ПРИЛОЖЕНИЕ № 2
к протоколу президиума Правительственной
комиссии по цифровому развитию, использованию
информационных технологий для улучшения качества жизни
и условий ведения предпринимательской деятельности
от 10 марта 2022 г. № 7

УТВЕРЖДЕНА
протоколом президиума Правительственной
комиссии по цифровому развитию, использованию
информационных технологий для улучшения качества жизни
и условий ведения предпринимательской деятельности
от 10 марта 2022 г. № 7

Концепция информационной безопасности в сфере здравоохранения

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

г. Москва, 2022

Содержание

Сокращения, термины и определения

В настоящем документе использованы следующие сокращения и термины с соответствующими определениями.

Архитектура (системы)	Основные понятия или свойства системы в окружающей среде, воплощенной в ее элементах, отношениях и конкретных принципах ее проекта и развития (ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011)
Архитектура системы обеспечения информационной безопасности	Совокупность основных организационных и технических мер защиты информации, предназначенных для достижения уровня защищенности, обеспечивающего конфиденциальность, целостность и доступность информации
Аудит информационной безопасности	Независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения установленных требований по обеспечению информационной безопасности (ГОСТ Р 50922-2006)
Верификация	Подтверждение на основе предоставления объективных свидетельств того, что установленные требования были выполнены (ГОСТ Р 56839-2015/IEC/TR 80001-2-1:2012)
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Государственные информационные системы	Федеральные информационные системы и региональные информационные системы, созданные на основании федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов (Федеральный закон от 27.07.2006 № 149-ФЗ)
Доверие	Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности (ГОСТ Р ИСО/МЭК 15408-1-2012)
ЕГИСЗ	Единая государственная информационная система в сфере здравоохранения. Созданная Министерством здравоохранения Российской Федерации единая информационная система, необходимая для решения следующих задач: • информационного обеспечения государственного регулирования в сфере здравоохранения; • информационной поддержки деятельности медицинских организаций, включая поддержку осуществления медицинской деятельности; • информационного взаимодействия поставщиков информации в единую систему и пользователей информации, содержащейся в единой системе; • информирования населения по вопросам ведения здорового образа жизни, профилактики заболеваний, получения медицинской помощи, передачи сведений о выданных рецептах на лекарственные препараты из медицинских информационных систем медицинских организаций в информационные системы фармацевтических организаций; • обеспечения доступа граждан к услугам в сфере здравоохранения в электронной форме, а также взаимодействия информационных

	систем в сфере здравоохранения, иных информационных систем и информационных систем государственных внебюджетных фондов. (Федеральный закон от 21.11.2011 № 323-ФЗ, Постановление Правительства Российской Федерации от 05.05.2018 № 555)
Жизненный цикл	Развитие системы, продукта, услуги, проекта или других изготовленных человеком объектов, начиная со стадии разработки концепции и заканчивая прекращением применения (ИСО/МЭК 12207:2008)
Защита информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006)
Зона ответственности центра ГосСОПКА	Совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты (Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)
Защищенная сеть передачи данных (ЗСПД)	Сеть передачи данных, создаваемая и эксплуатируемая с целью обеспечения надежной, безопасной и достоверной передачи информации
Информационная безопасность	Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки (ГОСТ Р ИСО/МЭК 13335-1-2006)
Информационные ресурсы Российской Федерации	Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, находящиеся на территории Российской Федерации и в дипломатических представительствах и (или) консульских учреждениях Российской Федерации (Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)
Информационные системы	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 149-ФЗ)
Информационные системы в сфере здравоохранения	• Федеральные государственные информационные системы в сфере здравоохранения; • информационные системы в сфере здравоохранения Федерального фонда обязательного медицинского страхования и территориальных фондов обязательного медицинского страхования; • государственные информационные системы в сфере здравоохранения субъектов Российской Федерации; • медицинские информационные системы медицинских организаций; • информационные системы фармацевтических организаций. (Федеральный закон от 21.11.2011 № 323-ФЗ)
Информационные системы общего пользования	Федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности

	правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет (Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные Приказом ФСБ России, ФСТЭК России от 31.08.2010 № 416/489)
Инцидент информационной безопасности	Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности (ГОСТ Р ИСО/МЭК ТО 18044-2007)
Источник угрозы безопасности информации	Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации (ГОСТ Р 50922-2006)
Информация	Сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ)
Иные информационные системы	Информационные системы, предназначенные для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг (Федеральный закон от 21.11.2011 № 323-ФЗ)
Компьютерная атака	Целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации (Федеральный закон от 26.07.2017 № 187-ФЗ)
Компьютерный инцидент	Факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки (Федеральный закон от 26.07.2017 № 187-ФЗ)
Концепция	Концепция информационной безопасности в сфере здравоохранения
Мониторинг	Систематический сбор и обработка информации по процессам и объектам внимания для оценки их состояния и прогнозов развития с целью принятия решения (ГОСТ Р 56875-2016)
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
Объект информатизации	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров (ГОСТ Р 51275-2006)
Объекты критической информационной инфраструктуры	Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры (Федеральный закон от 26.07.2017 № 187-ФЗ)

Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ)
Приложение	Решение в области ИТ, включающее прикладное программное средство, прикладные данные и процедуры, предназначенные для содействия пользователям организации в осуществлении определенных задач или обработке конкретных видов задач ИТ посредством автоматизации процесса или функции бизнеса (ГОСТ Р ИСО/МЭК 27034-1-2014)
Риск информационной безопасности	Возможность того, что Угроза безопасности информации сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации. Измеряется исходя из комбинации вероятности события и его последствия (ГОСТ Р ИСО/МЭК 27005-2010)
Свидетельство доверия	Документированные результаты, представленные данными, полученными при анализе доверия к оцениваемому объекту, включая отчеты (обоснования) в поддержку утверждения о доверии (ГОСТ Р 54581-2011)
Сеть связи	Технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи (Федеральный закон от 07.07.2003 № 126-ФЗ)
Система обеспечения информационной безопасности	Совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности (Указ Президента Российской Федерации от 05.12.2016 № 646)
Социальная инженерия	Метод манипулирования мыслями и поступками людей, базирующийся на психологических особенностях личности и закономерностях человеческого мышления
Субъект критической информационной инфраструктуры	Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей (Федеральный закон от 26.07.2017 № 187-ФЗ)
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 50922-2006)
Уровень доверия	Уровень, характеризующий безопасность применения средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа (Приказ ФСТЭК России от 30.07.2018 № 131)
Центр ГосСОПКА	Структурная единица ГосСОПКА, представляющая совокупность подразделений и должностных лиц субъекта ГосСОПКА, которые

	принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и реагировании на компьютерные инциденты в своей зоне ответственности (Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)
Центр ГосСОПКА, ведомственный	Центр ГосСОПКА, созданный заинтересованным органом государственной власти или в интересах органа государственной власти, организацией, осуществляющей лицензируемую деятельность в области защиты информации (Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)
Центр ГосСОПКА, корпоративный	Центр ГосСОПКА, созданный государственной корпорацией, оператором связи или другой организацией, осуществляющей лицензируемую деятельность в области защиты информации (Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации)
Центр ГосСОПКА, отраслевой	Ведомственный центр ГосСОПКА, являющийся головным центром ГосСОПКА в сфере здравоохранения
Эскизное решение	Описание базового набора мер защиты информации и средств защиты информации, необходимое для их реализации в информационных системах в сфере здравоохранения в соответствии с установленными требованиями

Введение

Расширение областей применения информационных технологий в различных отраслях, включая здравоохранение, является одним из основных факторов совершенствования функционирования институтов государственной власти. Вместе с тем эпоха масштабной реализации проектов цифровой трансформации системы государственного управления Российской Федерации характеризуется повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на создаваемые информационное ресурсы. При этом практика централизованного внедрения единых цифровых решений без одновременного создания системы обеспечения их информационной безопасности существенно повышает риски проявления угроз безопасности и, как следствие, нанесения ущерба интересам личности, общества и государства.

Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации, относится к национальным интересам Российской Федерации в информационной сфере и направлено на формирование безопасного информационного пространства оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры.

В соответствии со Стратегией национальной безопасности Российской Федерации достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач[1]:

- снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных;
- обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий;
- обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления.

В соответствии с Доктриной информационной безопасности Российской Федерации[2] Министерство здравоохранения Российской Федерации входит в состав организационной основы системы обеспечения информационной безопасности Российской Федерации и в рамках своей деятельности по развитию и совершенствованию системы обеспечения информационной безопасности в сфере здравоохранения выполняет в числе прочего:

- планирование, осуществление и оценку эффективности комплекса мер по обеспечению информационной безопасности в сфере здравоохранения;
- организацию деятельности и координацию взаимодействия сил обеспечения информационной безопасности в сфере здравоохранения, совершенствование их правового, организационного, информационно-аналитического, кадрового и экономического обеспечения;
- укрепление вертикали управления и централизацию сил обеспечения информационной безопасности в сфере здравоохранения на федеральном, региональном, муниципальном уровнях, а также на уровне объектов информатизации и операторов информационных систем в сфере здравоохранения.

---

[1] Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400

[2] Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646.

Настоящая Концепция является базовым отраслевым документом стратегического планирования, определяющим направления развития системы обеспечения информационной безопасности в сфере здравоохранения, систему взглядов, принципы, подходы и требования к обеспечению защиты информации, обрабатываемой в информационных системах в сфере здравоохранения, и включает:

- результаты анализа текущего состояния защиты информации в информационных системах в сфере здравоохранения;
- задачи и цели, достижение которых обеспечит реализацию единого комплексного подхода к созданию и совершенствованию системы обеспечения информационной безопасности в сфере здравоохранения и позволит минимизировать возможные негативные последствия реализации угроз безопасности информации в информационных системах в сфере здравоохранения;
- базовые принципы и подходы к обеспечению защиты информации в информационных системах в сфере здравоохранения, к построению системы реагирования на компьютерные атаки и инциденты информационной безопасности, к созданию и функционированию защищенных сетей передачи данных;
- эскизные решения по реализации мер защиты информации в информационных системах в сфере здравоохранения;
- основные этапы реализации концепции.

