сторона и предоставляющая сторона не договорились об ином.

Ответственность за оперативное управление в зоне ЧС лежит на компетентном органе запрашивающей стороны, за исключением таких зон, которые могут находиться на территории государства другой стороны. Компетентный орган запрашивающей стороны организовывает и управляет действиями групп реагирования предоставляющей стороны. Члены группы реагирования находятся под юрисдикцией государства предоставляющей стороны в области трудового законодательства и связанных с ним вопросов

Группы реагирования должны иметь ресурсы помощи в количестве, достаточном для ведения автономных действий в зоне ЧС в течение 24 часов. Запрашивающая сторона при необходимости предоставляет группам реагирования дополнительные ресурсы для их дальнейшей работы и обеспечивает надлежащей медицинской помощью, продуктами и помещениями для проживания. При этом запрашивающая сторона не возмещает предоставляющей стороне расходы по оказанию помощи, если они не договорятся об ином. Запрашивающая сторона может в любой момент отозвать свой запрос об оказании помощи. В этом случае предоставляющая сторона имеет право на возмещение уже произведенных ею расходов. Оплата расходов, если таковые будут иметь место, осуществляется в соответствии с существующими процедурами между предоставляющей и запрашивающей сторонами.

Приграничное сотрудничество с прибалтийскими республиками **Литвой, Латвией и Эстонией** по вопросам ЧС на международном уровне определяется рамками ООН, а также в рамках договоров с Белоруссией. Так в Беларуси заключено соглашения с Латвийской республикой об оперативном оповещении о ядерных авариях, обмене информацией и сотрудничестве в области ядерной безопасности и радиационной защиты. Беларусь по российскому проекту строит свою первую атомную электростанцию в Гродненской области, вблизи города Островец (2 энергоблока вступят в строй поочередно в 2019 и 2020 годах). Правительством Литвы из политических соображений принят специальный законопроект, запрещающий импорт белорусской атомной энергии вследствие необоснованных претензий к проекту Росатома.

На региональном уровне в 1996 года в Пылве (Эстония) был создан Совет по сотрудничеству приграничных регионов, в который вошли представители Выруского и Пылвского уездов Эстонии, Алуксненского и Балвского районов Латвии, а также Палкинского, Печерского и Псковского районов Псковской области. Основными задачами Совета являются разработка совместной стратегии приграничного сотрудничества и реализация проектов в вопросах совершенствования инфраструктуры и охраны окружающей среды. Литва ввела визы для граждан России, следующих транзитом через ее территорию. Это решение затрагивает интересы жителей российского полуанклава, Калининградской области. Экономические проблемы у области могут возникнуть также из-за введения визового режима со стороны Польши. Большие надежды на решение визовых вопросов власти Калининградского региона связывают с только что ратифицированной Россией Европейской рамочной конвенцией о приграничном сотрудничестве территориальных сообществ и властей.

На договорной основе Калининградская область взаимодействует с семью воеводствами Польши, четырьмя уездами Литвы и округом Борнхольм (Дания). В 1998 году область присоединилась к многостороннему приграничному сотрудничеству в рамках еврорегиона «Балтика», а три ее муниципальных образования – к работе по созданию еврорегиона «Сауле» (с участием Литвы и Латвии). Во второй половине 90-х годов подписан ряд соглашений по линии межрегионального сотрудничества Калининградской области и Клайпедского, Паневежисского, Каунасского, Мариямпольского уездов Литвы.

С 1 января 2004 года Эстония перешла на жесткий визовый режим, установленный Шенгенским соглашением. Латвия отказалась от упрощенного порядка еще в марте 2001 года. На сегодняшний день приграничное сотрудничество в области предупреждения и ликвидации последствий ЧС со с прибалтийскими республиками затруднено политическими факторами, действующими внутри самих республик.

Япония расположена вблизи восточного побережья азиатского материка на четырех крупных и свыше 3 тыс. мелких островах. Она находится на стыке нескольких тектонических плит, что предопределило повышенную вулканическую и сейсмическую активность в зоне всего архипелага. Высочайшей и одновременно самой красивой вершиной, как известно, является гора Фудзи (иногда не совсем точно именуемая у нас Фудзиямой).. Фудзи – действующий вулкан (последнее извержение состоялось в 1707 году).

Тогда слой пепла, выброшенного на улицы Эдо (современного Токио), достигал 4 см. Вот уже 300 лет вулкан Фудзи безмолвствует, однако в любой момент может «проснуться».Всего в Японии насчитывается более 150 вулканов, в том числе не менее 40 действующих – больше, чем в какой-либо другой стране мира. Наиболее активными из них являются Асама, Михара, Асо и Сакурадзима. Извержения в стране происходят практически ежегодно и зачастую приводят к человеческим жертвам, однако еще большую опасность для ее населения, безусловно, представляют собой землетрясения.

Самое разрушительное землетрясение с точки зрения техногенных последствий произошло 11 марта 2011 года на северо-востоке Японии произошло землетрясение, которое получило официальное название "Великое землетрясение Восточной Японии". Землетрясение подобной силы, по оценкам ученых, происходит в этой стране не чаще одного раза в 600 лет. До этого самым разрушительным землетрясением последнего времени в Японии считалось произошедшее 1 сентября 1923 года. Тогда непосредственно под завалами погибло около 15 тыс. человек, но вспыхнувшие одновременно во многих местах пожары сожгли деревянный город с трехмиллионным населением дотла. Погибло более 140 тыс. человек. Землетрясение вызвало крупнейшее цунами, которое накрыло территорию общей площадью 561 квадратный километр, что соответствует 90% площади 23 специальных районов, составляющих ядро Токио. Стихийное бедствие привело к развитию тяжелой аварии на японской АЭС «Фукусима-1».

Число погибших и пропавших без вести превысило 20 тысяч человек. Около 93% погибших стали жертвами гигантской волны. Ущерб, который нанесло гигантское цунами японской экономике, транспорту и инфраструктуре, не считая затрат, связанных с аварией на АЭС "Фукусима-1" около 215 миллиардов долларов.

Не менее значимый урон нанесен экологии региона. В следствие аварии произошел выброс радиоактивности во внешнюю среду. Радиоактивные вещества были обнаружены в питьевой воде, овощах, чае, мясе и других продуктах. Общий объем выбросов йода-131 и цезия-137 после аварии на АЭС составил 900тыс. терабеккрелей, что составляет 20% от выбросов после Чернобыльской аварии 986 году, который составил 5,2 миллиона терабеккерелей.

ЧС рассматриваются японским руководством как два типа экологической катастрофы: первый непосредственно связан с процессами природного происхождения, а второй представляет собой продукт производственно-хозяйственной деятельности. При этом чрезвычайные ситуации природного характера рассматриваются в качестве стихийно-разрушительных процессов, а техногенного характера как нерациональное использование технического прогресса, наносящего прямой или косвенный ущерб здоровью людей.

Предотвращение ЧС и ликвидация последствий стихийных бедствий, по мнению ВПР Японии, является одним из важнейших направлений деятельности исполнительных органов различного уровня. В стране разработан ряд законодательных актов, направленных на снижение потерь среди населения и сокращение материального ущерба. В первую очередь это «Основной закон по защите от стихийных бедствий», принятый в 1961 году. В соответствии с ним установлен порядок работы субъектов власти, определены обязанности должностных лиц, а также порядок проведения и характер мероприятий по защите от ЧС.

Руководство страны создало общегосударственную трехуровневую систему по предотвращению ЧС – национальный, на уровне префектур и муниципальный. В стране создана развитая нормативно-правовая база по привлечению японских вооруженных сил к решению задач по предотвращению ЧС и ликвидация последствий стихийных бедствий.

На приграничное сотрудничество регионов России и Японии влияет интерес японской стороны к островам Южной Курильской гряды. В 2000 году на государственном уровне была подписана «Программа японо-российского сотрудничества в области развития совместной хозяйственной деятельности на островах Итуруп, Кунашир, Шикотан и Хабомаи». Бывшие жители островов и члены их семей – японские граждане могут посещать острова по упрощенному визовому режиму. Уже много лет существуют безвизовые обмены между сторонами. МИДом Японии организуются курсы японского языка. Объективные сложности связаны с тем, что японцы не признают острова российскими.

Россия и Япония, несмотря на территориальные разногласия сотрудничают в пограничной сфере с целью поддержания стабильности и порядка в их сопредельных акваториях. В современном характере внешней политики Японии заключен целый набор весомых предпосылок для кардинального обновления отношений между нею и Россией. Так в ходе последних встреч на высшем уровне между Японией и РФ установлен ряд договоренностей в области предупреждения террористических угроз, использования природных и морских ресурсов и др. Однако установлению более тесных отношений препятствует установившийся японо-американский альянс, первоначально создававшийся как военное противостояние Советскому Союзу. Несмотря на то, что Япония остается подконтрольна своему «большому союзнику» по сути дела работая по боль-

шей части на него и укрепление его влияния в регионе, в настоящее время развитие связей с Россией японская сторона считает одним из важнейших факторов обеспечения безопасности в прилегающих в Японии районах. В интересах обмена опытом по вопросам прогнозирования, предупреждения и ликвидации последствий землетрясений, цунами и извержений вулканов в сопредельных районах РФ и Японии в феврале 2012 г. в г. Сэндае прошла российско-японская встреча экспертов с участием представителей МЧС России, Росгидромета и РАН.

Сотрудничество между РФ и **США** в области ЧС осуществляется на основе Меморандума о понимании между Правительством Российской Федерации и Правительством Соединённых Штатов Америки о сотрудничестве в области предупреждения и ликвидации ЧС от 16 июля 1996 г. и дополнительного Протокола к нему от 26 июня 2007 г. в рамках двусторонней российско-американской Президентской комиссии. В рамках этого сотрудничества проводятся заседания профильного Совместного российско-американского комитета под председательством Министра МЧС России и заместителя руководителя Федерального агентства по ЧС США (ФЕМА). В ходе заседаний рассматриваются основные направления совместной работы на перспективу, а также ь вопросы комплексного обеспечения безопасности массовых мероприятий, например, Олимпиады 2014 г. в г. Сочи, развития сотрудничества в сфере научного обеспечения работ по преодолению стихийных бедствий с участием Геологической службы США. На сегодняшний день достигнуты договорённости о взаимодействии в подготовке кадров спасательных служб.

