2. Уголовный кодекс Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп. от 6 июля 2016 г.) // Собр. законодательства Рос. Федерации. 1996. № 25. Ст. 2 954.

3. Никольская С.А. Преступления, посягающие на пожарную безопасность: автореф. дис. … канд. юрид. наук. Тамбов, 2005. С. 14–15.

4. О пожарной безопасности: Федер. закон Рос. Федерации от 21 дек. 1994 г. № 69-ФЗ (с изм. и доп. от 23 июня 2016 г.) // Собр. законодательства Рос. Федерации. 1994. № 35. Ст. 3 649.

5. Стахов А.И. Организационно-правовые основы обеспечения пожарной безопасности в России: дис. … канд. юрид. наук. М., 2011. С. 22, 27–28.

6. Кодекс Российской Федерации об административных правонарушениях от 30 дек. 2001 г. № 195-ФЗ (с изм. и доп. от 6 июля 2016 г.) // Собр. законодательства Рос. Федерации. 2002. № 1 (Ч. 1). Ст. 1.

7. Технический регламент о требованиях пожарной безопасности: Федер. закон от 22 июля 2008 г. № 123-ФЗ (с изм. и доп. от 3 июля 2016 г.) // Собр. законодательства Рос. Федерации. 2008. № 30 (Ч. I). Ст. 3 579.

8. Об утверждении правил пожарной безопасности на судах внутреннего водного транспорта Российской Федерации: Приказ Минтранса Рос. Федерации от 24 дек. 2002 г. № 158 (в ред. от 22 апр. 2003 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об утверждении правил пожарной безопасности на железнодорожном транспорте: Приказ МПС РФ от 11 нояб. 1992 г. № ЦУО-112 (в ред. Приказа МПС Рос. Федерации от 6 дек. 2001 г. № 47). Доступ из справ.-правовой системы «КонсультантПлюс».

О СОСТОЯНИИ И НАПРАВЛЕНИЯХ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР РОССИЙСКОЙ ФЕДЕРАЦИИ

А.Д. Катаржнов, кандидат технических наук, доцент.
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики.
С.Б. Хитов.
Санкт-Петербургский университет ГПС МЧС России.
О.Г. Смирнова, кандидат юридических наук, доцент.
Санкт-Петербургский университет МВД России

Рассмотрено состояние и направления развития нормативного правового и нормативного регулирования защищенности критической информационной инфраструктуры Российской Федерации, обеспечения устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры Российской Федерации.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, ключевая система информационной инфраструктуры, автоматизированная система управления производственными и технологическими процессами, нормативно-правовой акт, законодательство

STATUS AND TRENDS OF IMPROVEMENT OF LEGAL REGULATION OF SAFETY CRITICAL INFRASTRUCTURE OF THE RUSSIAN FEDERATION

A.D. Katarzhnov.
Saint-Petersburg national research university of information technologies, mechanics and optics.
S.B. Khitov. Saint-Petersburg university of State fire service of EMERCOM of Russia.
O.G. Smirnova. Saint-Petersburg university of the Ministry of internal affairs of Russia

The state and directions of development of normative legal and regulatory protection of Critical Information Infrastructure of the Russian Federation, to ensure sustainability of its functioning, the development of mechanisms for the detection and prevention of information threats and mitigation of their manifestations, increased protection of citizens and territories from emergency situations caused by information and technical impact on objects of Critical Information Infrastructure of the Russian Federation.

Keywords: information security, critical information infrastructure, a key information infrastructure system, automated manufacturing and process control system, normative legal act, legislation

В настоящее время перед нашей страной сохраняет особую остроту реализация угроз информационной безопасности посредством проведения компьютерных атак на государственные информационные системы и ресурсы, число которых, как уже отмечалось [1], значительно растет.

В подписанной Президентом Российской Федерации обновленной Доктрине информационной безопасности среди национальных интересов в информационной сфере особо отмечается обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры Российской Федерации (КИИ РФ), развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций (ЧС), вызванных информационно-техническим воздействием на объекты КИИ [2].