1. Область действия Концепции

Настоящая Концепция определяет систему взглядов, принципы и подходы к обеспечению защиты информации, не составляющей государственную тайну, а также к построению единой системы обеспечения информационной безопасности в сфере здравоохранения.

В настоящей Концепции рассматривается обеспечение информационной безопасности в информационных системах, автоматизированных системах управления и информационно-телекоммуникационных сетях в сфере здравоохранения, включающее в себя:

- реализацию мер защиты информации, предусмотренных нормативными правовыми актами Российской Федерации и техническими заданиями на создание информационных систем с учетом модели угроз безопасности информации, а также уровней защищенности персональных данных при их обработке в информационных системах персональных данных;
- реализацию мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения в соответствии с нормативными правовыми актами Российской Федерации, включая осуществление мониторинга информационной безопасности в сфере здравоохранения и информационно-телекоммуникационных сетей, обеспечивающих их функционирование.

Единая система обеспечения информационной безопасности в сфере здравоохранения включает в себя совокупность сил обеспечения информационной безопасности в сфере здравоохранения, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности[3].

К силам обеспечения информационной безопасности в сфере здравоохранения относятся подразделения и должностные лица, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности, следующих категорий участников системы обеспечения информационной безопасности в сфере здравоохранения:

- Министерство здравоохранения Российской Федерации;
- федеральные органы исполнительной власти, являющиеся операторами информационных систем в сфере здравоохранения;
- организации, подведомственные Министерству здравоохранения Российской Федерации;
- Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования;
- органы государственной власти субъектов Российской Федерации в сфере охраны здоровья;
- органы местного самоуправления в сфере охраны здоровья;
- медицинские и фармацевтические организации;
- организации, информационные ресурсы и (или) инфраструктура которых используются в сфере здравоохранения;
- организации – операторы иных информационных систем, которые могут взаимодействовать с информационными системами в сфере здравоохранения;
- организации, имеющие соответствующие лицензии и привлекаемые к обеспечению информационной безопасности информационных систем в сфере здравоохранения.

К средствам обеспечения информационной безопасности в сфере здравоохранения относятся:

- программные, программно-аппаратные и технические средства, применяемые для реализации мер защиты информации в информационных системах в сфере здравоохранения и информационно-телекоммуникационных сетях, обеспечивающих их функционирование;

---

[3] Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646, статья 2.

- средства обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения и информационно-телекоммуникационные сети, обеспечивающие их функционирование.

Настоящая Концепция определяет архитектуру и функции системы обеспечения информационной безопасности в сфере здравоохранения на основе правовой базы Российской Федерации, а также результатов анализа текущего состояния информационных систем и тенденций цифровой трансформации сферы здравоохранения.

2. Характеристика текущего состояния защиты информации сферы здравоохранения

2.1. Структура информационных систем в сфере здравоохранения

2.1.1. Систематизированная информация об информационных системах в сфере здравоохранения

Информационное обеспечение в сфере здравоохранения осуществляется посредством создания, развития и эксплуатации федеральных государственных информационных систем в сфере здравоохранения, информационных систем в сфере здравоохранения Федерального фонда обязательного медицинского страхования, в том числе развития и эксплуатации государственной информационной системы обязательного медицинского страхования, и территориальных фондов обязательного медицинского страхования, государственных информационных систем в сфере здравоохранения субъектов Российской Федерации, медицинских информационных систем медицинских организаций, информационных систем фармацевтических организаций (информационные системы в сфере здравоохранения)[4].

На федеральном уровне уполномоченным федеральным органом исполнительной власти в сфере здравоохранения создается, развивается и эксплуатируется единая государственная информационная система в сфере здравоохранения (ЕГИСЗ) с целью обеспечения доступа граждан к услугам в сфере здравоохранения в электронной форме, а также для организации иерархического взаимодействия информационных систем в сфере здравоохранения[5].

Информационное взаимодействие ЕГИСЗ с федеральными государственными информационными системами и информационными системами государственных внебюджетных фондов осуществляется с использованием единой системы межведомственного электронного взаимодействия[6]. Для организации информационного взаимодействия с государственными информационными системами в сфере здравоохранения субъектов Российской Федерации, медицинскими информационными системами медицинских организаций государственной, муниципальной и частной систем здравоохранения, а также с иными информационными системами используется защищенная сеть передачи данных[7].

Пользователи информации, содержащейся в ЕГИСЗ, получают информацию из ЕГИСЗ, в том числе посредством единой системы межведомственного электронного взаимодействия[8]. Доступ граждан к услугам в сфере здравоохранения в электронной форме осуществляется посредством взаимодействия ЕГИСЗ с единым порталом государственных и муниципальных услуг[9].