В июле 2012 г. прошёл российско-американский симпозиум по проблематике геологических рисков, организованный Минобрнауки России и МЧС России с участием Российской Академии наук, Геологической службы США и ФЕМА, по итогам которого достигнуто соглашение о разработке совместных действий в целях минимизации рисков бедствий в геодинамически опасной зоне между Россией и США, включая территорию Курильских островов, Камчатки, Алеутских островов и Аляски.

В целом сотрудничество между РФ и США в области ЧС развивалось достаточно динамично и позитивно до 2014 г.

Особый статус имеют международные договоренности в области ядерной энергетики и обращения с отходами атомной промышленности. РФ имеет соглашения в области оперативного оповещения о ядерной аварии и обмене информацией о ядерных установках практически со всеми приграничными государствами, заключенные как на государственном, так и на региональном уровнях. Так в сентябре 2015 года на 59-й генконференции **МАГАТЭ** был подписан двухсторонний протокол между госкопорацией "Росатом" РФ и Государственным управлением Королевства Норвегии по ядерной и радиационной безопасности. Под документ подпадают Кольская и Ленинградская АЭС (по четыре энергоблока на каждой), судовые реакторы, хранилища свежего и отработанного топлива, исследовательские реакторы и прочие ядерные установки, находящиеся на всей территории Норвегии, а также в 300-километровой приграничной зоне в РФ. Предусматриваются регулярные учения и консультации. На государственном уровне заключено подобное соглашение с республикой Польша.

РФ последовательно осуществляет сотрудничество по вопросам предупреждения и ликвидации ЧС в рамках Организации объединенных наций (ООН). Одним из направлений сотрудничества в рамках ООН явилось участие РФ в разработке Глобальной платформы по уменьшению опасностей бедствий (ГПУОБ). ГПУОБ реализуется раз в два года в виде форума для обмена информацией, обсуждения последних разработок и знаний и наращивания партнерских связей между секторами, с целью повышения эффективности снижения рисков бедствий, за счет улучшения взаимодействия и координации между заинтересованными сторонами. Первая Глобальная платформа по уменьшению опасности бедствий в 2007 стала крупнейшим международным событием после Всемирной конференции по снижению риска бедствий, которая прошла в Кобе, Япония, в январе 2005 года и где была принята Хиогская рамочная программа действий – 10 летний план по борьбе со стихийными бедствиями. В работе сессии приняли участие государственные деятели, эксперты, ученые, представители международных и общественных организаций из 120 стран.

2-я сессия Глобальной платформы по снижению риска бедствий (июнь 2009 года) проходила в условиях растущей обеспокоенности, связанной с глобальным изменением климата и растущими рисками бедствий. В рамках Глобальной платформы политические лидеры, включая глав государств и правительств, жестко и однозначно заявляли, что снижение риска бедствий играет важнейшую роль при устранении последствий изменений климата, а также в борьбе с ухудшением социальной и экономической обстановки. Приоритетным является включение действий по снижению риска бедствий и адаптации к изменениям климата в базовую политику и программные цели в планах национального развития, а также во вспомогательные стратегии по уменьшению бедности и планы помощи странам. Необходима более высокая готовность к гуманитарным последствиям изменений климата, включая системы раннего оповещения и программы

реализации на местном уровне.

Третья сессия Глобальной платформы по снижению риска бедствий проводилась одновременно с Мировой Конференцией по Реконструкции, в Женеве, в мае 2011 г. Она была открыта Генеральным секретарем ООН Пан Ги Муном. Он обратил внимание на увеличение рисков, связанных с природными катастрофами и призвал государства направлять больше инвестиций в усилия на смягчение последствии землетрясении, наводнении, ураганов и снижению числа их жертв. Было отмечено, что выполнение Хиогской рамочной программы действий на 2005 – 2015 годы помогло добиться заметного прогресса на глобальном, региональном и международном уровне в повышении готовности противостоять вызовам стихийных бедствий.

В работе сессии приняло участие уже более 2600 делегатов, представлявших 168 правительств, 25 межправительственных организаций, 65 неправительственных организаций, Международную федерацию обществ Красного Креста и Красного Полумесяца, местные правительства, парламенты, частный сектор, научные учреждения, гражданское общество и международные организации [4].

Четвертая сессия состоялась в Женеве в мае 2013 года для выработки общего видения и направления решения проблемы снижения риска на последующие 30 лет. Она разработала критические и необходимые рекомендации для подготовки к рамочной программе действий после 2015 года, а также для Третьей Всемирной конференции по снижению риска бедствий в марте 2015 года, где и планировалось принятие новой рамочной программы.

Было отмечено, что экономический ущерб от бедствий за последние 13 лет составляет 2,7 триллионов долларов США, что означает примерно 16,2 миллионов долларов убытков в каждый час, начиная с 2000 года. Подобные финансовые потери неприемлемы. За этот период от бедствий пострадало 2,9 миллиарда человек, в среднем более 650000 человек в день.

На Третьей Всемирной конференции в Сендае (Япония) была принята Сендайская рамочная программа по снижению риска бедствий на 2015–2030 гг., которая является инструментом-преемником Хиогской и вводит ряд новшеств, направленных на управлении рисками бедствий в противовес ликвидации последствий бедствий. Кроме того, значительно расширен охват по уменьшению риска бедствий с целью сосредоточения внимания на природных опасных явлениях и техногенных угрозах, а также связанных с ними экологических, технологических и биологических угрозах и рисках.

Кроме того, в Сендайской рамочной программе сформулировано следующее: необходимость более глубокого понимания риска бедствий во всех его аспектах, связанных с характеристиками воздействия, уязвимости и опасности; укрепление систем управления рисками бедствий, в том числе национальных платформ; ответственность за управление рисками бедствий; готовность к восстановлению по принципу «лучше, чем было»; признание заинтересованных сторон и их ролей; мобилизация учитывающих риски инвестиций для предотвращения появления нового риска; устойчивость инфраструктуры здравоохранения, культурного наследия и рабочей среды; усиление международного сотрудничества и глобального партнерства, а также основанных на информации о рисках политики и программ доноров, в том числе финансовой поддержки и привлечения займов международных финансовых институтов.

Пятая сессия Глобальной платформы по снижению риска бедствий проходила в мае 2017 года в Канкуне (Мексика). Сессия явилась крупнейшим на сегодняшний день форумом, в котором участвовало более 7000 зарегистрированных участников, включая глав государств и правительств, министров, мэров, парламентариев и представителей ооновской системы, межправительственных организаций, местных органов власти, местных сообществ, организаций гражданского общества, коренных народов, групп женщин, детей и молодежи, инвалидов, научных и академических кругов и частного сектора. На сессии была проведена оценка прогресса, достигнутого за последние два года после принятия Сендайской рамочной программы и предоставлена возможность для ускорения осуществления Сендайской рамочной программы, налаживания партнерских связей и укрепления национальных и международных усилий по снижению риска бедствий.

В целях поддержки национальных и местных усилий и содействия коллективному управлению трансграничными рисками на сессии разработаны стратегии, планы работы и механизмы, обеспечивающие анализ по конкретным регионам, директивное руководство, инструменты и укрепление потенциала. Они также служат ориентиром для государственных министерств и заинтересованных сторон из разных секторов в деле осуществления последовательного и основанного на участии многих заинтересованных сторон подхода к снижению риска бедствий, устойчивому развитию и адаптации к изменению климата и способствуют накоплению на региональном уровне информации для мониторинга и отчетности в различных секторах.

В качестве неотъемлемой части усилий по осуществлению Сендайской рамочной программы и Парижского соглашения была выдвинута инициатива по созданию систем мониторинга климатических рисков и раннего преду-

преждения для обеспечения возможности предоставления климатологических услуг в наименее развитых странах и малых островных развивающихся государствах в целях укрепления их потенциала осуществлять ранние предупреждения и принимать эффективные ответные меры.

В период подготовки к сессии Глобальной платформы по итогам конференции по вопросам раннего предупреждения об угрозах разного вида был выработан ряд мер по контролю доступа стран к системе раннего предупреждения, с тем, чтобы они могли отслеживать прогресс в деле выполнения глобальной целевой задачи Сендайской рамочной программы. Кроме того, была сформулирована концепция глобальной системы метеорологического предупреждения в целях разработки системы оповещения, которая предоставит целевым пользователям, в том числе вновь созданному Оперативному кризисному центру Организации Объединенных Наций, а также гуманитарным организациям и частному сектору, возможность получать из авторитетных источников предупреждения о гидрометеорологических угрозах и связанную с этим информацию.

Сотрудничество России с Североатлантическим союзом (НАТО) осуществляется с июня1994 года, когда Россия стала первой страной, присоединившейся к программе НАТО «Партнерство ради мира» (ПРМ) – программе практического двустороннего сотрудничества между НАТО и государствами-партнерами. В мае 2002 года в Риме руководители стран НАТО и Президент Путин подписали декларацию «Отношения Россия–НАТО: новое качество». Был учрежден Совет Россия–НАТО (СРН). НАТО и Россия договорились «работать вместе в областях, представляющих общий интерес, и совместно противостоять общим угрозам и рискам нашей безопасности». СРН помимо сотрудничества в области контроля над вооружениями определил сотрудничество в борьбе с терроризмом и кризисным регулированием. Не смотря на кризис 2008 г. (военный конфликт с Грузией) на встрече в Лиссабоне в ноябре 2010 года, руководители стран НАТО и Президент Медведев договорились вступить в «новый этап сотрудничества, ведущего к подлинному стратегическому партнерству». В частности, НАТО и Россия договорились укреплять сотрудничество в борьбе с терроризмом и пиратством.

Дальнейшее развитие в 2010 г. получило сотрудничество РФ по вопросам взаимодействия при реагировании на ЧС в рамках Совета Россия – НАТО (СРН) и Совета евроатлантического партнерства (СЕАП). В целях координации совместных действий, при оказании взаимной помощи в ликвидации ЧС на постоянной основе осуществлялся обмен оперативной информацией между МЧС России и Евроатлантическим центром координации реагирования на катастрофы НАТО (ЕКЦРК). Так, в период ликвидации ЧС в РФ, связанных с лесными и торфяными пожарами в 2010 г., через ЕКЦРК в страны НАТО передавалась информация о потребностях российских пожарных и спасательных служб в технике, оборудовании и иных материальных средствах, необходимых для ликвидации пожаров и их последствий. На основании этой информации 12 государств – членов альянса предоставили РФ необходимую помощь на двусторонней основе.