В этой связи от государства, как от гаранта безопасности КИИ РФ, требуется дальнейшее усиление роли по совершенствованию правового регулирования в области обеспечения ее информационной безопасности.

В соответствии с действующими в нашей стране нормативными документами в области защиты и обеспечения безопасности критически важных объектов (КВО) и ключевых систем информационной инфраструктуры (КСИИ) [2–4] КВО признается объект, оказывающий существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к ЧС или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны либо для жизнедеятельности населения, проживающего на соответствующей территории. Основными признаками принадлежности объекта к КВО выделяются следующие:

– наличие на объекте экологически опасного или социально значимого производства либо технологического процесса, нарушение штатного режима которого приводит к ЧС определенного уровня и масштаба;

– наличие на объекте информационно-телекоммуникационной системы (ее элемента), которая осуществляет функции управления чувствительными (важными) для Российской Федерации процессами и нарушение функционирования которой, приводит к негативным для страны последствиям.

Под КСИИ понимается информационно-управляющая или информационно-телекоммуникационная система (ИТКС), которая осуществляет управление КВО (процессом), либо информационное обеспечение управления таким объектом (процессом)

либо официальное информирование граждан. В результате деструктивных информационных воздействий на КСИИ может сложиться ЧС или будут нарушены выполняемые системой функции управления со значительными негативными последствиями. Таким образом, понятие КСИИ обобщает в себе множество различных классов информационных, автоматизированных систем и ИТКС (системы предупреждения и ликвидации ЧС, географические и навигационные системы, системы управления водоснабжением, энергоснабжением, транспортом и другие системы и сети).

Одним из важных классов КСИИ, обладающим специфическими особенностями, являются автоматизированные системы управления производственными и технологическими процессами (АСУ ТП) на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Таким образом, в категорию КСИИ попадают не только многочисленные АСУ ТП объектов топливно-энергетического комплекса, транспортной отрасли, но и системы государственного управления, телевидения, банковской отрасли.

АСУ ТП подлежат отнесению к соответствующему уровню важности в соответствии с утвержденной системой признаков и включаются в реестр ключевых систем информационной инфраструктуры в порядке, установленном Положением о реестре КСИИ [5]. Информационные системы и ИТКС относятся к ключевым системам, в зависимости от их назначения в соответствии с перечнем критически важных сегментов информационной инфраструктуры. В свою очередь, критически важными сегментами информационных систем и ИТКС информационной инфраструктуры России признаются сегменты, образуемые системами, нарушение штатного режима функционирования которых может нарушить функции управления чувствительными для государства процессами, в том числе:

– системами органов государственной власти и органов местного самоуправления;

– системами органов управления правоохранительных структур;

– системами финансово-кредитной и банковской деятельности;

– системами предупреждения и ликвидации кризисных и ЧС;

– географическими и навигационными системами;

– программно-техническими комплексами центров управления взаимоувязанной сети связи России;

– сетями связи общего пользования на участках, не имеющих резервных или альтернативных видов связи;

– системами специального назначения;

– спутниковыми системами, используемыми для обеспечения органов управления и в специальных целях;

– системами управления таких отраслей и объектов инфраструктуры как: добыча и транспортировка нефти и газа, транспорт (воздушный морской и наземный), электро и водоснабжение, потенциально опасные объекты.

Особенностями и проблемами функционирования АСУ ТП с позиций обеспечения их безопасности являются:

1. Отраслевая специфичность для управляемого объекта или процесса.

2. Функционирование в режиме реального времени, нарушение которого даже при незначительном сбое, может привести к лавинообразному нарушению работы объекта с критичными последствиями.

3. Применение промышленных технических средств и технологий, как правило, имеющих длительные сроки эксплуатации, с довольно редкой заменой или модернизацией, причиной которых является необходимость обеспечения непрерывности технологического процесса. Обновление и установка нового программного обеспечения в АСУ ТП либо запрещается технологической документацией, либо связана со значительными административными и технологическими трудностями.