На региональном уровне органами исполнительной власти субъектов Российской Федерации, уполномоченными высшим исполнительным органом государственной власти субъекта Российской Федерации, создаются, развиваются и эксплуатируются ГИС в сфере здравоохранения субъектов Российской Федерации, содержащие информацию, необходимую для информационной поддержки управленческой деятельности в сфере охраны здоровья граждан в субъекте Российской Федерации, включая информацию о медицинских и фармацевтических организациях на территории субъекта Российской Федерации и об осуществлении ими медицинской и фармацевтической деятельности на территории субъекта Российской Федерации[10]. К ГИС в сфере здравоохранения субъектов

---

[4] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», п. 1 ст. 91.

[5] Там же, п. 1 ст. 91.1.

[6] Положение о единой государственной информационной системе в сфере здравоохранения, утвержденное Постановлением Правительства Российской Федерации от 05.05.2018 № 555, п.п. 43, 52.

[7] Там же, п.п. 48, 53.

[8] Там же, п. 43.

[9] В соответствии с п. 5 ст. 91.1 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

[10] Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций, утвержденные Приказом Министерства здравоохранения Российской Федерации от 24.12.2018 № 911н, п.п. 2, 6.

Российской Федерации предоставляется доступ и (или) осуществляется подключение медицинских информационных систем медицинских организаций[11].

В то же время ГИС в сфере здравоохранения субъектов Российской Федерации в отдельных случаях могут обеспечивать выполнение функций медицинских информационных систем медицинских организаций[12]. Также допускается взаимодействие ГИС в сфере здравоохранения субъектов Российской Федерации с региональными порталами государственных и муниципальных услуг[13].

Медицинские информационные системы медицинских организаций (МИС МО) предназначены для обеспечения автоматизации процессов оказания и учета медицинской помощи, а также информационной поддержки медицинских работников[14]. При этом системы хранения результатов диагностических исследований (архив медицинских изображений), а также системы хранения результатов лабораторных исследований могут быть удаленными, самостоятельными и не входящими в состав МИС МО, полностью интегрированными с МИС МО или являться ее частью[15]. Взаимодействие МИС МО с информационными системами территориальных фондов обязательного медицинского страхования и страховых медицинских организаций осуществляется через интеграцию с данными системами либо через автоматизированную передачу данных о медицинской помощи[16].

Информационные системы фармацевтических организаций предназначены для автоматизации процессов осуществления фармацевтической деятельности и информационной поддержки фармацевтических работников[17].

С информационными системами в сфере здравоохранения и медицинскими организациями также могут взаимодействовать информационные системы, предназначенные для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, в порядке, на условиях и в соответствии с требованиями, установленными Правительством Российской Федерации[18].

В настоящее время состояние информационных систем в сфере здравоохранения характеризуется в числе прочего:

- разнотипностью решаемых задач;
- разнообразием программных и технических решений;
- разнообразием подходов и способов реализации ИТ-архитектуры (локальные, облачные и гибридные решения);
- консолидацией информации различного назначения, принадлежности и конфиденциальности;
- подходом к управлению доступом различных категорий пользователей без учета их функциональных обязанностей;

---

[11] Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций, утвержденные Приказом Министерства здравоохранения Российской Федерации от 24.12.2018 № 911н, п. 10.

[12] Там же, п. 5.

[13] Требования к региональным порталам государственных и муниципальных услуг (функций), утвержденные Постановлением Правительства Российской Федерации от 24.10.2011 № 861, п. 1. Положения о единой государственной информационной системе в сфере здравоохранения, утвержденного Постановлением Правительства Российской Федерации от 05.05.2018 № 555, п. 19 приложения 1.

[14] Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций, утвержденные Приказом Министерства здравоохранения Российской Федерации от 24.12.2018 № 911н, п. 3.

[15] Там же, п. 30.

[16] Приказ ФФОМС от 07.04.2011 № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования».

[17] Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций, утвержденные Приказом Министерства здравоохранения Российской Федерации от 24.12.2018 № 911н, п. 4.

[18] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», п.п. 5 и 6 ст. 91.

- разнородностью способов реализации информационного взаимодействия;
- недостаточностью уровня обеспечения отказоустойчивости;
- территориальной распределенностью и интенсивностью информационного обмена;
- интеграцией разнородных функциональных подсистем;
- отсутствием единых форматов и структуры данных;
- непрерывным развитием функциональных возможностей.

2.1.2. Результаты анализа фактического состояния защиты информации в информационных системах в сфере здравоохранения

Согласно оценкам Всемирного экономического форума, компьютерные атаки занимают 9-е место в рейтинге наиболее вероятных причин глобального кризиса. Возрастают масштабы компьютерной преступности и увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий[19].

Анализ статистической информации, публикуемой правоохранительными органами Российской Федерации и экспертными организациями, показывает постоянный рост количества компьютерных атак на информационные системы во всех сферах деятельности. В 2020 году общее количество компьютерных атак на информационные системы в сфере здравоохранения по сравнению с 2019 годом выросло на 91%. При этом 68% компьютерных атак на информационные системы в сфере здравоохранения связаны с использованием вредоносного программного обеспечения; более половины из них – это атаки с использованием программ-шифровальщиков, блокирующих доступ к информации[20].

Подверженность информационных систем в сфере здравоохранения компьютерным атакам обусловлена особенностями реализации как самих информационных систем, так и систем защиты информации, а также видами обрабатываемой информации.