В 2012 г. в рамках Специальной рабочей группы по чрезвычайному гражданскому планированию СРН в марте и сентябре 2012 г. были проведены занятия, а в ноябре – семинар по вопросам обеспечения безопасности при проведении крупных международных мероприятий, в том числе Олимпийских игр в г. Сочи в 2014 г., с участием специалистов МЧС России, ФСБ России и Минздрава России, а также экспертов ряда ведущих стран НАТО. В октябре 2012 г. проведен крупный семинар в г. Брюсселе на тему «Стратегические вызовы международному планированию и управлению в ЧС», а в г. Стокгольме – семинар по проблемам массовой медицинской эвакуации. Самым заметным мероприятием в рамках Совета Евро-Атлантического Партнёрства (СЕАП) в области чрезвычайного гуманитарного планирования в 2012 г. стало проведение в ноябре 2012 г. Международного командно-штабного учения по теме: «Обеспечение безопасности крупных международных мероприятий с большим скоплением людей» с участием экспертов из профильных российских ведомств.

В марте 2014 года, необоснованно обвиняя Россию в участии в военном конфликте в Украине НАТО приостановила сотрудничество с Россией практически во всех областях. При этом диалоги и встречи в формате Россия НАТО по текущим отношениям сохраняются.

Выводы[20]**.** Совместная работа по предупреждению и ликвидации трансграничных чрезвычайных ситуаций только начинает налаживаться. Для осуществления приграничного сотрудничества по направлениям деятельности МЧС России имеется необходимая правовая основа [4].

В качестве основной задачи приграничного сотрудничества предусмотрено создание условий для интеграции систем предупреждения и ликвидации чрезвычайных ситуаций сопре-

[20] Отражены в докладе департамента международной деятельности МЧС России за 2016 г.

дельных государств с целью повышения эффективности реагирования на чрезвычайные ситуации, имеющие трансграничные последствия.

В Прибалтийском регионе на сегодняшний день не завершено формирование необходимой правовой базы, так как не подписаны межправительственные соглашения по линии МЧС России с Литвой и Эстонией.

Главным управлением МЧС России по Калининградской области продолжается активное взаимодействие с Литвой, в том числе в части осуществления на регулярной основе обмена информацией о ЧС.

На субъектовом уровне также заключаются международные акты с административными единицами других государств в области предупреждения и ликвидации ЧС, что, в свою очередь, способствует разработке соответствующих планов взаимодействия между территориальными органами МЧС России и спасательными службами иностранных чрезвычайных ведомств.

В настоящее время наиболее активное приграничное сотрудничество в области предупреждения и ликвидации чрезвычайных ситуаций осуществляется с Казахстаном, Монголией, Китаем и Финляндией. В последнее время также активизировалось взаимодействие на приграничном уровне с Республикой Беларусь.

Особое внимание уделяется регулярному проведению учений на приграничном уровне (российско-казахстанские и российско-финляндские пожарно-тактические учения по борьбе с природными пожарами на приграничных территориях, российско-китайские учения по борьбе с наводнениями и паводками, российско-монгольские учения по реагированию на степные пожары и др.), а также совместные тренинги и семинары.

О одним из важнейших аспектов приграничного сотрудничества является оперативное решение вопросов, связанных с пограничными и таможенными процедурами при пересечении границы спасательными формированиями в соответствии с требованиями ООН.

Исходя из необходимости обеспечения безопасности населения на приграничных территориях, представляется целесообразным рассмотреть вопрос об организации в образовательных учреждениях МЧС России курсов языковой подготовки для сотрудников диспетчерских служб, работающих в приграничных регионах непосредственно с обращениями иностранных граждан.

В целом, международное сотрудничество, осуществляемое на приграничном уровне, лежит в русле Концепции внешней политики Российской Федерации и является одним из приоритетов международной деятельности МЧС России до 2030 года.

Значимость приграничного взаимодействия, направленного на эффективное реагирование на ЧС, продиктованы необходимостью обеспечения пояса добрососедства по всему периметру российских границ

Список использованных источников

1. Федеральный закон N 68-ФЗ 21 декабря 1994 года «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=200121&rnd=C007139EFABB22DBA5F31FA4E69F4533&from=194047-0#095191392617188

2. Федеральный закон "О внесении изменений в статью 16 Федерального закона "Об охране окружающей среды и отдельные законодательные акты Российской Федерации" от 30.12.2008 N 309-ФЗ (последняя редакция) http://www.consultant.ru/document/cons_doc_LAW_83309/

3. Приказ ФСБ России от 7 августа 2017 г. № 454 «Об утверждении Правил пограничного режима» ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/71659826/#ixzz58r7vsjJ0

4. Распоряжение Правительства РФ от 09.02.2001 N 196-р <Об утверждении Концепции приграничного сотрудничества в Российской Федерации> http://legalacts.ru/doc/rasporjazhenie-pravitelstva-rf-ot-09022001-n-196-r/

5. Конвенция о приграничном сотрудничестве государств-участников Содружества Независимых Государств заключена в г. Бишкеке 10.10.2008 г. // Бюллетень международных договоров. - 2010. - № 1.

6. Европейская рамочная конвенция о приграничном сотрудничестве территориальных сообществ и властей заключена в г. Мадриде 21.05.1980 г. (Вместе с «Типовыми и рамочными соглашениями, уставами и контрактами о приграничном сотрудничестве между территориальными сообществами и властями») // Собрание законодательства РФ. - 2003. - № 31, ст. 3103.

7. Федеральный закон от 26 июля 2017 г. № 179-ФЗ “Об основах приграничного сотрудничества” http://www.garant.ru/products/ipo/prime/doc/71630188/

8. Соглашение между правительствами государств – членов Совета Баренцева/Евроарктического региона о сотрудничестве в области предупреждения, готовности и реагирования на чрезвычайные ситуации//Электронный фонд/ URL: http://docs.cntd.ru/document/902187674

УДК 13058

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ПЕРИОД ОРГАНИЗАЦИИ ЛЕТНЕЙ ОЗДОРОВИТЕЛЬНОЙ КАМПАНИИ НА ПРИМЕРЕ ГБОУ "БАЛТИЙСКИЙ БЕРЕГ" САНКТ-ПЕТЕРБУРГА

Н. Н. Гордиенко[1], В. Н. Гордиенко[2]

[1]*Санкт-Петербургский государственный университет промышленных технологий и дизайна* (*СПбГУПТД*),191186, *Санкт-Петербург, ул. Большая Морская,* 18.
[2]*Государственное бюджетное нетиповое образовательное учреждение детский оздоровительно-образовательный туристский центр Санкт-Петербурга «Балтийский берег»* (*ГБОУ «Балтийский берег»*), 191119, *Санкт-Петербург, ул. Черняховского,* 49, *лит. А.*

Данная статья посвящена актуальным вопросам обеспечения комплексной безопасности образовательных учреждений.

Ключевые слова: чрезвычайные ситуации, комплексная безопасность, экологическая безопасность, терроризм

FEATURES OF SAFETY ENSURING DURING THE ORGANIZATION OF SUMMER HEALTH-IMPROVING CAMPAIGN ON THE EXAMPLE OF STATE BUDGETARY EDUCATIONAL INSTITUTION "BALTIYSKIY BEREG", SAINT-PETERSBURG

N. N. Gordienko, V. N. Gordienko
Saint-Petersburg State University of Industrial Technologies and Design,
191186, *Saint-Petersburg, Bolshaya Morskaya str.*
State Budgetary Atypical Educational Institution Child Health-Improving and Educational Tourist Center of Saint-Petersburg "Baltiyskiy Bereg", 191119, *Saint-Petersburg, Chernyakhovsky str.,* 49, *lit. A.*

The article is devoted to the actual problems of complex safety ensuring of the educational institutions.

Keywords: emergency situations, complex safety, ecological safety, terrorism.

Важнейший приоритет для каждого человека – жизнь и здоровье ребенка, поэтому одним из условий их сохранения является обеспечение безопасности, создание условий, в которых минимизированы риски травм, заболеваний, гибели детей и молодежи.

Система комплексной безопасности подразумевает состояние защищённости образовательного учреждения от реальных и прогнозируемых угроз социального, техногенного и природного характера, обеспечивающее его безопасное функционирование.

Указом Президента Российской Федерации от 31 декабря 2015 г. N 683 утверждена Стратегия национальной безопасности Российской Федерации [1]. Настоящая Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации.

Безопасность образовательного учреждения – это комплекс мероприятий, направленных на сохранение жизни и здоровья обучающихся и работников, а также материальных ценностей образовательного учреждения от возможных несчастных случаев, пожаров, аварий и других чрезвычайных ситуаций. Практической разработкой вопросов обеспечения безопасности в социальной среде, а также подготовки специалистов, занимающихся организацией досуга и перевозкой детей, занимались такие исследователи как: Воронцова Г.Г., Карпова Г.А., Степанова С.А., Печерица Е.В., Шарафанова Е.Е. и др. [2,3,4].

Безопасность образовательного учреждения включает все виды безопасности, содержащиеся в Федеральном законе «О техническом регулировании» [5] и в первую очередь: пожарную безопасность, электробезопасность, взрывобезопасность, безопасность, связанную с техническим состоянием среды обитания. Система комплексной безопасности подразумевает состояние защищённости образовательного учреждения от реальных и прогнозируемых угроз социального, техногенного и природного характера,

[1]*Гордиенко Наталья Николаевна – кандидат психологических наук, доцент СПбГУПТД, e-mail: nngrd@mail.ru;*
[2]*Гордиенко Валентина Николаевна – заместитель генерального директора по безопасности ГБОУ «Балтийский берег», e-mail: vngrd@mail.ru.*

обеспечивающее его безопасное функционирование.

Приказом государственного автономного учреждения «Федеральный институт развития образования» от 30 июня 2017 г. № 325 ГБОУ «Балтийский берег» присвоен статус экспериментальной площадки ФИРО по теме «Разработка и апробация эффективных моделей и методик организации отдыха и оздоровления детей».

Учреждение принимает участие во всероссийских конкурсах программ, методических материалов организации отдыха и оздоровления детей и молодёжи. Неоднократно становилось победителем. За 2017 год коллективом разработано 43 тематических программы каникулярного отдыха детей; круглогодично реализуется 11 развивающих программ различной направленности. Одним из ключевых направлений развития ГБОУ «Балтийский берег» является рекреационно-оздоровительное (детские оздоровительно-образовательные лагеря: ДООЛ «Солнечный», ДООЛ «Заря», ДООЛ «Молодежное»). В состав многопрофильного учреждения входит также турбаза «Школьная», Спортивная детско-юношеская школа олимпийского резерва, Станция юных туристов, Центр гражданского и патриотического воспитания, Городской опорный центр безопасности дорожного движения, Центр психолого-педагогической коррекции и реабилитации, Оздоровительная санаторная школа-интернат, Автохозяйство.