4. Наличие технологических и программных средств, поставляемых иностранными

производителями, определяющими порядок их сервисного обслуживания и ремонта. Такие производители или поставщики зачастую требуют наличия удаленного дистанционного доступа и управления «своими» средствами, в связи с чем для заказчика проблематично проведение контроля над вносимыми изменениями. Выезд представителей иностранных производителей на объект для проведения гарантийного или сервисного обслуживания несет для заказчика риски внедрения в АСУ ТП вредоносных закладок иностранного производства.

5. Ярко выраженная программная и аппаратная неоднородность, так как исторически почти все АСУ ТП развивались как изолированные системы, работающие по специализированным протоколам. В технологическую сеть могут входить серверы SCADA под управлением Windows либо Linux, серверы СУБД (SQL Server либо Oracle), множество программируемых логических контроллеров (PLC) различных производителей, панели оператора (HMI), интеллектуальные датчики и различные каналы связи. При этом технологическая производственная сеть может иметь несколько точек прямого подключения к корпоративной сети организации (управленческому персоналу).

6. Функционирование большинства АСУ ТП без учета возможности кибератак. В качестве примера можно отметить, что большинство протоколов обмена данными, используемых SCADA и PLC, вообще не подразумевают никакой аутентификации и авторизации. Это приводит к тому, что любое появившееся в технологической сети устройство способно получать и выдавать управляющие команды на любое другое устройство. Кроме того, в открытом доступе есть довольно много информации по уязвимостям как контроллеров и SCADA-систем, так и уязвимостям операционных систем, СУБД и даже интеллектуальных датчиков.

7. Конфликт между информационной и промышленной (функциональной) безопасностью. Промышленная безопасность хорошо нейтрализует многие угрозы естественного происхождения: случайные ошибки персонала, природные и т.п. Однако против целенаправленных угроз ее методы недостаточно эффективны. Поэтому для защиты АСУ ТП должны использоваться методы информационной безопасности и изоляция технологической среды АСУ ТП от возможного канала получения команды на активацию закладки. Закладки могут внедряться как разработчиком (иностранными поставщиками), так и лицами, сопровождающими АСУ ТП. Последствием может быть полный выход из строя системы управления без возможности замены узлов, поскольку в них та же закладка.

Работы по обеспечению безопасности функционирования ключевых объектов инфраструктуры Российской Федерации, в том числе критических объектов и объектов повышенной опасности, являются одним из основных направлений реализации «Стратегии развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г.

На предприятиях, эксплуатирующих АСУ ТП, отнесенных к КСИИ, должна быть создана система обеспечения безопасности критически важной информации в КСИИ, реализующая выполнение комплекса организационных и технических мероприятий.

Отметим, что под критически важной информацией понимается закрепленная в документации на КСИИ информация, уничтожение, блокирование или искажение которой может привести к нарушению функционирования КСИИ, а также информация о КСИИ (о ее составе, характеристиках управляемого процесса, характеристиках программного и программно-аппаратного обеспечения, размещении, коммуникациях), которая в случае ее хищения (ознакомления с ней) может быть непосредственно использована для деструктивных информационных воздействий на КСИИ. Угрозы для КСИИ на КВО почти неотличимы от других отраслей и предприятий – разница только в масштабе возможного ущерба. Перехват управления, модификация управляющих команд, нарушение работоспособности систем управления технологическими процессами могут привести к экологической катастрофе или гибели людей.

Защита АСУ ТП, включая формирование требований к защите информации,

разработку и внедрение системы защиты, обеспечение защиты информации в ходе эксплуатации автоматизированной системы и вывода из эксплуатации, должна обеспечиваться в соответствии с Требованиями ФСТЭК (Федеральная служба по техническому и экспортному контролю) России [6].

Для определения угроз безопасности информации в АСУ ТП применяются методические документы ФСТЭК России [5, 7]. Дополнительно при защите АСУ ТП также могут применяться Методические документы ФСТЭК России [8, 9] в той их части, которая не противоречит указанным выше Требованиям ФСТЭК России [6].

Организационные мероприятия системы ОБИ в КСИИ определяются и выполняются в соответствии с организационно-распорядительными и руководящими документами, которые должны быть разработаны и введены в действие на предприятии в соответствии с требованиями нормативных и методических документов ФСТЭК России [6–15].