В информационных системах в сфере здравоохранения обрабатываются следующие основные виды информации ограниченного доступа (распространения):

- информация ограниченного доступа органов государственной власти;
- информация, обрабатываемая в государственных информационных системах;
- сведения, составляющие врачебную тайну;
- персональные данные;
- иные сведения ограниченного доступа (распространения).

Фактическое состояние защиты информации в информационных системах в сфере здравоохранения характеризуется в числе прочего следующим:

- организационные меры защиты информации в информационных системах в сфере здравоохранения разработаны не в полном объеме;
- внедрение и эксплуатация средств защиты информации носят несистемный, фрагментарный характер;
- защита информации, передаваемой по защищенной сети передачи данных при взаимодействии информационных систем в сфере здравоохранения, реализована с применением российских сертифицированных средств криптографической защиты;
- подтверждение соответствия требованиям информационной безопасности получено не для всех информационных систем в сфере здравоохранения;
- в информационных системах в сфере здравоохранения используется недоверенное прикладное и системное программное обеспечение;
- анализ защищенности информационных систем в сфере здравоохранения носит нерегулярный характер;
- укомплектованность организаций в сфере здравоохранения специалистами по защите информации имеет несистемный характер и в большинстве случаев не соответствует требованиям правовых актов Российской Федерации в области защиты информации;

---

[19] Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646, п. 14.

[20] По данным аналитических исследований компании АО «Позитивные Технологии» (Positive Technologies).

- подходы и способы реализации архитектуры систем защиты информации имеют разнородный характер;
- внутренний контроль и (или) аудит соответствия обработки защищаемой информации требованиям нормативных правовых актов Российской Федерации в сфере защиты информации и локальных актов оператора информационной системы осуществляются на нерегулярной и несистемной основе.

2.1.3. Результаты анализа проектов по цифровизации здравоохранения, в том числе влияния результатов их реализации на защиту информации в информационных системах в сфере здравоохранения

В рамках цифровизации государственного управления Российской Федерации реализуются проекты, направленные на создание механизмов взаимодействия медицинских организаций на основе единой государственной информационной системы в сфере здравоохранения, что обеспечивает повышение эффективности отрасли на всех уровнях.

Цифровизация здравоохранения планомерно ведет к непрерывному развитию услуг и сервисов в сфере здравоохранения, предоставляемых в электронной форме, постоянному повышению сложности применяемых ИТ-решений и технологий, а также значительному росту количества информационных систем, интегрируемых в единый цифровой контур в сфере здравоохранения. Ведутся федеральные проекты по разработке специализированных вертикально интегрированных медицинских информационных систем по отдельным профилям оказания медицинской помощи. В целях обеспечения взаимодействия информационных систем в сфере здравоохранения в рамках единого цифрового контура осуществляется развитие защищенной сети передачи данных.

На федеральном уровне реализуется проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)», который включает в себя мероприятия по организации условий для создания и активного применения современных технологий, внедрению и развитию медицинских информационных систем в медицинских организациях, созданию механизмов юридически значимого электронного документооборота, развитию информационно-телекоммуникационной инфраструктуры, дооснащению медицинских организаций компьютерной техникой[21].

На основе федерального проекта субъекты Российской Федерации реализуют региональные проекты по созданию единого цифрового контура здравоохранения субъекта Российской Федерации на основе ЕГИСЗ. Анализ реализации проектов цифровизации показал, что при внедрении и развитии информационных систем в сфере здравоохранения учитывается необходимость соблюдения требований нормативных правовых актов Российской Федерации в сфере защиты информации, при этом сами требования, а также принципы и способы их выполнения не детализируются. В паспортах региональных проектов требования к информационной безопасности преимущественно сфокусированы на обеспечении функционирования защищенных сетей передачи данных.

Проекты по цифровизации сферы здравоохранения реализуются по следующим направлениям:

- использование технологических решений на основе искусственного интеллекта;
- внедрение рецептов на лекарственные препараты, сформированных в форме электронных документов;
- создание единой интегрированной электронной медицинской карты;
- внедрение электронных медицинских свидетельств о рождении и смерти;
- разработка цифрового медицинского ассистента;
- создание ситуационного центра Минздрава России;
- и другие.

В результате реализации проектов по цифровизации в числе прочего:

---

[21] Паспорт федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)».

- увеличиваются количество и сложность реализации информационных систем в сфере здравоохранения;
- многократно увеличивается количество участников информационного взаимодействия;
- увеличивается количество пользователей услуг и сервисов в сфере здравоохранения, предоставляемых в электронной форме;
- значительно увеличивается объем данных, обрабатываемых в информационных системах в сфере здравоохранения;
- увеличивается территориальная распределенность информационных систем в сфере здравоохранения;
- расширяется география покрытия электронных услуг и сервисов в сфере здравоохранения, предоставляемыми в электронном виде.