Важными направлениями в работе по обеспечению требований комплексной безопасности ГБОУ «Балтийский берег» являются следующие: создание безопасных условий деятельности; принятие мер по противодействию террористическим угрозам, проявлениям экстремистского характера; выполнение требований контрольно- пропускного режима; усиление контроля по вопросам безопасности сотрудников, детей, посетителей, проживающих, а также готовности к действиям в случае угрозы или возникновения чрезвычайных ситуаций; создание комфортных условий для работы сотрудников в соответствии с требованиями охраны труда и техники безопасности.

Следует подчеркнуть, что обеспечение безопасности – это планомерная систематическая работа по всему спектру направлений (организационному, информационному, адаптационному и обучающему).

Безопасность ГБОУ «Балтийский берег» является одним из основных направлений деятельности администрации учреждения и педагогического коллектива. Основной целью является создание безопасных условий для организации учебно- воспитательного процесса, а также повышение уровня пожарной и технической безопасности зданий и оборудования. Пока сохраняется угроза терроризма и экстремизма, мы вынуждены принимать меры по предупреждению и профилактике этих проявлений, а также меры по обеспечению безопасности обучающихся, отдыхающих, посетителей и работников.

Воспитание культуры безопасности сотрудников и обучающихся позволяет, при условии системного подхода к её образованию, позитивно влиять на снижение уровня опасных ситуаций и аварийности в среде их обитания, в данном случае – в образовательном учреждении.

Главная задача – научить обучающихся знать и уметь правильно, рационально действовать в различных чрезвычайных ситуациях. На наш взгляд, необходимо методическое сопровождение по данной проблеме, внесение дополнений в программы по обучению мерам безопасности и действиям обучающихся в возможных чрезвычайных ситуациях. В планах воспитательной работы важно предусмотреть комплекс мероприятий, направленных на формирование у обучающихся и воспитанников знаний, умений и навыков действия в случае возникновения пожаров или иных чрезвычайных ситуаций.

Вопросы обеспечения комплексной безопасности включены в должностные обязанности генерального директора ГБОУ «Балтийский берег»; заместителей генерального директора по направлениям деятельности; начальников ДООЛ «Молодежное», ДООЛ «Заря», ДООЛ «Солнечный»; руководителей структурных подразделений учреждения. С 2018 г. введена новая должность заместителя генерального директора по безопасности.

Вопросы обеспечения комплексной безопасности ГБОУ «Балтийский берег» рассматриваются:

- на общем собрании трудового коллектива;

- педагогических советах структурных подразделений учреждения (перед началом нового учебного года);

- заседаниях Совета трудового коллектива, Управляющего Совета Учреждения (один раз в квартал);

- аппаратных совещаниях (один раз в неделю);

- совещаниях при Генеральном директоре учреждения (по мере необходимости).

Особое внимание уделяется обеспечению комплексной безопасности учреждения. В настоящее время разработаны и утверждены:

- Паспорт антитеррористической защищенности ГБОУ «Балтийский берег».

- Актуализированные технические паспорта КСОБ ГБОУ «Балтийский берег».

- Паспорта КСОБ на 35 зданий.

Разработаны, согласованы и утверждены следующие документы:

- Паспорт безопасности мест массового пребывания людей;

- Паспорта безопасности объекта образования.

На объектах ГБОУ «Балтийский берег» организовано выполнение мероприятий по поддержанию КСОБ в рабочем режиме:

- выполнены работы по определению категорий взрывопожарной опасности складских и производственных помещений.

- Установлены и обслуживаются кнопки экстренного вызова полиции.

- Ежемесячно проводится тестирование.

- Оказываются услуги по физической охране с обеспечением контрольно-пропускного режима. Разработаны новые инструкции по контрольно- пропускному и внутриобъектовому режиму.

- Проведена модернизация и дооснащение системы контроля загазованности пищеблока турбазы «Школьная» выводом сигнала на пульт оперативного дежурного Городского Мониторингового Центра Санкт-Петербурга.

- Осуществлен прием извещений о пожаре от пожарной сигнализации на оборудование, установленное в ФКУ «Центр управления в кризисных ситуациях по г. Санкт-Петербургу» на постоянной основе.

- Проведена модернизация системы Автоматической пожарной сигнализации и системы оповещения людей о пожаре. Выполнены работы по монтажу автоматических средств противопожарной защиты, монтажу противопожарных дверей и люков.

- Установлено видеонаблюдение на всех объектах.

- Проводится ежемесячное тестирование автоматической установки пожарной сигнализации на прохождение сигнала в «Городской мониторинговый центр».

- Учреждение оснащено средствами автономного пожаротушения (пиростикерами).

- Вся территория ДООЛ ограждена и обеспечена источниками света.

В настоящее время прорабатываются вопросы обеспечения комплексной безопасности на объектах ДООЛ ГБОУ «Балтийский берег» в 2018 году с учетом рекомендаций комиссий, полученных при проведении обследования и категорирования объектов образования согласно постановлению Правительства РФ № 1235 от 7 октября 2017 г.

В последние годы большое значение уделяется *экологической безопасности.* При осуществлении своей деятельности ГБОУ «Балтийский берег» руководствуется требованиями природоохранного (ФЗ № 7 от 10.01.2002 "Об охране окружающей среды") [6] и санитарного (ФЗ № 52 от 30.03.1999 «О санитарно-эпидемиологическом благополучии населения») законодательства [7].

Получены лицензии на пользование недрами, с целью хозяйственно-питьевого водоснабжения всех ДООЛ. Все скважины приведены в соответствие с санитарными правилами и нормами; оборудованы необходимыми зонами санитарной охраны, с ограничением доступа на их территорию. Организован производственный контроль за качеством воды из скважин: перед каждым заездом детей в лагерь вода исследуется на санитарно-химические и микробиологические показатели. Также, раз в год воду исследуют на радиационно-гигиенические показатели.

Значительный вклад в экологическую безопасность ГБОУ «Балтийский берег» внес при переключении выпуска сточных вод с ручья Смолячков в систему городской коммунальной канализации. В 2016 году канализационно-очистные сооружения, находящиеся на балансе учреждения, были переданы на баланс ГУП «Водоканал».

Немаловажное значение при осуществлении своей деятельности ГБОУ «Балтийский берег» уделяет и отходам производства и потребления, в связи с увеличивающимся потоком детей в лагерях. Разрабатываются новые паспорта на отходы, регламенты по обращению с ними.

Места для временного хранения опасных отходов (отходы I класса опасности: ртутные и люминесцентные лампы) приведены в строгое соответствие с требованиями санитарного и природоохранного законодательства; доступ к ним имеют только специально обученные люди.

В ГБОУ «Балтийский берег» оборудованы места временного хранения обработанных люминесцентных ламп – установлены металлические ящики, хранение отходов осуществляется в закрытых помещениях в заводской картонной упаковке.

Охрана труда – одно из важных направлений деятельности учреждения. Обучение по охране труда, пожарной безопасности, электробезопасности, безопасной эксплуатации лифтов, газовых приборов, энергетических теплоустановок проходят все руководители структурных подразделений и ответственные лица**.** Сотрудники обеспечиваются в соответствии с нормативами обезвреживающими средствами, спецодеждой и спецобувью.

В структуре ГБОУ «Балтийский берег» имеется *медицинская служба*, которая осуществляет свою деятельность на основании лицензии, полученной бессрочно в 2013 году. Медицинская часть соответствует современным требованиям и позволяет проводить широкий спектр профилактических, реабилитационных и лечебных услуг.

Оборудованы: кабинет физиотерапии, водолечебница, галокамера, фотарий, зал ЛФК и аэрофитокомната. В конце 2017 года в ДООЛ «Солнечный» введена в строй 2-я соляная пещера на 17 посадочных мест. Медицинская помощь оказывается круглогодично: учащимся ОСШИ, где обучаются преимущественно часто и длительно болеющие дети, имеющие «букет» хронических заболеваний; подросткам ЦППРК и учащимся образовательных школ Санкт-Петербурга, приезжающим на кратковременные курсы оздоровления.

Большое внимание уделяется организации рационального питания. В 2017 году в соответствии с требованиями СанПиН проведена корректировка цикличного меню по возрастным группам: отдельно для учащихся начальной и средней школы. Разработано 3-х недельное меню на период летней оздоровительной кампании (было 2-х недельное, как в большинстве лагерей Санкт-Петербурга), что позволило сделать рацион смены более разнообразным. При лабораторном контроле за качеством питания Роспотребнадзором, Управлением социального питания в 2017 году проб, не соответствующих гигиеническим нормативам, не было.

Обеспечение безопасности в период организации летней оздоровительной кампании – это комплекс мероприятий, систематическая работа по сохранению жизни и здоровья людей, материальный ценностей от несчастных случаев и чрезвычайных ситуаций.

Невозможно самостоятельно, усилиями одного только учреждения обеспечить безопасность детей, сотрудников, посетителей. Для этого необходимы чёткие продуманные, технически обеспеченные, консолидированные действия различных Комитетов, ведомств, структур. Не все сразу можно решить, жизнь постоянно вносит коррективы. Будем бдительны! Думая о возможной опасности, мы обязаны обеспечить безопасность детям, сотрудникам и гостям.

Список использованной литературы:

1. Стратегия национальной безопасности Российской Федерации [Текст]: от 31 декабря 2015 г. № 683 //www.consultant.ru [дата обращения 29.03.2018].

2. Воронцова Г.Г., Воронцова А.В., Федоров Г.А. Практикум по организации производственных процессов на предприятиях туризма и индустрии гостеприимства: учеб. пособие /Г.Г. Воронцова, Г.А. Федоров. – СПб.: ФГБОУВПО «СПГУТД», 2014. – 157с.

3. Детский и юношеский туризм на сельских территориях: коллективная монография. Под ред. Е. Е. Шарафановой, Е. В. Печерица. /О.В. Архипова, Г.Г. Воронцова и др. – СПб.: Изд-во СПбГЭУ, 2015. – 100 с.

4. Эффективное управление в гостиничном и ресторанном бизнесе: теория, практика, подготовка кадров: коллективная монография. Под ред. С.А. Степановой /Т.В. Бедяева, Г.Г. Воронцова и др. – СПб.: Изд-во СПбГЭУ, 2017. – 175 с.

