ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «БЕЗОПАСНОГО ГОРОДА»: ГАРМОНИЗАЦИЯ ПОДХОДОВ

Метельков А.Н.[1]

Ключевые слова: *риск, угрозы, аппаратно-программный комплекс, защита информации, система оповещения.*

Аннотация

Цель исследования: анализ подходов к техническому регулированию развития аппаратно-программного комплекса «Безопасный город» (АПК БГ) в условиях угроз ударов беспилотных средств и терактов в отношении российской городской критической информационной инфраструктуры с позиции гармонизации системы защиты информации (ЗИ), обеспечения ее устойчивости и безопасности.

Методы исследования: междисциплинарный подход, компаративный анализ релевантных документов технического регулирования, концептуальное моделирование, формализация, категориальный подход.

Полученные результаты: разработаны модель объектов ЗИ в АПК БГ, предложения о необходимости развития его подсистемы обеспечения информационной безопасности (ИБ) как функциональной системы с внедрением методов криптографической ЗИ, передаваемой по каналам оповещения и информирования населения.

Научная новизна: рассмотрение АПК БГ в условиях роста киберугроз, современное раскрытие объектов защиты информации и систематизация требований к их техническому регулированию, обоснование гармонизации технических терминов, формулирование предложений о технических мерах обеспечения информационной безопасности комплекса, направленных на нейтрализацию актуальных угроз обрабатываемой информации в контуре информирования и оповещения населения об опасностях.

DOI: 10.24682/1994-1404-2024-3-58-67

Введение

В условиях ведения в киберпространстве в отношении России гибридной войны безопасная информационная среда играет важную роль в обеспечении реализации ИБ как одного из девяти стратегических национальных приоритетов [1]. Создание гарантий безопасного проживания и деятельности населения является одной из актуальных задач государства в условиях вооруженного противостояния России и недружественных ей стран Запада в связи с угрозами ударов ракет и беспилотных систем по объектам вглубь территории России.

Для углубления понимания опасностей важно учитывать и зарубежный опыт. Американские исследователи сомневаются в надежности срабатывания сирен аварийного оповещения в случае террористической атаки на объекты с ядерными реакторами в густонаселенном регионе. В отчетах о событиях, представленных в регулирующие органы, отмечается, что через несколько часов после отключения электроэнергии атомные электростанции (АЭС) Индиан-Пойнт и Джинна отметили сбои в работе и о неработоспособность не менее 25% сирен, охватывающих территорию вокруг АЭС Джинна. 4 апреля 2003 г. пять АЭС в Нью-Йорке и Висконсине сообщили о несрабатывании более половины аварийных сирен из-за прерывания в подаче электроэнергии [2]. В декабре 2002 г. бывший директор Федерального агентства по чрезвычайным ситуациям (FEMA) Дж. Ли Уитт в результате оценки планов эвакуации в случае выброса радиации в результате теракта на АЭС пришел к выводу о неадекватности плана реагирования прогнозируемой опасности. Американские специалисты предполагают, что при крупной аварии или теракте в густонаселенном регионе может воцариться хаос. В апреле 2017 г. хакеры взломали систему оповещения в г. Даллас, в результате чего 156 сирен полтора часа подавали знак тревоги. Жители города обращались в средства массовой информации и службу спасения, чтобы убедиться в отсутствии

[1] ***Метельков Александр Николаевич,*** *кандидат юридических наук, доцент, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России, г. Санкт-Петербург, Российская Федерация.*

E-mail: metelkov5178@mail.ru

опасности. Возникла кризисная ситуация, выросла нагрузка на спасательные службы, которыми оказана психологическая помощь местным жителям. 28 июля 2022 г. испанская полиция после года розыска сообщила об аресте двух хакеров, обвиняемых во взломе национальной сети оповещения о радиоактивности (Red de Alerta a la Radioactividad, RAR) в марте-июне 2021 г. Арестованные — бывшие работники компании, которую Главное управление гражданской защиты и чрезвычайных ситуаций (Dirección General de Protección Civil y Emergencias, DGPCE) как оператор сети наняло для её обслуживания. Знание системы оповещения позволило нарушителям разработать способ проведения эффективной кибератаки. Система RAR способствует обнаружению внезапных всплесков уровня радиации и оповещению властей Испании, на территории которой эксплуатируется 7 реакторов на 6 АЭС, об угрозе для своевременного принятия защитных мер.

Не только системы оповещения, но и «умные» города сталкиваются с проблемами безопасности, охватывающими защиту технологической инфраструктуры, обеспечением конфиденциальности данных, сетевой безопасностью контролем доступа, безопасностью устройств IoT, принятием стандартов и правил в этой области и поведением людей [3].

Резонансные теракты, угроза радиационных и иных крупных аварий вследствие боевых действий, требуют расширения функциональности АПК БГ для предупреждения катастроф и минимизации их последствий.

Выбор муниципального образования как базового уровня создания АПК БГ придает комплексу широкий масштаб. Центром консолидации информации (*рис.* А) на муниципальном уровне являются единые дежурно-диспетчерские службы (ЕДДС).

Опыт создания региональных комплексных систем безопасности с учетом концептуального подхода в развитии АПК БГ и отдельных трудностей (несовместимость оборудования, неверные организационные решения, ошибки в проектировании) [4, с. 204] позволяет предложить направления по реализации инфраструктуры:

- создание доверенной среды за счет развертывания «частного облака» на базе ведомственного центра обработки данных (например, МЧС России или МВД России);
- развитие общедоступных и специальных сервисов прикладных информационных систем (ИС), а также предоставляющих необходимые услуги населению;
- построение интеграционной платформы обмена на единых правилах и алгоритмах передачи и обработки данных между всеми участниками [5];
- использование квалифицированной электронной подписи для передачи речевых и текстуальных сигналов оповещения.