Внедрение новых технологических решений может повлечь существенные изменения подходов к созданию и совершенствованию системы обеспечения информационной безопасности в сфере здравоохранения в части:

- своевременного и непрерывного нормативно-правового и методологического обеспечения информационной безопасности в процессе внедрения и эксплуатации современных технологий и ИТ-решений;
- регулярного анализа рисков и угроз информационной безопасности применяемых современных технологий;
- единых принципов создания ИТ-архитектур, контуров безопасности, а также правил обработки и хранения данных, в том числе обезличивания персональных данных;
- непрерывного анализа защищенности создаваемых и модернизируемых ИТ-решений и информационных систем;
- защиты информационно-телекоммуникационной инфраструктуры и каналов передачи информации, в том числе при использовании энергоэффективных технологий передачи данных, например таких, как NB IoT;
- контроля полноты, достоверности, целостности и актуальности данных, обрабатываемых с применением современных технологий, в том числе для машинного обучения;
- системного и регулярного внутреннего контроля и (или) аудита соответствия обработки защищаемой информации требованиям нормативных правовых актов Российской Федерации в сфере защиты информации и локальных актов оператора информационной системы.

Учитывая тенденции цифровизации в сфере здравоохранения и их влияние на защиту информации, особую важность приобретает реализация единого комплексного подхода при создании и совершенствовании системы обеспечения информационной безопасности в сфере здравоохранения.

2.1.4. Типовые подходы и эскизные решения реализации систем защиты информации в информационных системах в сфере здравоохранения

Фактическое состояние информационных систем в сфере здравоохранения является следствием исторически сложившегося децентрализованного подхода к созданию и развитию информационных систем в сфере здравоохранения, реализуемого в условиях ограниченности ресурсов. На современном этапе в рамках цифровизации государственного управления усилилась тенденция, направленная на создание и развитие централизованных платформенных решений, создание механизмов взаимодействия медицинских организаций на основе единой государственной системы в сфере здравоохранения и размещение технических средств информационной системы преимущественно на территории Российской Федерации. Примером реализации такого подхода в сфере здравоохранения является создание механизмов взаимодействия медицинских организаций на основе единой государственной системы в сфере здравоохранения.

Результаты анализа текущего состояния защиты информации в отрасли показали необходимость разработки типовых подходов и эскизных решений реализации систем защиты

информации в информационных системах в сфере здравоохранения. Набор эскизных решений[22], определенных в настоящей Концепции, создан на основе совокупности требований правовых актов ФСТЭК России в следующих областях:

- защита информации в государственных информационных системах;
- обеспечение безопасности персональных данных;
- обеспечение безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Выбор эскизного решения осуществляется на основе использования двух принципов:

- построение архитектуры информационной системы, основанной на модели распределения границ при оценке угроз безопасности информации между оператором и поставщиком облачных услуг;
- определение категории значимости информационной системы как объекта критической информационной инфраструктуры; уровня защищенности персональных данных при их обработке в информационных системах в сфере здравоохранения; класса защищенности государственной информационной системы (для государственных информационных систем в сфере здравоохранения).

Построение архитектуры информационной системы и информационно-телекоммуникационной инфраструктуры с учетом распределения границ при оценке угроз безопасности информации между оператором и поставщиком облачных услуг основывается на следующих моделях:

- использование только программных и аппаратных средств, принадлежащих оператору информационной системы на праве собственности или ином законном основании;
- использование облачных услуг по модели «инфраструктура как услуга», при которой оператор информационной системы получает и использует вычислительные ресурсы, ресурсы для хранения данных или сетевые ресурсы, предоставляемые поставщиком облачных услуг;
- использование облачных услуг по модели «платформа как услуга», при которой оператор информационной системы устанавливает, управляет и запускает прикладное программное обеспечение, используя вычислительные ресурсы, ресурсы для хранения данных или сетевые ресурсы и среду исполнения, предоставляемые поставщиком облачных услуг;
- использование облачных услуг по модели «программное обеспечение как услуга», при которой оператор информационной системы использует прикладное программное обеспечение, вычислительные ресурсы, ресурсы для хранения данных или сетевые ресурсы и среду исполнения, предоставляемые поставщиком облачных услуг.

[22] Приложение II к настоящей Концепции.