5. О техническом регулировании [Текст]: федеральный закон: принят 27 декабря 2002 г. № 184-ФЗ // Собр. Законодательства РФ. – 2002.

6. Об охране окружающей среды [Текст]: федеральный закон: принят 10 января 2002 г. № 7-ФЗ // Собр. Законодательства РФ. – 2002.

7. О санитарно-эпидемиологическом благополучии населения [Текст]: федеральный закон: принят 30 марта 1999 г. № 52-ФЗ // Собр. Законодательства РФ. – 2002.

УДК. 640.4-027.45 (571.51)

ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТЕВЫХ ОТЕЛЯХ «HOLIDAY INN»

А.В. Николаев[1]

СПб ГБ ПОУ Российский колледж традиционной культуры,
193230, *Санкт-Петербург, Дальневосточный пр. д.*51.

В статье рассмотрены вопросы обеспечения безопасности в гостиничной сети Holiday Inn. Автор обратил внимание на преимущества и достоинства корпоративной системы обеспечения безопасности сети отелей Holiday Inn. Несмотря на значительную техническую оснащённость, отели мало уделяют внимание обеспечению индивидуальной безопасности клиентов.

Ключевые слова: Безопасность отеля, техническая безопасность, гостиничная сеть Holiday Inn, индивидуальная безопасность клиентов.

SECURITY CHAIN HOTELS "HOLIDAY INN»

A. V. Nikolaev

SPb GB POU the Russian College of traditional culture, 193230, *Saint Petersburg, far East, etc.,* 51.

The article considers the issues of providing security in the hotel chain Holiday Inn. The author drew attention to the advantages and dignity of the corporate security system of the hotel chain Holiday Inn. Despite the considerable technical equipment, hotels pay little attention to the provision of individual customer safety.

Keywords: Hotel security, technical security, hotel chain Holiday Inn, individual customer safety.

Индустрия гостеприимства вынуждена считаться с многими вызовами и угрозами современного общества. Угрозу, возникающие в следствии технических сбоев, человеческого фактора или «информационной интервенции» заставляют переосмыслить методические и технологические подходы к обеспечению безопасности клиентов гостиницы (гостей), персонала и виртуально-информационного пространства гостиничного пространства. Комплексный подход к обеспечению безопасности гостей, персонала и коммерческой составляющей гостиничного предприятия не всегда оказывается эффективным, например, когда возникает угроза террористического акта.

В рамках данной статьи, предпринята попытка критически рассмотреть соответствие уровня безопасности, предъявляемого потенциальными клиентами гостиничного предприятия и возможностью их удовлетворения средствами размещения. В качестве объекта анализа была определена сеть отелей Holiday Inn, так как сетевые гостинцы ориентируются на международные стандарты безопасности и имеют дополнительные возможности для внедрения инноваций в обозначенной сфере.

Научной разработкой темы безопасности гостиничного предприятия занимались известные западные специалисты: Д. Уокер, Р. Браймер, Т. Джум, Ф. Котлер, Ю. Штюрмер и другие [1]. Среди отечественных специалистов отметим М. Пономарева, М. Стрельникова, Е. Филипповского, И. Ляпина, И. Игнатьева, Воронцова Г.Г. [2,3,4], а также С.А. Степанову и Т.В. Бедяеву, которые исследовали вопросы подготовки специалистов индустрии гостеприимства и кадровой безопасности [5].

Основные положения организации безопасности в гостинице формируются на основе положений, зафиксированных в основополагающих правовых документах.

Комплексный подход обеспечения безопасности гостиницы в своей основе рассматривает функциональное назначение эксплуатируемого объекта, далее следует разработка алгоритма возможных чрезвычайных ситуаций и мер противодействия им. Таким образом, эффективность разработанной системы безопасности зависит от выбора современных технических средств и их обслуживания. Приоритет технических средств в обеспечении безопасности в сфере гостеприимства объясняется следующими обстоятельствами:

– большая «износостойкость» в сравнении с человеком, неподверженность усталости, чувствам, погодным условиям;

– неподкупность, сложность обмана, невозможность запугивания;

– реакции, точность выполнения заложенных функций.

[1]*Николаев Андрей Валентинович – кандидат исторических наук, преподаватель колледжа, тел.:* +79312724925; *e-mail: nikolaev_av.63@mail.ru*

Отели сети Holiday Inn подчиняются жестким требованиям и внутренним стандартам безопасности, определяющим их имидж. В Российской Федерации в сеть отелей Holiday Inn входят гостиничные предприятия Москвы, Санкт-Петербурга, Самары, Уфы, Челябинска (всего 9 отелей). С целью установления и поддержания высокого уровня сервиса, стандартизации технологических процессов обеспечения безопасности и разъяснения стратегического влияния на бизнес и опыт работы с гостями компания Intercontinental Hotels Group разработала корпоративную систему обучения. На портале размещены видео- и аудиоматериалы, учебные пособия, требования и стандарты. Техническое обеспечение безопасности в отеле является составляющей Отдела Управления Рисками IHG. Данная структура руководствуется следующими принципами:

– помощь отелям цепи в определении имеющихся рисков;

– снижение последствий возможных происшествий;

– предоставление гарантии о готовности отеля к любым кризисным явлениям;

– поддержка непрерывности процессов;

– снижение финансовых потерь [6].

IHG определяет риск как вероятность возникновения опасности. Под опасностью подразумеваются различные кризисные явления, пожары, воровство, репутация, рентабельность бизнеса и прочее. Области рисков в IHG разделены следующим образом:

– кризис, происшествие, восстановление;

– пожар;

– безопасность;

– безопасность отдыха;

– безопасность питания;

– клиенты & персонал;

– защита персональных данных [6].

Категория Клиенты&персонал подразумевает все риски отеля, связанные со взаимоотношениями клиентов с персоналом, а также обеспечение личной безопасности обеих сторон. IHG принимает все необходимые меры для защиты здоровья, безопасности и благосостояния коллег, гостей, подрядчиков и других «заинтересованных сторон» путем минимизации или устранения рисков до приемлемого уровня с учетом проблем, времени и средств контроля.

Защите персональных данных в IHG уделяют особое внимание. Цель конфиденциальности – доверительные отношения с клиентом и сотрудниками. Все осуществляемые операции должны соответствовать 6 принципам: прозрачность, согласованность, точность данных, сохранность данных, предоставление гарантий, запрет на контакт с третьими лицами.

Таким образом, мы рассмотрели основные принципы обеспечения безопасности в отелях сети Holiday Inn, составляющие элементы корпоративной системы безопасности и категории рисков, требующие особого внимания и контроля.

На сегодняшний день техническое обеспечение любого отеля достаточно высокого уровня представлено камерами видеонаблюдения, датчиками дыма, противопожарными установками, автоматизированными постами охраны. Обеспечением информационной безопасности в отеле как правило занимается IT-отдел. В сфере безопасности его задача состоит в постоянном контроле и оптимизации процессов безопасного доступа к внутренней сети отеля. Кроме того, IT-отдел контролирует работу гостевой сети, решает вопросы безопасности в отношении доступа клиентов и гостей к ресурсам гостиницы.

Руководитель службы безопасности отелей Holiday Inn Moscow lesnaya и Holiday Inn Moscow Suschevsky Е. Филиппов отметил, что названные гостиничные комплексы имеют высокий уровень безопасности имущества личной безопасности гостей. Доступ в номер осуществляется с помощью электронных ключей, для сохранности вещей в каждом номере имеется сейф с персонализированным замком [8]. Приведённое выше мнение считается наиболее распространенным, не вызывающем сомнения в установленном порядке.

Действительно реальную безопасность вполне можно доверить системе электронных замков. В качестве примера можно привести проверенной временем систему электронных замков Ilko Unikan Sistem. Выбор может быть и более разнообразным, так как современные гостиничные предприятия используют различные варианты замков, совмещённых с пластиковой карточкой: тач-мемори, чип-карты, бесконтактные проксимити карты. Подобные технологии позволяют обеспечить безопасность не только гостей, но и персонал.

Принципиальная схема системы контроля доступа сводится к использованию разнообразных турникетов: миниатюрных, высокоскоростных, с высокой степенью секретности и пропускной способностью. Для управления турникетами используются пульты ручного управления, считыватели карточек, радиобрелки, клавиатуры, что дает возможность включать турникеты в число сетевых компьютеризированных систем контроля доступа.

На территории отеля могут использоваться автоматические ворота или шлагбаум, необходимые для оперативного управления потоком автотранспорта и регулирования движения въезда (выезда) на автостоянки. Наличие охраняемой стоянки для автомобиля, также, как и перечисленные средства автоматизации, являются одним из главных достоинств отеля, подчеркивают престиж гостиницы и являются знаком уважения к своим клиентам, которые оставляют автомобили под охраной.

Большое внимание уделяется защите окон, особенно расположенных на небольшой высоте с плохо просматриваемой стороны здания, а также вентиляционных каналов. Для этого используют каркасные и бескаркасные решетки.

Кнопки тревожной сигнализации – необходимый элемент безопасности современного отеля. Для скрытой передачи сигнала тревоги, кнопки тревожной сигнализации монтируют в различных местах отеля, в том числе на стойке администратора, у кассы приема денег в зоне регистрации, у кассы гостиницы, в офисе руководства. Оборудованная устройствами звуковой и визуальной сигнализации, система охранной сигнализации позволяет в случае опасности привлечь внимание персонала. Размещаются ручные сигналы-кнопки в холлах, в коридорах вблизи лестничных клеток и находятся под стеклом, чтобы избежать случайного нажатия.

Безопасность в отелях Holiday Inn обеспечивается не только с помощью служб охраны, технического контроля, но и системой пожарной сигнализации, благодаря использованию эффективного комплекса предупредительных мер. Строгий противопожарный режим установлен в складских, служебных и подсобных помещениях; назначены лица, ответственные за пожарную безопасность в каждом помещении. Программное обеспечение современной системы позволяет определить сигнал тревоги. В отелях регулярно проводится техническое обслуживание систем противопожарной защиты, в частности, системы противодымовой защиты и оповещения посетителей о пожаре, установок пожарной сигнализации, внутреннего противопожарного водопровода. В зданиях отелей сети имеются аварийные выходы и информационные указатели для ориентации в чрезвычайной ситуации. Специалистами разработаны инструкции по пожарной безопасности и памятки для проживающих о соблюдении правил и действиях на случай возникновения пожара, имеется наглядная информация о маршрутах эвакуации, запасных выходах и ближайшей системе пожарной сигнализации, размещен план действий персонала и посетителей отеля в случае пожара.