Подсистемы, входящие в состав системы защиты КСИИ, согласно требований нормативных документов ФСТЭК России, представлены на рисунке.

Рис. **Подсистемы, входящие в состав СЗИ КСИИ по требованиям нормативных документов ФСТЭК России**

Средства защиты информации, применяемые в АСУ ТП, должны пройти оценку соответствия в соответствии с законодательством Российской Федерации о техническом регулировании [10]. Требования к защите информации в АСУ ТП должны устанавливаться заказчиком и включаться в техническое задание на создание (модернизацию) АСУ и (или) техническое задание (частное техническое задание) на создание ее системы защиты. При этом АСУ ТП, введенные в эксплуатацию до вступления в силу указанных требований, могут эксплуатироваться без доработки их системы защиты. В случае принятия решения владельцем АСУ ТП о ее плановой модернизации, такие мероприятия проводятся с учетом указанных требований.

Требования ФСТЭК России [6] не устанавливают обязательную аттестацию АСУ ТП. Тем не менее оценка соответствия системы защиты АСУ ТП должна проводиться в ходе приемочных испытаний этой автоматизированной системы, порядок проведения которых определяется национальными стандартами и стандартами организации.

Исходя из этого, заказчик вправе самостоятельно принимать решение об аттестации АСУ ТП на соответствие требованиям защиты информации. В данном случае аттестация проводится в соответствии с положениями национальных стандартов и методических документов ФСТЭК России.

Основными путями развития систем защиты КСИИ могут быть:

– создание отечественной базы данных уязвимостей программного и аппаратного обеспечения;

– создание системы оценки рисков с определением вероятного ущерба и возможности реализации угрозы;

– прогнозирование последствий реализации угроз (материальные, экономические, экологические и пр.);

– оценка возможности защиты от угроз безопасности информации имеющимися средствами, с учетом эффективности их применения;

– разработка средств и систем защиты информации для КСИИ в соответствии с новыми документами (которые должны быть разработаны или доработаны), устанавливающими соответствие между категориями критически важных объектов и существующими классами систем защиты информации, привязанных к степени конфиденциальности информации. Здесь необходимо отметить, что в АСУ ТП КВО даже высокой категории опасности может отсутствовать информация ограниченного доступа;

– разработка типовых решений для защиты КСИИ (например, использованием на периметре сети межсетевых экранов). При этом между корпоративной сетью и АСУ ТП может формироваться одна (или несколько) демилитаризованных зон. Более защищенный сценарий предусматривает исключение прямых сессий между корпоративной сетью организации и АСУ ТП. Для такого случая в демилитаризованной зоне ставится терминальный сервер;

– разработка типовых методик обследования (аудита) для КСИИ, с учетом специфики ее отраслевого характера функционирования, территориальной распределенности объектов, количества объектов, необходимости обеспечения информационной безопасности на стыке офисной и технологической сетей и контроля работы персонала;

– разработка безопасной операционной системы для многих типовых КСИИ (по модульному принципу);

– создание отраслевых центров тестирования технологических процессов и разных последствий их нарушения с активным участием министерств, ведомств и организаций из заинтересованных отраслей (топливно-энергетический комплекс, транспорт, нефтехимия, водоснабжение и т.д.), определение порядка аккредитации и лицензирования организаций, осуществляющих деятельность по оценке соответствия АСУ ТП КВО предъявляемым требованиям в области обеспечения информационной безопасности.

В рамках реализации положений Стратегии национальной безопасности до 2020 г. со стороны государства в направлении развития и реализации системы правовых мер обеспечения безопасности критических инфраструктур Российской Федерации уже проделана значительная работа, разработаны и утверждены основные концептуальные документы [2–4].