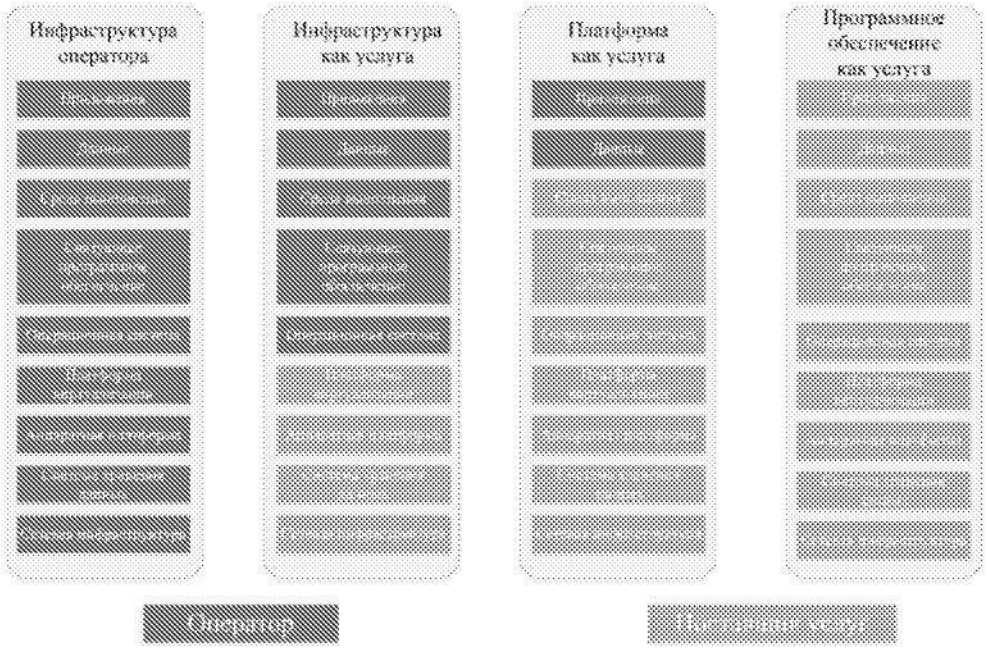


Рисунок 1. Распределение границ при оценке угроз безопасности информации между оператором и поставщиком облачных услуг

Для выбора эскизного решения используется наивысшее значение из следующих возможных характеристик информационной системы:

- класс защищенности (для государственных информационных систем);
- уровень защищенности персональных данных (для информационных систем персональных данных);
- категория значимости (для значимых объектов критической информационной инфраструктуры).

Для информационных систем, не обладающих ни одной из перечисленных характеристик, рекомендуется применять эскизное решение, соответствующее третьей категории значимости объектов критической информационной инфраструктуры.

2.2. Цели и задачи защиты информации в информационных системах в сфере здравоохранения

2.2.1. Результаты анализа нормативных правовых актов Российской Федерации и национальных стандартов Российской Федерации в сфере защиты информации

Базовыми законодательными актами в сфере защиты информации в информационных системах в сфере здравоохранения являются:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

Законодательство Российской Федерации[23] выделяет две категории информации, для которых нормативными правовыми актами Российской Федерации устанавливаются обязанности по защите информации:

- информация, доступ к которой ограничивается федеральными законами;
- информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению.

Кроме того, законодательство Российской Федерации предоставляет обладателю информации право в случаях, когда иное не предусмотрено федеральными законами, самостоятельно разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

По результатам анализа нормативных правовых актов Российской Федерации в сфере защиты информации можно выделить следующие области регулирования:

- защита информации, не составляющей государственную тайну, в государственных информационных системах;
- защита информации в информационных системах общего пользования;
- обеспечение безопасности персональных данных;
- защита информации в государственных информационных системах в сфере здравоохранения субъектов Российской Федерации, медицинских информационных системах медицинских организаций и информационных системах фармацевтических организаций;
- обеспечение безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Защита информации, не составляющей государственную тайну, обрабатываемой в государственных информационных системах, регулируется следующими правовыми актами:

- Постановление Правительства Российской Федерации от 06.07.2015 № 676 определяет обязанности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по обеспечению защиты информации в государственных информационных системах на разных стадиях их жизненного цикла;
- Приказ ФСТЭК России от 11.02.2013 № 17 утверждает Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 г., содержит методические указания по выбору мер защиты информации, а также раскрывает содержание мер защиты информации, установленных в указанных выше требованиях.

---

[23] См. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В соответствии с указанными правовыми актами защита информации, содержащейся в государственной информационной системе, обеспечивается путем выполнения требований к организации защиты информации и требований к мерам защиты информации, дифференцированных по трем классам защищенности государственных информационных систем. Приказ ФСТЭК России от 11.02.2013 № 17 определяет:

- требования к организации защиты информации;
- порядок формирования требований к защите информации;
- порядок разработки и внедрения системы защиты информации;
- порядок аттестации и ввода в действие;
- требования по обеспечению защиты информации в ходе эксплуатации, при выводе из эксплуатации или после принятия решения об окончании обработки информации;
- состав мер защиты информации и их базовые наборы для соответствующих классов защищенности.

При этом в обязанности заказчика государственной информационной системы входят адаптация и дополнение базового набора мер защиты информации в зависимости от особенностей реализации информационной системы.

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, могут применяться:

- для защиты информации, содержащейся в негосударственных информационных системах, по решению заказчиков или операторов таких систем[24];
- для защиты информации в информационных системах в сфере здравоохранения в соответствии и нормативными правовыми актами Минздрава России[25].

Отдельные требования по защите информации устанавливаются для информационных систем общего пользования. Такие требования устанавливаются следующими нормативными правовыми актами:

- Постановление Правительства Российской Федерации от 24.11.2009 № 953 устанавливает перечни сведений, которые должны публиковаться Правительством Российской Федерации и федеральными органами исполнительной власти в информационных системах общего пользования;
- совместный Приказ ФСТЭК России № 489 и ФСБ России № 416 от 31.08.2010 устанавливает требования о защите информации в информационных системах общего пользования.

В соответствии с законодательством Российской Федерации требования указанных правовых актов распространяются на иные информационные системы, предназначенные для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, взаимодействующие с информационными системами в сфере здравоохранения и медицинскими организациями[26].