Таким образом, рассмотрев комплексную систему обеспечения безопасности в отелях Holiday Inn, их техническое оснащение, необходимо отметить, что главным её критерием является надёжность.

Тем не менее, техническая безопасность сети отелей Holiday Inn слабо ориентирована на потребительский сегмент. Ознакомившись с техническим оснащением гостиничных предприятий в сфере безопасности и проанализировав отношение гостей к уровню безопасности в отеле, было выявлено, что корпоративная система обеспечения безопасности сети Holiday Inn статична, не способна гибко реагировать на индивидуальные потребности гостей, хотя и соответствует необходимым требованиям, регламентам, стандартам и прочим нормативным документам в области обеспечения безопасности на гостиничном предприятии.

Система безопасности отелей не обладает никакими принципиальными отличиями от стандартной организации безопасности отелей, что не способствует повышению её конкурентоспособности. В регионах достаточно гостиниц данного потребительского сегмента. Уникальные предложения для комфортного и безопасного пребывания гостей в отелях Holiday Inn могли бы значительно повысить уровень конкурентоспособности и престиж на рынке гостиничных услуг.

Ознакомившись с организацией системы безопасности в гостиничных предприятиях сети Holiday Inn в городах Москва, Санкт-Петербург, Самара, их техническим обеспечением, а также с потребностями гостей, отметим, что ключевую роль должен играть индивидуальный подход,

доступность, понятность и функциональность предлагаемых средств безопасности.

Приведём несколько примеров внедрения и применения технических средств, которые могли бы способствовать распространению индивидуального подхода в системе безопасности отелей.

Датчик StickNFind. Зачастую гости отеля забывают в номерах личные вещи. Обезопасить гостей от потерь, таких как мобильные телефоны, ключи и даже ноутбуки поможет датчик StickNFind. Маленький чип диаметром с 25-центовую монету и весом всего 4,5 грамма будет почти незаметен. Один из шести различных оттенков стикера можно подобрать под дизайн любого предмета. StickNFind просто крепят к нужной вещи. И если вдруг что-то потеряется, об этом уведомит специальный «локатор» в приложении для смартфона [7].

Устройство для поиска и слежения за небольшими предметами работает через встроенный модуль Bluetooth. Липкая пленка на задней поверхности датчика позволяет его легко приклеить на вещь. Следует учесть, что у этой клейкой пленки такая липучесть, что отодрать ее, по крайней мере, первое время, будет очень непросто. Но в этом есть и свои преимущества. Если кто-то с нечистыми намерениями посягнет на собственность гостя, снять чип с поверхности вряд ли получится. Для поиска в запасе будет как минимум пара часов.

Для того, чтобы датчик StickNFind заработал, его нужно настроить. Для этого сначала необходимо установить бесплатное программное обеспечение на планшет или смартфон. Приложение сможет работать с операционной системой iOS и Android версии 4.0 и выше.

Далее датчик следует активировать: постучать по нему и дождаться звукового сигнала из встроенного динамика. Затем присвоить имя и следовать инструкциям, которые появляются на экране. Приложение синхронизирует и обновит прошивку датчика. Производитель гарантирует, что устройство будет работать, по меньшей мере, один год без замены батарейки. Именно поэтому один комплект умных датчиков может использовать несколько сотен постояльцев отеля.

Приложение позволяет задать радиус области, где должен находиться StickNFind, но не более 30 метров. И если вдруг предмет каким-то образом окажется за ее пределами, радар сразу же просигнализирует.

Стоимость одного датчика на сегодняшний день составляет 35-40 $. При относительно невысокой цене и долгосрочности работы на предоставлении StickNFind гостям отеля в качестве дополнительной услуги отель может получить хорошую прибыль.

Owlet Baby Monitor. Путешествие с маленьким ребенком зачастую создает определенные проблемы. Родители вынуждены пристально следить за безопасностью ребенка, его физическим состоянием. Разработанный специально для юных путешественников биометрический гаджет Owlet позволит гостям отеля контролировать состояние их детей и при необходимости вовремя обратиться за помощью.

Owlet Baby абсолютно гипоаллергенный, в нем не используются клеи. Электронные датчики и разные компоненты размещены в водостойком медицинском силиконе. Поэтому ребенок будет надежно защищен от любого электрического воздействия [7].

Данный прибор может стать незаменимым помощником гостей с маленькими детьми.

Прибор надевается на ребенка и беспрерывно контролирует следующие показатели:

– температура тела;

– температуру кожи (датчик дает представление как температура в комнате влияет на малыша – жарко ему или холодно);

– частота сердечных сокращений (самой важной мышцы в организме человека);

– измеряет и записывает уровень кислорода в крови (показывает, насколько хорошо дышит ребенок);

– следит за качеством сна (свободный доступ воздуха к органам дыхания, и чтобы рот и нос малыша случайно не накрыло одеялом).

Родители будут постоянно получать уведомления о самочувствии своего ребенка. Сигнал тревоги оповестит их в том случае, если сердцебиение ребенка замедлилось или наоборот участилось, появилось затрудненное дыхание, а также в целом ряде других ситуаций.

Данные о состоянии ребенка передаются на смартфон со специально установленным приложением при помощи Bluetooth 4.0 или же через USB, подключенным к компьютеру. Но самым удобным способом будет Wi-Fi, в этом случае родители смогут наблюдать за состоянием ребенка на любом подключенном к Интернету устройстве.

Кроме контроля за состояние здоровья ребенка родителям такой прибор даст массу других преимуществ: хороший сон, меньше стрессов и больше спокойствия.

Миниатюрная универсальная сигнализация Cavius Nano. Среди гостей Holiday Inn часто встречаются семейные пары с детьми и бизнес-туристы. Для обоих сегментов потребителей свойственен повышенный интерес к личной безопасности. В связи с потребностями основных целевых групп отеля в качестве дополнительной услуги может быть предложена универсальная сигнализация Cavius Nano. Она предназначена для установки в ограниченном пространстве, обитатели которого хотят обезопасить себя от проникновения злоумышленников, возможных пожаров и прочих проблем, которые приходят внезапно.

Параллельно система отслеживает уровень освещения при помощи оптических сенсоров. Если до них доходит слишком мало света, а уровень свободных ионов в воздухе одновременно достигает установленного порога, устройство подает световой сигнал и испускает звук, громкость которого с расстояния 3 м составляет 85 дБ.

Эти же компоненты могут использоваться и для других целей. В частности, Cavius Nano может отреагировать на внезапно открытую дверь или появление в помещении человека, если таковое не планировалось.

Чипы Linen Technology Tracking. Практически ежедневно гостиница сталкивается с проблемой кражи полотенец, халатов и прочих тканевых предметов из номеров. Подсчитано, что каждый месяц из оборота выходят 20-30 % полотенец, из них 3% приходится на кражи. Сократить расходы на закупки возможно путем пресечения краж предметов собственности гостиницы. Американская компания Linen Technology Tracking изобрела чипы, которые пользуются популярностью у многих отелей. Чип имеет круглую форму размером с пуговицу, вшивается в постельное белье, полотенца, халаты. В случае если данные предметы окажутся за пределами номера, горничная получит тревожный сигнал с указанием номера, именем постояльца.

Разработчики также позаботились о стирке белья. Чипы Line tracker выдерживают 300 стирок, что является вполне хорошим показателем и подтверждает целесообразность использования.

При формировании каждого предложения учитывались результаты опроса среди гостей. Ориентированность на потребности клиента позволит сделать пребывание гостей в отеле более комфортным и безопасным.

Мы привели всего несколько возможных вариантов, позволяющих повысить индивидуальную безопасность гостей сети отелей Holiday Inn, имеющей необходимые материальные ресурсы. Понятно, что в отношении каждого отеля подобные тактические и стратегические мероприятия должны решаться отдельно, но индивидуальный подход к обеспечению безопасности гостей также необходим, как и разработка корпоративных правил, стандартов и регламентов.

Литература

1. Уокер, Дж.Р. Управление гостеприимством [Текст]: учебник для вузов / Дж.Р. Уокер. - М.: Юнити-Дана, 2006. - 880 с.
2. Игнатьев, И.М. О роторных турникетах, как средствах безопасности. / И.М. Игнатьев // Охранные системы - 2004. - №2 - С. 22-26
3. Ляпина, И.Ю. Организация и технология гостиничного обслуживания [Текст] / И.Ю. Ляпина. - М.: Академия, 2005. - 176 с.
4. Воронцова Г.Г., Воронцова А.В., Федоров Г.А. Практикум по организации производственных процессов на предприятиях туризма и индустрии гостеприимства: учеб. пособие /Г.Г. Воронцова, Г.А. Федоров. – СПб.: ФГБОУВПО «СПГУТД», 2014. – 157с.
5. Эффективное управление в гостиничном и ресторанном бизнесе: теория, практика, подготовка кадров: коллективная монография / под ред. С.А. Степановой /Бедяева Т.В., Воронцова Г.Г., Жукова С.С. и др. – СПб.: Изд-во СПбГЭУ, 2017. – 175 с.
6. IHG Intercontinental Hotels Group: [Электронный ресурс] // IHG – глобальная гостиничная компания, 1996-2015. URL: http://www.ihg.com/hotels/ru/ru/reservation.
7. GRIDDER: [Электронный ресурс] // Новостной интернет-портал, 2015-2017. URL: http://gridder.ru/mobility/datchik-sticknfind-pomozhet-otyskat-propavshuju-veshh/.
8. GRIDDER: [Электронный ресурс] // Новостной интернет-портал, 2015-2017. URL: http://gridder.ru/technologies/zdorove-malysha-pod-kontrolem/.
9. Филиппов, Е. Безопасность превыше всего: [Электронный ресурс] // Интернет-портал АБТ- ACTE Russia, URL: http://www.businesstravelrussia.ru news /news-abt/bezopasnost-prevyshe-vsego/

УДК 334

УГРОЗЫ И РИСКИ В ДИСТРИБЬЮТЕРСКОЙ ДЕЯТЕЛЬНОСТИ

Е.В. Печерица[1], А.А. Низовцев[2]

[1]*Санкт-Петербургский государственный экономический университет*, 192007, *Санкт-Петербург, ул. Прилукская, д.*3.
[2]*ООО «Продстар – Торговый Дом»*, 197374, *Санкт-Петербург, улица Стародеревенская, дом* 13 *Литер "А", помещение* 2*Н.*

В статье рассматриваются основные виды рисков и угроз в дистрибьютерской деятельности.
Ключевые слова: угрозы, риски, экономическая безопасность, дистрибьютерская деятельность

THREATS AND RISKS IN THE DISTRIBUTION BUSINESS

E. V. Pecheritsa, A. A. Nizovtsev

The article considers the main types of risks and threats in the distribution business
Keywords: threats, risks, economic security, distribution activities

Российское законодательство не регулирует дистрибьютерскую деятельность, положений о данном виде деятельности не содержится ни в Гражданском Кодексе Российской Федерации (далее — ГК РФ), ни в иных нормативно-правовых актах. Но так как в соответствии с п. 2 ст. 1, п. 1 ст. 421 ГК РФ граждане и юридические лица свободны в заключении договора как предусмотренного, так и не предусмотренного законом или иными правовыми актами, дистрибьюторский договор является правомерной правовой конструкцией, которую широко используют и на территории Российской Федерации.