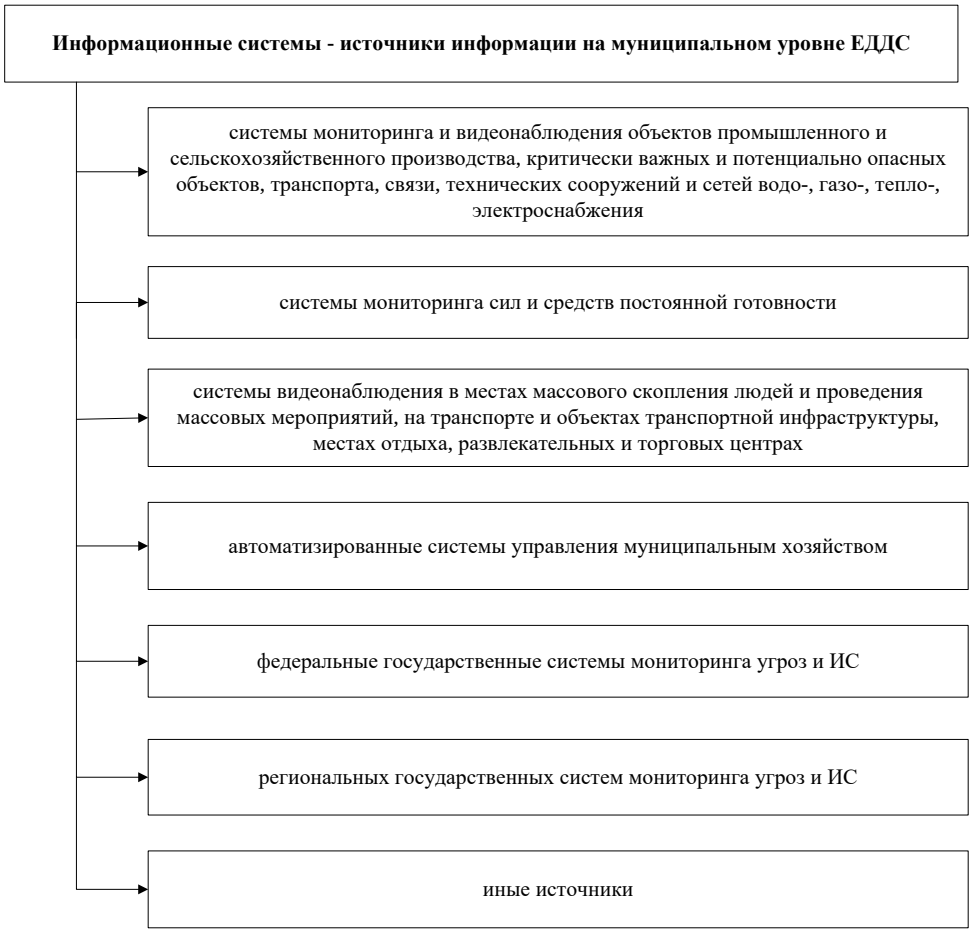

Рис. А. Информационные системы-источники информации в ЕДДС

Внедрение в региональных сегментах АПК БГ современных технологий (облачных, виртуальных, электронной подписи и др.) актуализирует проблему поиска новых методов ЗИ.

Угрозы безопасности информации

В Стратегии национальной безопасности Российской Федерации указано, что быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства, а также использованием для вмешательства во внутренние дела государств, подрыва их суверенитета.

Для доминирования в киберпространстве США используют сеть Интернет как инструмент ведения гибридной, ментальной и прокси-войн. В начале 2022 г. участились кибератаки на критическую информационную инфраструктуру. С февраля резко возросла мощность DDoS-атак на российские ресурсы. Число кибератак в 2022 г. увеличилось на 80%, их продолжительность достигала 57 часов [6, с. 69].

Ответственными за сбор, обработку и передачу информационных ресурсов о чрезвычайных ситуациях (ЧС) и происшествиях определены органы повседневного управления единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (РСЧС), включая ЕДДС. Требования МЧС России предусматривают информационное сопряжение систем информирования и оповещения, управляемых ЕДДС, с системами оповещения субъекта РФ [7].

В современной обстановке с целью повышения устойчивости и безопасности систем АПК БГ для реализации актуальных требований Указа Президента России от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» требуется обеспечение своевременного предупреждения и ликвидации последствий компьютерных атак. В 2023 г. элементы системы оповещения оказались уязвимыми для кибератак. 22, 28 февраля и 9 марта 2023 г. ложное объявление о воздушной тревоге с предупреждением об угрозе ракетного удара прозвучало в эфире телеканалов и радиостанций в ряде регионов страны. МЧС России объяснило ложные сигналы взломом серверов.

Инциденты безопасности вызывают обеспокоенность по поводу кибербезопасности АПК БГ, что требует реализации дополнительных мер, направленных на формирование безопасной среды оборота достоверной информации и устойчивой к деструктивным воздействиям. Такой подход реализуется в США, где система оповещения о ЧС (EAS) используется федеральными властями, властями штатов, местными властями, властями племен и территорий (FSLTT) для передачи важной информации по вопросам общественной безопасности пострадавшим общинам по радио и телевидению.

Риски и техническое регулирование

Известный немецкий социолог У. Бек в работе «Общество риска: на пути к новой современности» привлек общественное внимание к порожденным модернизацией антропогенным опасностям. Бек назвал иронией риска рациональность, т. е. опыт прошлого, побуждающий ожидать неправильного прогнозируемого вида риска, который можно уверено представить, рассчитать и контролировать, тогда как бедствие происходит от того, чего мы не знаем и не можем рассчитать. Актуальным становится прогнозирования рисков в информационной войне [8].

Применительно к рискам обеспечения ИБ в АПК БГ концептуально можно отнести:

- повышение уязвимости информационных ресурсов к воздействию из-за рубежа из-за применения иностранных информационных технологий и оборудования;
- проведение спецслужбами и организации недружественных государств разведывательных и иных тайных операций в российском информационном пространстве;
- нарушение информационного обеспечения служебной деятельности государственных, муниципальных и иных субъектов взаимодействия;
- перехват трансляций (систем оповещения и информирования, населения, телерадиовещания);
- несанкционированный доступ (НСД) к защищаемой информации и к управлению информационными ресурсами;
- целенаправленное деструктивное информационное воздействия на население через средства массовой информации и сеть Интернет;
- сужение возможности реализация прав граждан в получении и обмене достоверной информацией путем манипулирования массовым сознанием с применением информационно-психологического воздействия и др.