Вслед за утверждением обновленной «Доктрины информационной безопасности Российской Федерации» [2] в Государственную Думу внесен разработанный ФСБ России еще в 2013 г. проект федерального закона, посвященный безопасности КИИ РФ [16]. Указанный законопроект устанавливает организационные и правовые основы обеспечения безопасности КИИ, основные принципы и методы государственного регулирования в указанной сфере, порядок взаимодействия субъектов КИИ с государственной системой обнаружения и предупреждения компьютерных атак (ГосСОПКА), определяет полномочия

органов государственной власти, а также права, обязанности и ответственность субъектов КИИ.

Среди основных понятий, вводимых законопроектом, можно отметить такие понятия, как информационные ресурсы Российской Федерации, компьютерная атака, компьютерный инцидент, критически важный объект, КИИ, субъекты КИИ и ряд др. [16].

Законопроектом также предусматриваются основные направления обеспечения безопасности КИИ, включающие в том числе:

– определение уполномоченных федеральных органов исполнительной власти, осуществляющих мероприятия по обеспечению безопасности КИИ. Здесь необходимо отметить, что такими органами являются Президент Российской Федерации, Правительство Российской Федерации, ФСБ России и ФСТЭК России. Законопроект определяет для них соответствующие полномочия.

Установление обязательных требований по обеспечению безопасности и технической защищенности объектов КИИ, для чего предусматривается категорирование подобных объектов на основе предлагаемых законопроектом критериев. При этом устанавливаются следующие категории объектов:

– высокой категории опасности;

– средней категории опасности;

– низкой категории опасности.

Субъекты КИИ РФ на основании установленных критериев и в соответствии с утвержденными показателями этих критериев осуществляют отнесение принадлежащих им на праве собственности или ином законном основании объектов к установленным категориям и направляют сведения о результатах категорирования соответствующему регулятору.

В отношении объектов высокой категории опасности сведения направляются в ФСБ России, ведущую соответствующий реестр объектов КИИ, в отношении объектов средней и низкой категории опасности – во ФСТЭК России.

В целях обеспечения безопасности КИИ РФ законопроектом предусматривается оценка ее защищенности, проводимая на основе оценки защищенности ее объектов, анализа данных, получаемых при использовании технических средств ГосСОПКА, информации о признаках компьютерных атак в сетях электросвязи, а также иной информации, получаемой в соответствии с законодательством Российской Федерации.

Порядок проведения оценки защищенности КИИ предложено определять:

– в отношении объектов высокой категории опасности – ФСБ России;

– в отношении объектов средней и низкой категорий опасности – ФСТЭК России.

Для проведения подобной оценки ФСБ России наделяется правом установки в сетях электросвязи технических средств, предназначенных для поиска признаков компьютерных атак в сообщениях электросвязи. Причем технические условия, порядок установки и эксплуатации технических средств устанавливаются регулятором.

Законопроект допускает привлечение к проведению оценки защищенности объектов КИИ аккредитованных для этих целей в установленном порядке организаций, устанавливает требования к организациям для аккредитации.

В целях обеспечения безопасности объектов КИИ субъекты КИИ РФ создают на них системы безопасности, отвечающие установленным законопроектом требованиям, и обеспечивают их функционирование. Данные системы должны предусматривать взаимодействие с ГосСОПКА путем предоставления сведений, перечень и порядок предоставления которых устанавливается ФСБ России

Кроме того, документом определяются права и обязанности субъектов КИИ, среди которых особое внимание уделяется обязанности незамедлительно информировать в порядке, установленном ФСБ России, о компьютерных инцидентах, произошедших на объектах КИИ.

Проектом федерального закона наряду с дисциплинарной, гражданско-правовой и административной ответственностью предусматривается уголовная ответственность за нарушение законодательства о безопасности КИИ.

В целях обеспечения безопасности объектов КИИ субъекты КИИ РФ создают на них системы безопасности, отвечающие установленным законопроектом требованиям, и обеспечивают их функционирование. Данные системы должны предусматривать взаимодействие с ГосСОПКА путем предоставления сведений, перечень и порядок предоставления которых устанавливается ФСБ России.

Кроме того, документом определяются права и обязанности субъектов КИИ, среди которых особое внимание уделяется обязанности незамедлительно информировать в порядке, установленном ФСБ России, о компьютерных инцидентах, произошедших на объектах КИИ.