Сложность заключается в том, что однообразия в российской судебной практики по данному вопросу нет.

Понятие дистрибьютерской деятельности достаточно лаконично сформулировано в Постановлении ФАС Московского округа от 08.10.2002 N КА-А40/6725-02: «дистрибьютор не является потребителем товара, поскольку покупает товар не для удовлетворения личных нужд, а для его перепродажи в пределах оговоренной территории (рынка)».

Согласимся с мнением авторов Рубец К.Ю., Возисов К.А. [1] о том, что дистрибьютерский договор может:

1. быть квалифицирован как агентский;
2. быть квалифицирован как договор на организацию отношений по поставкам продукции с оказанием услуг по поиску покупателей;
3. квалифицироваться как смешанный договор поставки и агентирования;
4. регулироваться нормами гл. 30 ГК РФ о договоре купли-продажи;
5. квалифицироваться как смешанный договор, включающий элементы коммерческой концессии.

При ведении хозяйственной деятельности в любом бизнесе существуют угрозы и риски.

Рассмотрим дефиниции понятия «риск» и «угроза» в таблице 1.

Т. о. под риском будем понимать ситуацию, связанную с наличием выбора из предполагаемых альтернатив, с помощью оценки вероятности наступления рискосодержащего события, влекущего как положительные, так и отрицательные последствия, то есть вероятность генезиса отрицательных и нежелательных последствий.

Угрозу можно определить следующим образом: предполагаемая опасность или совокупность условий и факторов, создающая опасность жизненно важным интересам личности, общества и государства.

Классифицировать риски и угрозы можно по следующему принципу:

1. Экономические угрозы и риски (Причины возникновения *экономических угроз* чаще всего кроются не в самой экономике, а в других сферах, например, на колебания цен и курсов валют могут влиять политические события, погодно-климатические явления, демографические и социальные

[1]*Печерица Елена Васильевна – доцент кафедры экономической безопасности, доцент, тел.:* +7 962 684 77 34, *e-mail:* helene8@yandex.ru

[2]*Низовцев Алексей Александрович – генеральный директор, учредитель ООО «Продстар – Торговый Дом», тел.:* +7 911 967 9470, (812) 438-16-16, 438-16-00; e-mail: baza@prodstar.ru

процессы и т.п., угрозы невыполнения партнерами своих договорных обязательств могут быть вызваны, например, болезнью или смертью собственника, ключевых работников организации, и другими обстоятельствами, не являющимися свойствами данных экономических отношений и ситуаций. *Риски* рынка: изменение рыночной конъюнктуры; утрата рынков сбыта; утрата конкурентных преимуществ и конкурентоспособности; и т.д., финансовые риски: ослабление финансового состояния; потеря платежеспособности; снижение финансовой ликвидности; усиление финансовой зависимости; снижение финансовой устойчивости и т.д.);

Таблица 1 – **Дефиниции понятия «риск» и «угроза» современных авторов**

Риск	
Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»	Возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере в связи с реализацией угрозы экономической безопасности
Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»	Риск в области экономической безопасности - возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере в связи с реализацией угрозы экономической безопасности
Кравчук А.А. Категории «вызов», «опасность», «угроза» в теории национальной безопасности [2]	Вероятность причинения ущерба тому или иному объекту обеспечения безопасности, которая может изменяться в зависимости от конкретных условий обстановки
Угроза	
ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения в ред. от 19.01.2011	Совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности
Кравчук А.А. Категории «вызов», «опасность», «угроза» в теории национальной безопасности [2]	Действие или последовательность событий, которые могут кардинально ухудшить качество жизни населения страны за относительно небольшой промежуток времени
Вилисова А.С. Понятие и классификация рисков и угроз экономической безопасности [5, с.9]	с точки зрения безопасности – это совокупность факторов и условий, способствующих реализации опасности для конкретного объекта в определенный момент или интервал времени
Кунцман М.В. Экономическая безопасность: учебное пособие [6, с.12]	резкие изменения курса национальной валюты, мировых цен, уменьшение иностранных инвестиций, условий внешней торговли, увеличить долю сырья в экспорте продукции, большой внешний долг
Экономическая безопасность. Под общ. ред. Л.П. Гончаренко, Ф.В. Акулинина [4]	возможность наступления событий с отрицательными последствиями в результате определенных решений или действий

2. Социальные угрозы и риски (*Социальные угрозы:* ограничение демократических прав и свобод, распространение терроризма, утрата моральных ценностей, массовая безработица и обнищание населения, безнравственность, массовые эпидемии, смертельные болезни, межэтнические конфликты, войны. С*оциальные риски*: снижение жизненного уровня населения; ослабление трудовой мотивации; рост социальных конфликтов и т.д. [10]. Нормативно-правовые риски: коррупция, рост экономической преступности, рост теневой экономики, криминализация экономики, снижение правовой защищенности, изменение нормативно-правовой базы [11], административно-политические риски: режим санкций, ухудшение политической обстановки; изменение институциональных условий и гарантий для хозяйственной деятельности; смена руководства, принципов экономической политики и т.д.);

3. Экологические риски и угрозы (*Угрозы* - природные катастрофы, изменение климата [11], ухудшение состояния природной среды и загрязнение биосферы; аварии и катастрофы антропогенного и техногенного характера. *Риски* - изменение требований экологических стандартов и санитарных норм и правил и т.д.);

4. Ресурсно-технические риски и угрозы (*Угрозы:* сбои в поставках энергоносителей, «утечка умов», утечка капитала за рубеж, сворачивание научных исследований и разработок;

распад научных коллективов; усиление сырьевой зависимости. *Риски:* старение материально-технической и технологической базы; разрушение производственно-технического потенциала; снижение квалификации научно-технического персонала; нестабильное обеспечение ресурсами; и т.д. [11]).

К *угрозам* деятельности дистрибьютеров в современной России можно отнести:

- сложность таможенных правил, «специфика» импортных закупок и логистики в стране;
- нестабильность курса доллара;
- неоднозначность правил внутри рыночного регулирования, в том числе в области требований и технических регламентов;
- очень большая территория страны и распределенность внутренних рынков сбыта, а также специфика каждого из них;
- разнообразие «бизнес-схем», используемых дистрибьютерами и их клиентами: от многовариативности во взаиморасчетах до долгосрочных кредитов «под честное слово».

К *рискам* в дистрибьютерской деятельности можно отнести:

1. Сбой в поставках от производителя или их полное прекращение, снижение качества продуктов, получаемых от поставщика.

Для минимизации риска сбоя в поставках дистрибьютер может провести SWOT-анализ деятельности производителя и возможности эффективных продаж на региональном рынке его продукции еще до заключения дистрибьютерского соглашения, также можно проверить финансовую надежность партнера. После заключения соглашения данные действия следует периодически повторять;

2. Низкая доходность предпринимательской деятельности, к данному виду риска следует относить низкий уровень продаж и высокие издержки
3. Недостаток оборотных средств.
4. Высокая текучесть кадров в организации, кадровые проблемы.
5. Избыток неликвидной продукции на складах и нехватка ликвидной продукции.

Возникновение рисков последних четырех проблем можно попробовать уменьшить следующим комплексом мер:

- постоянное проведение анализа рентабельности, которое должно приводить к исключению низкорентабельных позиций (например, продукции, клиентов, поставщиков, подразделений самой компании и т.д.);
- стремление к постоянной работе с издержками (иногда следует сокращать производство, затраты на персонал, логистику, административные расходы, минимизировать налоги и т.д.);
- совершенствование коммерческих условий поставок от производителя (бонусы, отсрочки платежей, скидки, сервис и т.д.);
- развитие дистрибьютерской компании таким образом, чтобы она стала надежным каналом сбыта продукции для поставщиков, для получения наиболее выгодных условий при покупке товара (цена, бонусы, премии и т.д.);
- обеспечение дистрибьютером логистики от производителя до конечного потребителя;
- использование условий консигнации, для существенного улучшения ситуации с оборотным капиталом для дистрибьютера;
- предоставление возможности производителю самому отслеживать наличие товара на складе дистрибьютера, для снижения риска затаривания неликвидными товарами и нехватки ликвидной продукции, для чего следует добиваться снижения дебиторской задолженности и максимально возможно отпускать продукцию на условиях предоплаты;
- более тщательно изучать покупательский спрос, взаимодействовать с производителем в более активном рекламном и PR-продвижении его продукции;
- необходимость контроля и анализа действий партнёров, клиентов, конкурентов, сотрудников. Например, если оптовые покупатели часто запрашивают срочную отгрузку, значит, у них постоянно возникают сложности с управлением запасами; если же дистрибьютера постоянно просят об отсрочке – у покупателя существуют серьезные проблемы с оборотными средствами.

6. Риски, связанные с конкурентами. Для снижения данного типа рисков, необходимо совершенствовать внутренние бизнес-процессы, повышать эффективность получения оперативной информации о текущем спросе на продукцию, оперативно и как можно полнее доводить до производителя информацию об изменении конъюнктуры рынка, для принятия производителем мер по повышению конкурентоспособности поставляемой им продукции, стимулированию спроса на нее.

7. Риски, связанные с отношениями с кредитными организациями. Данный тип рисков одинаков для всех компаний, использующих заемные средства [10], соответственно их минимизация производится стандартными методами:

- ресурсы, полученные в кредит, должны быть максимально долгосрочными, дифференцированы по видам валюты и по кредитным учреждениям;
- товар следует застраховать от всех требуемых рисков (как минимум, на складах и дальних перевозках);
- анализ доходности / расходности должен проводиться по принципу profit center или центра прибыли, являющегося самостоятельным филиалом или подразделением компании, которое учитывается на отдельной основе при расчете прибыли. Центр прибыли отвечает за получение собственных результатов и прибыли, и поэтому его менеджеры обычно имеют полномочия по принятию решений, связанных с ценообразованием на продукт и операционными расходами.