Структура АПК учитывает контроль рисков возникновения противоправных действий, эпидемий, природных пожаров, подтоплений/затоплений, ЧС на транспорте, аварий на химически и радиационно опасных объектах, возникновения аварий на объектах ЖКХ, обрушения зданий, сооружений, пород. Однако контроль рисков ИБ как самостоятельный элемент комплекса рисков в ней не выделен.

В Федеральном законе от 27.12.2002 г. № 184-ФЗ «О техническом регулировании» техническое регулирование определено как «правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции...». В не имеющей нормативного характера Концепции построения и развития АПК БГ, утвержденной распоряжением Правительства РФ от 3.12.2014 г. № 2446-р, заложена идея объединения в АПК БГ систем видеонаблюдения и фотовидеофиксации, оповещения и информирования населения, обеспечения вызова экстренных

служб, «ЭРА-ГЛОНАСС» и других систем путем внедрения комплексной ИС на базе муниципальных образований. Единая межведомственная информационная среда создается на муниципальном, региональном и федеральном уровнях согласно общему регламенту организационно-информационного взаимодействия в рамках АПК БГ, утвержденному межведомственной рабочей группой согласно плану работы Межведомственной комиссии по внедрению и развитию систем аппаратно-программного комплекса технических средств «Безопасный город», системы обеспечения вызова экстренных оперативных служб по единому номеру «112» и Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС». Пилотные программы показали жизнеспособность комплекса средств автоматизации. Координатором развития АПК БГ на федеральном уровне определено МЧС России [9, с. 71].

АПК БГ — сложная комплексная система, структура которой должна основываться на «концептуальных вопросах построения надежных информационных систем с обязательным обеспечением требований по защите информации» [10, с. 39]. В родственной АПК БГ автоматизированной информационно-управляющей системе РСЧС согласно постановлению Правительства РФ от 24 января 2024 г. № 57 в целях ЗИ ее оператор должен обеспечить:

- предотвращение НСД к информации в ИС и (или) передачи такой информации лицам, не имеющим к ней права доступа;
- незамедлительное обнаружение фактов НСД к информации в ИС;
- недопущение несанкционированного воздействия на входящие в состав ИС технические средства, нарушающего их функционирование;
- незамедлительное выявления фактов модификации, уничтожения или блокирования информации, содержащейся в ИС, вследствие НСД и восстановление такой информации;
- обеспечение контроля за защищенностью информации в ИС.

Подобные требования должны предъявляться и к АПК БГ.

В научной литературе предлагается реализовать АПК БГ с использованием оборудования для создания информационной среды, подсистемы видеоанализа, геоинформационной подсистемы, коммуникационного программного обеспечения (ПО), подсистемы управления ситуационного центра мониторинга [9]. Представляется актуальным дополнить этот набор функциональной подсистемой — системой обеспечения ИБ.

Предупреждение и ликвидация угроз безопасности информации как реализация одной из целей информационного взаимодействия нуждается в гармонизации понятий и подходов к ЗИ [11,12]. Технические задания на создание АПК БГ и нормативные правовые акты субъектов РФ, размещенные на официальных и иных сайтах государственных органов, содержат негармонизированные подходы к ЗИ, использованию терминологического аппарата. Например, в Положении о государственной информационной системе «АИУС РСЧС», утвержденном постановлением Правительства РФ от 24 января 2024 г. № 57, определено расширенное понятие ИС в отличие от Федерального закона № 149-ФЗ. В ряде технических заданий на создание АПК БГ в регионах при описании требований используется понятие «подсистема информационной безопасности», смысл которой теряется, если под ИБ понимать доктринальное определение «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз…». Исходя из определения термина «обеспечение информационной безопасности в организации» в п. 3.6.1 ГОСТ Р 53114-2008, представляется уместным использование понятия «подсистема обеспечения информационной безопасности». В документах технического регулирования АПК БГ устоявшееся в терминологическом аппарате регулятора понятие «угрозы безопасности информации; УБИ»(1) нередко подменяется многоаспектным термином «угрозы информационной безопасности» [13, с. 249—250], который в Глоссарии не определен, а раскрыто в широком аспекте понятие «Угрозы АПК «Безопасный город» [13, с.206].

УБИ = *[возможности нарушителя; уязвимости ИС;* способ *реализации угрозы; последствия от реализации угрозы]* (1)

Состав информации, используемой в информационном взаимодействии, подразделяется на оперативную, плановую, нормативно-справочную и учетную и содержит актуальные сведения об объектах мониторинга, включая критически важные объекты (КВО) [13], сведения о технических и программных средствах (ПС), о лицах, ответственных за организацию взаимодействия и наделенных правами доступа к информации и др. Негативно отражается на дифференциации обмена служебной информацией ограниченного распространения и сведений, составляющих государственную тайну, использование разных режимов защиты оперативной и плановой информации. При сборе, обработке и обмене оперативной и плановой информацией обязательным условием является «соблюдение требований конфиденциальности и защиты информации в соответствии с законодательством Российской Федерации о государственной тайне» [14]. Единые требования к техническим параметрам сегментов АПК БГ от 28 июня 2017 г. № 4516п-П4 также предусматривают обработку сведений, составляющих государственную тайну. Включение сведений о КВО требует повышения уровня ЗИ, что недостаточно согласуется в действующими организационно-техническими и методическими документами по развитию АПК БГ. Например, в п. 10.1 Технического задания указано, что создаваемая «научно-техническая продукция не предполагает работу с секретными сведениями» [13, с. 299]. В тоже время Правила разработки паспорта безопасности критиче-

ски важного объекта, утвержденные постановлением Правительства РФ от 10.11.2022 г. № 2034, устанавливают, что разработка таких документов осуществляется с соблюдением требований российского законодательства о государственной и коммерческой тайне.