В заключение можно отметить, что наряду с рассмотренным законопроектом, в Государственную Думу Российской Федерации также внесен законопроект [17], предусматривающий изменения в Уголовном и Уголовно-процессуальном кодексах Российской Федерации, устанавливающие соответственно уголовную и административно-правовую ответственность за нарушения законодательства о безопасности КИИ.

Литература

1. Смирнова О.Г., Хитов С.Б. Правовые основы защиты информационных систем Российской Федерации от компьютерных атак // Право. Безопасность. Чрезвычайные ситуации. 2016. № 1 (30). С. 38–42.

2. Об утверждении Доктрины информационной безопасности Российской Федерации. Указ Президента Рос. Федерации от 5 дек. 2016 г. № 646. Доступ с Официального интернет-портала правовой информации.

3. Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий // Нормативная база защиты критически важных объектов.

4. Перечень критически важных объектов Российской Федерации (утв. Распоряжением Правительства Рос. Федерации от 23 марта 2006 г. № 411-рс). Доступ из справ.-правовой системы «Гарант».

5. Об утверждении Положения о реестре ключевых систем информационной инфраструктуры: Приказ ФСТЭК России от 4 марта 2009 г. № 74. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: Приказ ФСТЭК России от 14 марта 2014 г. № 31. Доступ из справ.-правовой системы «КонсультантПлюс».

7. РД. «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержден ФСТЭК России от 18 мая 2007 г. Доступ из справ.-правовой системы «Гарант».

8. РД. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России от 18 мая 2007 г.). Доступ из справ.-правовой системы «Гарант».

9. РД. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России от 19 нояб. 2007 г.). Доступ из справ.-правовой системы «Гарант».

10. О техническом регулировании: Федер. закон от 27 дек. 2002 г. № 184-ФЗ. Доступ из справ.-правовой системы «Гарант».

11. РД. «Методика определения актуальных угроз безопасности информации

в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России от 18 мая 2007 г.). Доступ из справ.-правовой системы «Гарант».

12. Положение о Реестре ключевых систем информационной инфраструктуры (утв. Приказом ФСТЭК России от 4 марта 2009 г. № 74). Доступ из справ.-правовой системы «Гарант».

13. Методические рекомендации по формированию аналитического прогноза по комплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период (утв. ФСТЭК России 23 апр. 2011 г.). Доступ из справ.-правовой системы «Гарант».

14. ГОСТ РО 0043-001–2010. Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения. М.: Стандартинформ, 2010.

15. ГОСТ РО 0043-002–2012. Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Система документов общие положения. М.: Стандартинформ, 2012.

16. О безопасности критической информационной инфраструктуры Российской Федерации: Законопроект № 47571-7 // Официальный сайт Государственной Думы Федерального Собрания Рос. Федерации. URL: http://www.gosduma.net/index.php (дата обращения: 12.02.2017).

17. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Законопроект № 47591-7 // Официальный сайт Государственной Думы Федерального Собрания Рос. Федерации. URL: http://www.gosduma.net/index.php (дата обращения: 12.02.2017).

ОСНОВНЫЕ ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ ВЫПОЛНЕНИИ МЕРОПРИЯТИЙ ГРАЖДАНСКОЙ ОБОРОНЫ В УСЛОВИЯХ ПРОВЕДЕНИЯ ВООРУЖЕННЫМИ СИЛАМИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРОТИВОДЕСАНТНОЙ ОБОРОНЫ

А.В. Меньшиков, кандидат педагогических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России.
В.М. Земсков;
Д.В. Степынин, кандидат военных наук, доцент.
Военная академия связи им. маршала Советского Союза С.М. Буденного

Исследуются особенности высадки противником на морское побережье Российской Федерации морского десанта, рассматриваются задачи в области гражданской обороны во время осуществления противодесантной обороны побережья, анализируются основные проблемы, возникающие при выполнении мероприятий гражданской обороны.

Ключевые слова: гражданская оборона, военный конфликт, локальная война, региональная война, десантная операция, противодесантная операция, Вооружённые Силы