Центры прибыли имеют решающее значение для определения того, какие подразделения являются наиболее и наименее прибыльными в рамках организации;

- взвешенное принятие решений о получении кредитов.

Квалифицированные действия каждой из сторон бизнес-союза «производитель-дистрибьютор» и их партнерское взаимодействие позволяет минимизировать риски деятельности дистрибьютора и обеспечить его долговременную эффективную работу в этом качестве.

8. При работе с крупными сетевыми клиентами, особенно высоки риски, связанные с проблемной дебиторской задолженностью большого числа контрагентов (торговых точек).

9. Риски, связанные с невозможностью прогнозирования глубины падения спроса и, в следствие этого невозможность прогнозирования объема закупок у производителей, ведущее в свою очередь к невыполнению плана и неполучению бонусов. Последние 2 вида рисков ведут к:

−разбалансированности всей цепочки сбыта: производитель — дистрибьютер — контрагент, что в свою очередь, порождает задержку поставок, снижает качество продукта и т.д.

−увеличению давления со стороны проверяющих и особенно налоговых органов.

−Снижения данных видов рисков возможно следующими путями:

−грамотное планирование, заключающееся в разработке нескольких планов-сценариев развития событий: пессимистический, реалистический и оптимистический, учитывающие возможное сокращение объема продаж, сокращение собственных издержек, в т.ч. складских площадей, персонала, расходов на маркетинговую деятельность и т.д.

−постоянная, а не только во время кризиса, оптимизация расходов задолго до начала кризиса, используя, например, аутсорсинг, применяя на складах адресную систему складирования и наборка товара, что позволяет значительно увеличить скорость и качество наборки накладных, привлекая к работе кладовщиков с более низкой заработной платой и низкой квалификацией без 100% знания ассортимента;

−пересмотр ассортиментного портфеля, чистка товарных позиций (SKU), сделан ABS-анализ, в следствие которых можно отказаться от плохо продающейся продукции и снизить складские и финансовые издержки;

−расширить в прайс-листах ассортимент «антикризисных продуктов», например, дешевых круп и макарон.

Важнейшими механизмами снижения рисков и угроз в дистрибьютерской деятельности является постоянный анализ внешней и внутренней среды и аргументированная стратегия компании [7,8]. Для чего существует ряд известных маркетинговых инструментов, таких как:

-SWOT-анализ, разделяющий факторы и явления на четыре категории: Strengths (Сильные стороны), Weaknesses (Слабые стороны), Opportunities (Возможности) и Threats (Угрозы);

- PEST анализ;

- модель 5 сил Майкла Портера;

- GAP анализ;

- матрица Анзоффа;

- матрица бостонской консалтинговой группы BCG;

- ABC анализ и др.

Литература

1. Рубец К.Ю., Возисов К.А. Правовое регулирование дистрибьюторских отношений в РФ. URL: http://www.inmarlegal.ru/press/publications/korporativnoe_pravo_m_a_bankovskoe_i_nalogovoe_pravo/pravovoe_regulirovanie_distrib_yutorskih_otnoshenij_v_rf/pravovoe_regulirovanie_distrib_yutorskih_otnoshenij_v_rf/ (дата обращения 23.03.2018).
2. Кравчук А. А. Категории «вызов», «опасность», «угроза» в теории национальной безопасности // Вестн. Забайкал. гос. ун-та. 2016. Т. 22. № 11. С. 65—74.
3. Кротов М.И., Мунтиян В.И. Экономическая безопасность России: Системный подход / М.И. Кротов, В.И. Мунтиян. – СПб.: Изд-во НПК «РОСТ», 2016. – 336 с.
4. Экономическая безопасность: учебник для вузов / под общ. ред. Л. П. Гончаренко, Ф. В. Акулинина. — М.: Издательство Юрайт, 2017. — 478 с.
5. Вилисова А.С. Понятие и классификация рисков и угроз экономической безопасности // Современные научные исследования и инновации. 2017. № 11 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2017/11/84656 (дата обращения: 11.01.2018).
6. Кунцман М.В. Экономическая безопасность. Учебное пособие. — М.: МАДИ, 2016. — 152 с.
7. Шарафанова Е.Е. Стратегическое планирование развития туристских организаций и гостиничных комплексов. монография / Е.Е. Шарафанова; Санкт-Петербургский государственный университет сервиса и экономики. Санкт-Петербург, 2005. — 276 с.
8. Абдалов А.М., Шарафанова Е.Е. Методические аспекты оценки рисков предпринимательской деятельности в области сельского туризма. Теория и практика сервиса: экономика, социальная сфера, технологии. 2014. № 1 (19). С. 140-145.
9. Безденежных Т.И. Стратегические риски и угрозы экономической безопасности. В сборнике: Экономическая безопасность: стратегические риски и угрозы III Межвузовская научно-практическая конференция с международным участием: сборник статей. под ред. Т.И. Безденежных, Р.В. Дронова, В.В. Шапкина. 2016. С. 8-12.
10. Курушина Е.В. О закономерностях экономической динамики в период кризиса. Проблемы современной экономики. 2014. № 2 (50). С. 105-109.
11. Дюжилова О.М., Вякина И.В. Анализ рисков и угроз экономической безопасности региона. Региональная экономика: теория и практика. 2015. 14 (389). С. 53-64.

ТРЕБОВАНИЯ
К МАТЕРИАЛАМ, ПРИНИМАЕМЫМ ДЛЯ ПУБЛИКАЦИИ В НАУЧНО-ТЕХНИЧЕСКОМ ЖУРНАЛЕ «ТЕХНИКО-ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ СЕРВИСА»

К публикации принимаются материалы научно-технического содержания по актуальным проблемам техники и технологии сервиса машин, приборов и инженерных систем жилищно-коммунального хозяйства, бытового обслуживания, дизайна, экологии, личного и общественного транспорта, не предназначенные для публикации в других изданиях.

Материалы, публикуемые в журнале, должны обладать несомненной новизной, относиться к вопросу проблемного назначения, иметь прикладное значение и теоретическое обоснование и быть оформлены по соответствующим правилам (см. http://unecon.ru/zhurnal-ttps).

Материалы для публикации должны сопровождаться: электронной версией статьи, представленной в формате редактора MicrosoftWord (CD-R, CD-RW, DVD или отправленные по e-mail).

Статья должна содержать следующие реквизиты:

• индекс универсальной десятичной классификации литературы (УДК);

• название статьи на русском и английском языках;

• фамилию имя отчество автора (авторов) полностью с указанием должности, звания, телефона и электронного адреса;

• полное наименование организации с указанием почтового индекса и адреса;

• аннотацию из 10 – 30 слов на русском и английском языках;

• 3 – 7 ключевых слова или словосочетания на русском и английском языках;

• текст статьи (8 – 15 страниц (14 пт.), номера страниц не указываются) на русском языке;

• литература (библиографические ссылки даются в конце текста в порядке упоминания по основному тексту статьи, в тексте в квадратных скобках указывается порядковый номер). Внутритекстовые, подстрочные и затекстовыебиблиографические ссылки (списки литературы) должны оформляться в соответствии с ГОСТ Р 7.0.5 – 2008 «Библиографическая ссылка. Общие требования и правила составления».

Статья представляется в электронном виде (на электронном носителе или высылается электронной почтой по адресу:GregoryL@yandex.ru.

При оформлении статьи должны соблюдаться следующие требования.

При наборе текста используется шрифт TimesNewRoman. Интервал текста кратный, без дополнительных интервалов. Лишние пробелы между словами не допускаются. Форматирование текста (выравнивание, отступы, переносы, интервалы и др.) должно производиться автоматически.

Иллюстрации представляются в графических редакторах MSWindows. Все иллюстрации сопровождаются подрисуночными подписями (не повторяющими фразы-ссылки на рисунки в тексте), включающими номер, название иллюстрации и при необходимости – условные обозначения.

Рисунки выполняются в соответствии со следующими требованиями:

• масштаб изображения – наиболее мелкий (при условии читаемости);

• буквенные и цифровые обозначения на рисунках по начертанию и размеру должны соответствовать обозначениям в тексте статьи;

• размер рисунка – не более 15х20 см;

• текстовая информация и условные обозначения выносятся из рисунка в текст статьи или подрисуночные подписи.

Иллюстрации (диаграммы, рисунки, таблицы) могут быть включены в файл текста или быть представлены отдельным файлом.

Все **графики, диаграммы** и прочие встраиваемые объекты должны снабжаться числовыми данными, обеспечивающими при необходимости их (графиков, диаграмм и пр.) достоверное воспроизведение.

Формулы должны быть созданы в редакторе формулMSEquation. Защита формул от редактирования не допускается. Формулы следует нумеровать в круглых скобках, например, (2). Величины, обозначенные латинскими буквами, а также простые формулы могут быть набраны курсивом. Все латинские буквы в формулах выполняются курсивом, греческие и русские – обычным шрифтом, функции – полужирным обычным.

Термины и определения, единицы физических величин, употребляемые в статье, должны соответствовать действующим национальным или международным стандартам.

На последней странице рукописи должны быть подписи всех авторов. Статьи студентов, соискателей и аспирантов, кроме того, должны быть подписаны научным руководителем.

Редакция не ставит в известность авторов об изменениях и сокращениях рукописи, имеющих редакционный характер и не затрагивающих принципиальных вопросов.

Итоговое решение об одобрении или отклонении представленного в редакцию материала принимается редакционным советом и является окончательным.

ISSN 2074-1146

Журнал зарегистрирован
в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Свидетельство о регистрации средства массовой информации –
ПИ № ТУ 78-01571 от 12 мая 2014 г.

Журнал входит в Российский индекс научного цитирования
http://elibrary.ru/title_about.asp?id=28520

Электронная версия журнала расположена по адресу:
http://unecon.ru/zhurnal-ttps
Подписной индекс в каталоге «Журналы России» –95008.

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Технико-технологические проблемы сервиса

№4(42)/2017

Подписано в печать 30.03.2018 г. Формат 60 x 84 1/8. Бумага офсетная. Гарнитура TimesNewRoman.
Печать офсетная. Объем 13,25 п.л. Тираж 500 экз. Заказ № 407

Адрес издателя и типографии: 191023, Санкт-Петербург, Садовая ул., д. 21
Отпечатано на полиграфической базе СПбГЭУ.