Недифференцированный подход к защите различных категорий информации на практике парализует обмен защищаемых несекретных сведений конфиденциального характера. Поэтому представляется необходимым использование в АПК БГ дифференцированного подхода к обмену информацией в зависимости от степени ее конфиденциальности.

Также в Техническом задании на АПК БГ не обосновано использование алгоритма блочного шифрования ГОСТ 28147-89 после 01.06.2019 для обеспечения совместимости с действующими криптографическими средствами и согласования заказчиком с Центром защиты информации и специальной связи ФСБ России с учетом извещения от 01.07.2019 о порядке использования алгоритма в связи с вводом в действие ГОСТ 34.12-2018 и ГОСТ 34.13.2018.

Для обеспечения информационного межведомственного взаимодействия и реализации функциональных возможностей АПК БГ в режиме реального времени предоставляется оперативная информация, содержание которой в руководящих документах определяется по-разному (*табл.* 1).

Регулирующие требования рассматривают ЗИ как комплекс правовых, организационных и технических мер защиты, группируемых в зависимости от объекта защиты. Точное определение объекта защиты играет ключевую методологическую роль в ЗИ. Сравнительный анализ объектов защиты в региональных документах технического регулирования (*рис.* 1) показывает из количественное и содержательное расхождение с требованиями регуляторов (ФСБ России и ФСТЭК России) к защите информации (*рис.* 3).

В требованиях ФСТЭК России в качестве объектов ЗИ определены информационные технологии и сами средства защиты, которые, например, выпали из Временных единых требований к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город», одобренных 23.12.2014 на заседании Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем АПК технических средств «Безопасный город» и утвержденных 29.12.2014 министром МЧС России. Следует отметить, что в требованиях МЧС России используется суженное по объему в сравнении с требованиями ФСТЭК России понятие «программные средства» по сравнению с термином «программное обеспечение». В частности, в состав ПО (компьютерной системы обработки информации) включены программные документы, к которым в ГОСТ 19.101-77 отнесены документы, содержащие сведения, необходимые для разработки, изготовления, сопровождения и эксплуатации программ, а к их видам — спецификация, ведомость держателей подлинников, текст программы, описание программы, программа и методика испытаний, техническое задание, пояснительная записка, эксплуатационные документы.

Таблица 1

Определение оперативной информации в различных документах

Приказ МЧС РФ от 26 августа 2009 г. № 496 «Об утверждении Положения о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» (с изм.).	Постановление Правительства Нижегородской области от 27.10.2021 № 951 «О порядке функционирования аппаратно-программного комплекса "Безопасный город" Нижегородской области»	Методическое пособие по разработке организационных документов по созданию и развитию аппаратно-программного комплекса «Безопасный город». Москва — 2016. Разработано коллективом ФГБУ ВНИИ ГОЧС под руководством д-ра технич. наук С.А. Качанова.
сведения о прогнозируемых и (или) возникших ЧС ситуациях природного, техногенного, биолого-социального характера и их последствиях, сведения о силах и средствах РСЧС постоянной готовности, привлекаемых для предупреждения и ликвидации ЧС, а также об их деятельности, направленной на предупреждение и ликвидацию ЧС.	данные мониторинга угроз общественной безопасности, правопорядка и безопасности среды обитания на территории муниципального образования; – результаты моделирования развития кризисных ситуаций и происшествий и оценки последствий возможного их воздействия на население, объекты инфраструктуры и окружающую среду, а также сведения о динамических параметрах процессов мониторинга; – результаты расчетов требуемых сил и средств для предупреждения и ликвидации последствий кризисных ситуаций и происшествий в разрезе ведомственной и организационной принадлежности, а также последующего осуществления восстановительных мероприятий; – информация о фактах возникновения кризисных ситуаций и происшествий и их параметрах; – информация о силах и средствах, привлекаемых к предупреждению и ликвидации негативных последствий кризисных ситуаций и происшествий.	сведения о прогнозируемых и (или) возникших ЧС и происшествиях, сведения о силах и средствах постоянной готовности, привлекаемых для предупреждения и ликвидации ЧС и происшествий, а также об их деятельности, направленной на предупреждение и ликвидацию ЧС, сведения о динамических параметрах процессов (превышение критических параметров систем обеспечения жизнедеятельности населения, информация о ЧС и происшествиях).

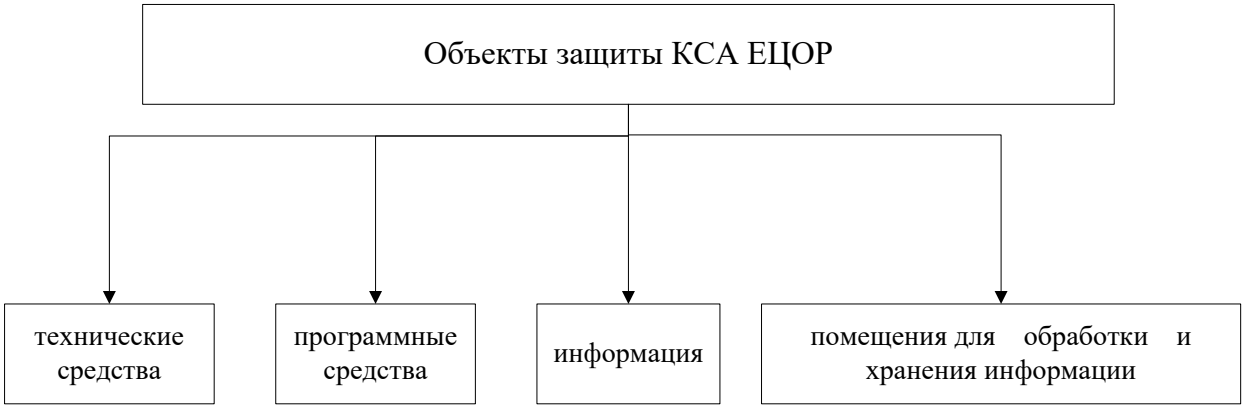

Рис.1. Объекты ЗИ в комплексе средств автоматизации единого стека открытых протоколов (КСА ЕЦОП)

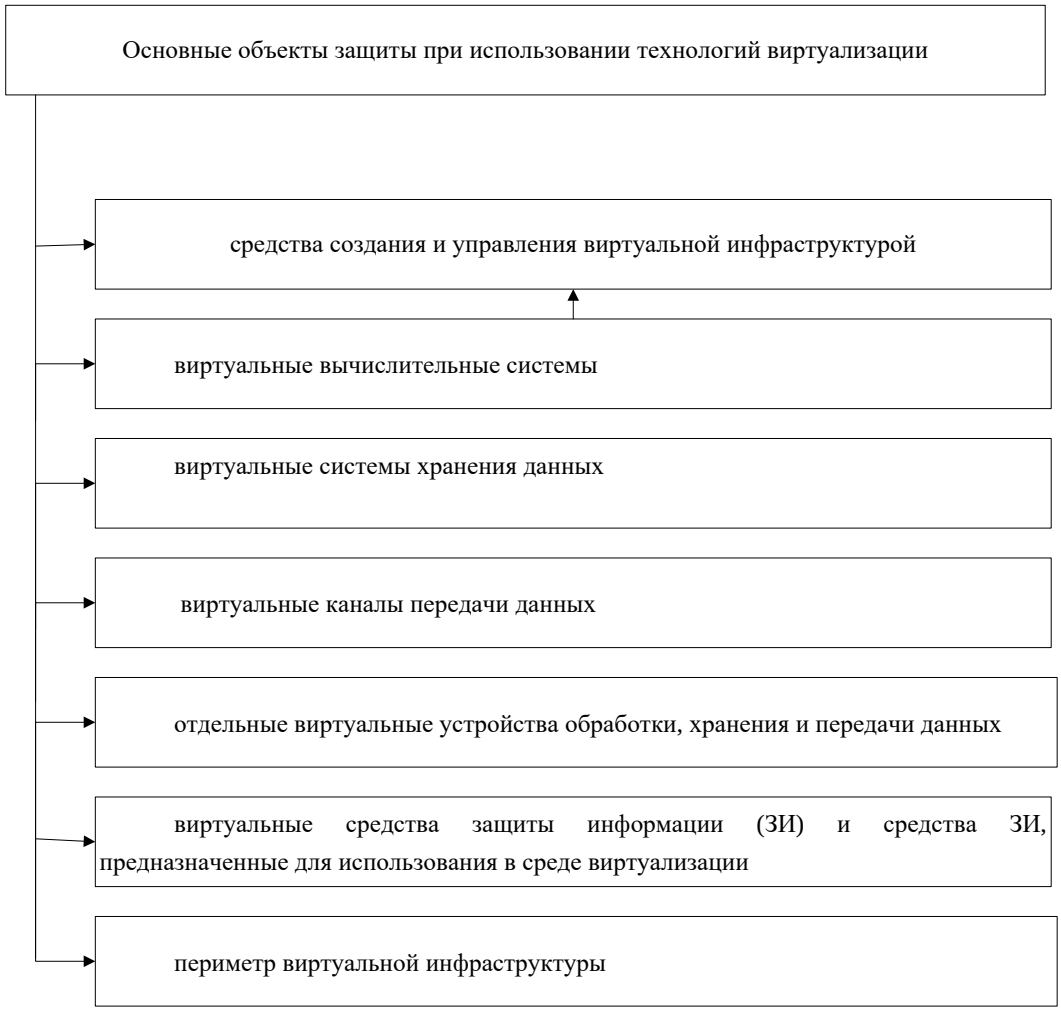

Рис. 2. Основные объекты ЗИ при использовании среды виртуализации

Предотвращению взломов элементов системы и взаимодействующих систем способствует развитие системы парольной ЗИ, учитывая существующую потребность в уточнении требований к которой как методу защиты от НСД к информации в АПК БГ. В современных условиях к такой защите должны предъявляться более строгие требования, чем изложенные во Временных требованиях, которые нуждаются в пересмотре в части правил формирования паролей, требований к их генерации и вводу, порядку смены и хранения, а также к паролям пользователя средств виртуализации, согласно Требованиям по безопасности ин-

формации к средствам виртуализации, утвержденным приказом ФСТЭК России от 27.10.2022 г. № 187. Пароли служебных учетных записей для доступа к информационным ресурсам субъектов взаимодействия должны генерироваться и распределяться централизованно либо вводиться самостоятельно с учетом современных требований (например, длина пароля должна быть не менее 8 символов и даже 10—12). Рекомендуемые в подпункте 4.2.8.1 документа [16] требования «не менее 6 символов» характеризуют слабые пароли.

В ряде репрезентативных документов технического регулирования на региональном уровне содержатся положения о применении в АПК БГ виртуальных технологий. Анализ показывает использование таких технологий в АПК БГ, однако в документах защита среды виртуализации и ее объекты защиты (*рис.* 2) часто не выделяются, что является характерным недостатком. В техническом задании на АПК БГ (НИОКР «Безопасный город») указывается, что подсистема виртуализации должна включать серверы виртуализации с установленными гипервизорами, а также ПО управления средой виртуализации и кластеризации [13, с. 278]. В документе не говорится о подсистеме защиты среды виртуализации, хотя указывается, что для защиты виртуальной инфраструктуры должно быть применено специальное ПО [13, с. 282]. В отношении ЗИ при использовании технологий виртуализации 01.06.2017 был введен в действие ГОСТ Р 56938-2016, развивающий требования ФСТЭК России, изложенные в приказах ФСТЭК России № 17 от 11.02.2013 и от 18.02.2013 № 21 к обеспечению защиты виртуализованных сред. В перечне руководящих документов в техническом задании на НИОКР Рассматриваемый ГОСТ Р, Федеральный закон «Об электронной подписи», а также ГОСТы Р и документы ФСБ России, определяющие требования к средствам, используемым в подсистеме криптографической защиты, не учтены. Кроме того, комплекс организационно-технических мероприятий по исключению несанкционированной передачи сигналов оповещения и экстренной информации должен быть реализован согласно Положению о системах оповещения населения, предусмотренных приказом МЧС России и Минцифры России от 31.07.2020 № 578/365, а требования к защите ИС оповещения должны соответствовать требованиям, изложенным приказах ФСТЭК России от 14.03.2014 № 31, от 23.03.2017 № 49 и от 9.08.2018 № 138.

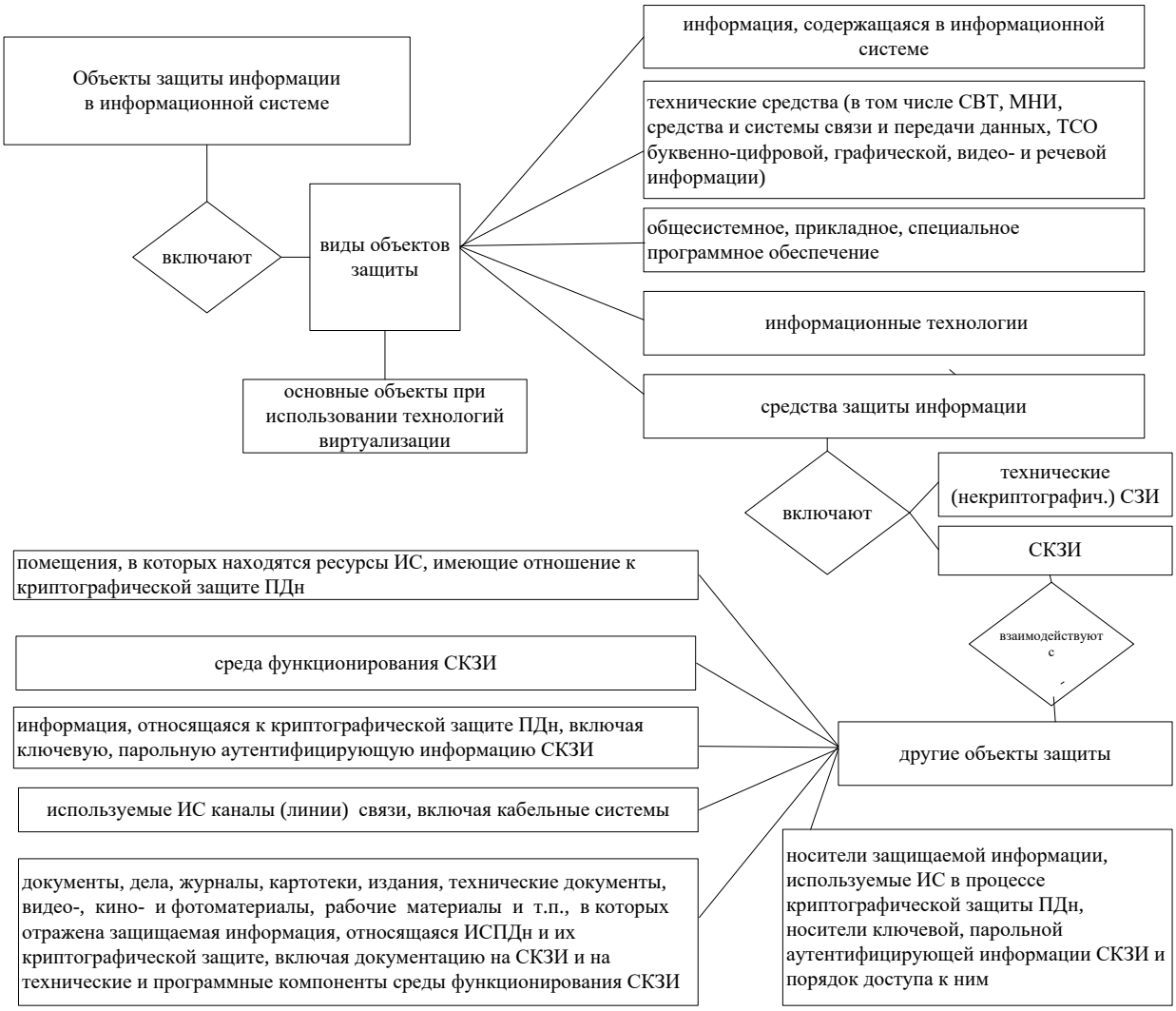

Рис 3. Модель объектов ЗИ в АПК БГ

Для защиты перечисленных выше объектов ГОСТ Р 56938-2016 рекомендует использовать как виртуальные средства ЗИ, средства ЗИ, предназначенные для использования в среде виртуализации, и другие виды средств ЗИ. Принимая это во внимание в подсистеме обеспечения ИБ необходимо выделить подсистему защиты среды виртуализации и подсистему криптографической защиты. С учетом таких предложений и требований государственного регулятора модель объектов ЗИ в АПК БГ можно формализовать в виде схем, представленных на рисунках 2 и 3.

Обезопасить обмен служебной информацией в контуре взаимодействия АПК БГ с системой оповещения населения и обмена информацией с КВО возможно с использованием квалифицированной электронной подписи и шифрования. Возникновение уязвимости, возможности нарушения функционирования АПК БГ считается отказом комплекса, а развитие модели его надежности состоит в построении детализированных моделей его отдельных составляющих [17, с. 136], подсистем, включая системы оповещения и информирования населения об угрозах ЧС и происшествий.

Выводы

В заключение исследования можно сделать следующие выводы.

1. Дальнейшее развитие АПК БГ требует разработки прогнозной модели последствий компьютерных атак на критическую и иную значимую информационную инфраструктуру как угроз ИБ, учитываемых в единой системе информационно-аналитического обеспечения безопасности среды жизнедеятельности и общественного порядка «Безопасный город».

2. Анализ технических заданий и других документов технического регулирования показывает недостаточную защищенность АПК БГ от угроз безопасности информации, что требует уточнения концептуальных технических решений в сфере информирования и оповещения населения. Рассматривая ИБ как стратегический национальный приоритет, предлагаем разрабатывать подсистему обеспечения ИБ в структуре АПК БГ в виде функциональной, а не обеспечивающей системы.

2. В качестве объектов защиты для АПК БГ на региональном уровне в документах технического регулирования необходимо выделять информационные технологии и СЗИ, а также ПО вместо ПС.

3. В АПК БГ необходимо принимать меры к защите среды виртуализации с учетом Требований по безопасности информации к средствам виртуализации ФСТЭК России и стандартов.

4. Целостность общедоступной информации об угрозах населению также должна обеспечиваться в АПК БГ согласно требованиям государственных регуляторов. Размещение информации в АПК БГ должно осуществляться с соблюдением требований законодательства России об информации, информационных технологиях и о ЗИ, в области персональных данных, о государственной тайне, о коммерческой тайне или об иной охраняемой законом тайне.

5. Для защиты передаваемых сигналов оповещения и информирования населения в АПК БГ возможно использование усиленной электронной подписи и шифрования информации.

Достоверность выводов обеспечиваются четким методологическим подходом, применением комплекса адекватных объекту защиты современных технических методов, репрезентативностью исследуемых документов технического регулирования.

Статья подготовлена в рамках выполнения в 2024 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России.

Литература

1. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27 (часть II). Ст. 5351.
2. Nukes Neg DDI 2008 GT. URL: https://textarchive.ru/c-2548297.html (дата обращения: 04.07.2023).
3. Almeida F. Prospects of Cybersecurity in Smart Cities. Future Internet. 2023; 15(9):285. URL: https://doi.org/10.3390/fi15090285 (дата обращения: 02.07.2024).
4. Исаева М.А., Кислый О.А. Цифровизация органов внутренних дел на примере АПК «Безопасный город» // Эпомен. 2021. № 55. С. 198—208.
5. Дунин В.С. Некоторые аспекты реализации положений концепции АПК «Безопасный город» // Общественная безопасность, законность и правопорядок в III тысячелетии. 2015. № 1-3. С. 19—23.
6. Коротков С. Злонамеренные дезинформационные кампании — дестабилизирующий фактор поддержания международной информационной безопасности // Международная жизнь. 2022. № 11. С. 68—75.
7. Методические рекомендации по построению и развитию АПК «Безопасный город» в субъектах Российской Федерации от 08.12.2016 г. URL: https://static.mchs.gov.ru/uploads/document/19.09.2019/8c0096d549f70913aa215f82869712b1.pdf (дата обращения: 01.07.2024).

8. Манойло А.В., Костогрызов А.И. О вероятностном прогнозировании рисков в информационной войне. Часть 1. Анализ стратегий операций и контроопераций для математического моделирования // Вопросы кибербезопасности. 2023. № 6 (58). С. 2—19.
9. Евдокимов А.С. Концепция построения и развития аппаратно-программного Комплекса «Безопасный город»: итоги реализации, организационно-правовые проблемы и нерешенные вопросы // Актуальные проблемы российского права. 2019. № 5. С. 69—77.
10. Боков Д.М., Мельников М.И., Шелупанов А.А., Мицель А.А., Ехлаков Ю.П. Использование mesh-сетей в системах типа «Безопасный город» // Вопросы защиты информации. 2015. № 2. С. 35—41.
11. Метельков А.Н. Обращение со служебной информацией в МЧС России: гармонизация терминологии / А.Н. Метельков, О.В. Уткин // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2023. № 3. С. 84—94.
12. Метельков А.Н. Конфиденциальная и служебная информация в МЧС России: модели описания информационных процессов // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2021. № 2. С. 92—99.
13. Акимов В.А., Мишурный А.В., Якимюк О.В. Прогнозно-аналитические решения по природным, техногенным и биолого-социальным угрозам единой системы информационно-аналитического обеспечения безопасности среды жизнедеятельности и общественного порядка «Безопасный город» : монография / Под ред. А.П. Чуприяна. М. : ФГБУ ВНИИ ГОЧС (ФЦ), 2022. 316 с.
14. Постановление Правительства Нижегородской области от 27.10.2021 № 951 «О порядке функционирования аппаратно-программного комплекса «Безопасный город» Нижегородской области». URL: http://publication.pravo.gov.ru/Document/View/5200202110290002 (дата обращения: 29.06.2024).
15. Положение о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций. Приложение к Приказу МЧС России от 26.08.2009 г. № 496 (ред. от 26.12.2019) // Российская газета. 23.10.2009. № 202.
16. АПК «Безопасный город». Типовое техническое задание, утв. 14.12.2015 г., утвержденное зам. председателя межведомственной комиссии по вопросам, связанным с внедрением и развитием АПК «Безопасный город» А.П. Чуприян. URL: https://17.mchs.gov.ru/deyatelnost/ (дата обращения: 02.07.2024).
17. Удалов В.И., Печенин Е.А. Математическая модель надежности системы видеонаблюдения АПК «Безопасный город» // Вестник Воронежского института ФСИН России. 2023. № 4. С. 133—136.

SECTION:
INFORMATION AND COMPUTER SECURITY

TECHNOLOGICAL REGULATION OF INFORMATION SECURITY OF THE "SECURE CITY": HARMONISATION OF APPROACHES

Aleksandr Metel'kov, *Ph.D. (Law), Associate Professor at the Department of Applied Mathematics and Information Technologies of the Saint Petersburg University of the State Fire Service of the Ministry of Emergency Situations of the Russian Federation, Saint Petersburg, Russian Federation.*
E-mail: metelkov5178@mail.ru

Keywords: *risk, threats, hard- and software system, information protection, warning system.*

Abstract

Purpose of the study: analysing approaches to technological regulation of the development of the Secure City hard- and software system (SC HSS) in the conditions of threats of drone strikes and terrorist attacks against critical Russian urban information infrastructure from the perspective of harmonisation of information protection (IP) system and ensuring its stability and security.

Methods used in the study: interdisciplinary approach, comparative analysis of relevant technological regulation documents, conceptual modelling, formalisation, categorial approach.

Study findings: a model of IP objects in SC HSS and proposals concerning the need to develop its information security subsystem as a functional system using methods of cryptographic IP transmitted through channels used for warning and informing the population were worked out.

Research novelty: consideration of the SC HSS in the conditions of increasing cyber threats, modern description of IP objects and systematisation of requirements for their technological regulation, justification for a harmonisation of technical terms, wording proposals for technical measures to ensure information security of the SC HSS which are aimed at neutralising current threats to processed information in the system used for warning and informing the population about dangerous situations.

References

1. Ukaz Prezidenta RF ot 2 iiulia 2021 g. No. 400 "O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii". Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2021. No. 27 (chast' II), st. 5351.
2. Nukes Neg DDI 2008 GT. URL: https://textarchive.ru/c-2548297.html (data obrashcheniia: 04.07.2023).
3. Almeida F. Prospects of Cybersecurity in Smart Cities. Future Internet. 2023; 15(9):285. URL: https://doi.org/10.3390/fi15090285 (data obrashcheniia: 02.07.2024).
4. Isaeva M.A., Kislyi O.A. Tsifrovizatsiia organov vnutrennikh del na primere APK "Bezopasnyi gorod". Epomen, 2021. No. 55, pp. 198–208.
5. Dunin V.S. Nekotorye aspekty realizatsii polozhenii kontseptsii APK "Bezopasnyi gorod". Obshchestvennaia bezopasnost', zakonnost' i pravoporiadok v III tysiacheletii, 2015. No. 1-3, pp. 19–23.
6. Korotkov S. Zlonamerennye dezinformatsionnye kampanii – destabiliziruiushchii faktor podderzhaniia mezhdunarodnoi informatsionnoi bezopasnosti. Mezhdunarodnaia zhizn', 2022. No. 11, pp. 68–75.
7. Metodicheskie rekomendatsii po postroeniiu i razvitiiu APK "Bezopasnyi gorod" v sub"ektakh Rossiiskoi Federatsii ot 08.12.2016 g. URL: https://static.mchs.gov.ru/uploads/document/19.09.2019/8c0096d549f70913aa215f82869712b1.pdf (data obrashcheniia: 01.07.2024).
8. Manoilo A.V., Kostogryzov A.I. O veroiatnostnom prognozirovanii riskov v informatsionnoi voine. Chast' 1. Analiz strategii operatsii i kontroperatsii dlia matematicheskogo modelirovaniia. Voprosy kiberbezopasnosti, 2023. No. 6 (58), pp. 2–19.
9. Evdokimov A.S. Kontseptsiia postroeniia i razvitiia apparatno-programmnogo Kompleksa "Bezopasnyi gorod": itogi realizatsii, organizatsionno-pravovye problemy i nereshennye voprosy. Aktual'nye problemy rossiiskogo prava, 2019. No. 5, pp. 69–77.
10. Bokov D.M., Mel'nikov M.I., Shelupanov A.A., Mitsel' A.A., Ekhlakov Iu.P. Ispol'zovanie mesh-setei v sistemakh tipa "Bezopasnyi gorod". Voprosy zashchity informatsii, 2015. No. 2, pp. 35–41.
11. Metel'kov A.N. Obrashchenie so sluzhebnoi informatsiei v MChS Rossii: garmonizatsiia terminologii. A.N. Metel'kov, O.V. Utkin. Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoi protivopozharnoi sluzhby MChS Rossii, 2023. No. 3, pp. 84–94.
12. Metel'kov A.N. Konfidentsial'naia i sluzhebnaia informatsiia v MChS Rossii: modeli opisaniia informatsionnykh protsessov. Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoi protivopozharnoi sluzhby MChS Rossii, 2021. No. 2, pp. 92–99.
13. Akimov V.A., Mishurnyi A.V., Iakimiuk O.V. Prognozno-analiticheskie resheniia po prirodnym, tekhnogennym i biologo-sotsial'nym ugrozam edinoi sistemy informatsionno-analiticheskogo obespecheniia bezopasnosti sredy zhiznedeiatel'nosti i obshchestvennogo poriadka "Bezopasnyi gorod" : monografiia. Pod red. A.P. Chupriiana. M. : FGBU VNII GOChS (FTs), 2022. 316 pp.
14. Postanovlenie Pravitel'stva Nizhegorodskoi oblasti ot 27.10.2021 No. 951 "O poriadke funktsionirovaniia apparatno-programmnogo kompleksa "Bezopasnyi gorod" Nizhegorodskoi oblasti". URL: http://publication.pravo.gov.ru/Document/View/5200202110290002 (data obrashcheniia: 29.06.2024).
15. Polozhenie o sisteme i poriadke informatsionnogo obmena v ramkakh edinoi gosudarstvennoi sistemy preduprezhdeniia i likvidatsii chrezvychainykh situatsii. Prilozhenie k Prikazu MChS Rossii ot 26.08.2009 g. No. 496 (red. ot 26.12.2019). Rossiiskaia gazeta. 23.10.2009. No. 202.
16. APK "Bezopasnyi gorod". Tipovoe tekhnicheskoe zadanie, utv. 14.12.2015 g., utverzhdennoe zam. predsedatelia mezhvedomstvennoi komissii po voprosam, sviazannym s vnedreniem i razvitiem APK "Bezopasnyi gorod" A.P. Chupriian. URL: https://17.mchs.gov.ru/deyatelnost/ (data obrashcheniia: 02.07.2024).
17. Udalov V.I., Pechenin E.A. Matematicheskaia model' nadezhnosti sistemy videonabliudeniia APK "Bezopasnyi gorod". Vestnik Voronezhskogo instituta FSIN Rossii, 2023. No. 4, pp. 133–136.