Основой для регулирования вопросов защиты персональных данных является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Реализация мер защиты персональных данных регулируется следующими нормативными правовыми актами:

- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливает правила классификации информационных систем персональных данных и требуемые уровни

---

[24] В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными Приказом ФСТЭК России от 11.02.2013 № 17.

[25] В соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

[26] См. Постановление Правительства Российской Федерации от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями».

их защищенности, а также устанавливает требования к отдельным организационным мерам защиты;

- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 определяет состав и содержание организационных и технических мер защиты персональных данных при их обработке в информационных системах персональных данных, дифференцированных по уровням защищенности персональных данных;
- Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 г., устанавливает рекомендации по реализации указанных выше мер защиты персональных данных.

При этом в государственных информационных системах требования по защите персональных данных должны выполняться наряду с требованиями по защите информации, не составляющей государственную тайну, в государственных информационных системах. В государственных информационных системах (информационных систем персональных данных) обрабатывающие специальные категории ПДн должны предъявлять повышенные требования и максимальный класс защищенности для государственных информационных систем и уровню защищенности информационных систем персональных данных

В соответствии с Федеральным законом № 323-ФЗ от 21.11.2011 «Об основах охраны здоровья граждан в Российской Федерации» сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Закон устанавливает конфиденциальность сведений, составляющих врачебную тайну, но не конкретизирует требования о защите таких сведений. Сведения, составляющие врачебную тайну, относятся к определенному физическому лицу и, следовательно, включают в себя персональные данные этого лица. Таким образом, требования по защите информации, составляющей врачебную тайну, устанавливаются:

- в части, касающейся защиты персональных данных, – нормативными правовыми актами Российской Федерации, устанавливающими требования по защите персональных данных;
- в части, касающейся обеспечения конфиденциальности сведений, не являющихся персональными данными, в государственных информационных системах, – нормативными правовыми актами Российской Федерации, устанавливающими требования по защите информации в государственных информационных системах;
- в части, касающейся обеспечения конфиденциальности сведений, не являющихся персональными данными, в прочих информационных системах, – законодательством Российской Федерации об информации, информационных технологиях и о защите информации[27];
- в информационных системах в сфере здравоохранения – Минздравом России.

Вопросы криптографической защиты информации при ее обработке в государственных информационных системах и в информационных системах персональных данных регулируются следующими нормативными правовыми актами:

- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых

[27] Приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Приказ ФСБ России от 09.02.2005 года № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная Приказом ФАПСИ от 13.06.2001 № 152.

В соответствии с указанными нормативными правовыми актами для нейтрализации актуальных угроз устанавливается обязательность применения средств криптографической защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации. При выборе средств криптографической защиты информации предпочтение следует отдавать отечественному программному обеспечению, использующие российские криптографические алгоритмы и средства шифрования, а также отечественному оборудованию, соответствующему требованиям безопасности

Отдельной областью в сфере защиты информации является обеспечение безопасности критической информационной инфраструктуры Российской Федерации. Правовой основой регулирования в данной области является Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который:

- устанавливает, что информационные системы, функционирующие в сфере здравоохранения, являются объектами критической информационной инфраструктуры;
- определяет необходимость категорирования объектов критической информационной инфраструктуры;
- устанавливает права и обязанности субъектов критической информационной инфраструктуры в части обеспечения безопасности объектов критической информационной инфраструктуры;
- устанавливает права и обязанности субъектов критической инфраструктуры в части обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Правила категорирования объектов критической информационной инфраструктуры и обеспечение безопасности значимых объектов критической информационной инфраструктуры регулируются следующими нормативными правовыми актами:

- Постановление Правительства Российской Федерации от 08.02.2018 № 127 устанавливает правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также показатели, по которым проводится категорирования, и значения этих показателей, дифференцирующие значимые объекты критической информационной инфраструктуры на три категории значимости;
- Приказ ФСТЭК России от 25.12.2017 № 239 устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации;
- Приказ ФСТЭК России от 21.12.2017 № 235 устанавливает требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.

Обнаружение, предупреждение и ликвидация последствий компьютерных атак и компьютерных инцидентов регулируются следующими нормативными правовыми актами Российской Федерации:

- Приказ ФСБ России от 19.06.2019 № 282 устанавливает порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, а также принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении объектов критической информационной инфраструктуры;

- Приказ ФСБ России от 24.07.2018 № 367 устанавливает перечень сведений, представляемых субъектами критической информационной инфраструктуры в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и порядок представления такой информации;
- Приказ ФСБ России от 06.05.2019 № 196 устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
- Приказ ФСБ России от 24.07.2018 № 368 устанавливает порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры;
- Приказ ФСБ России от 19.06.2019 № 281 устанавливает порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Отдельные вопросы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации регулируются правовыми актами ограниченного распространения ФСБ России.

Правовой основой применения национальных стандартов является Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации». Закон устанавливает, что национальные стандарты применяются на добровольной основе, кроме следующих случаев:

- изготовитель продукции публично заявил о ее соответствии национальному стандарту;
- ссылка на национальный стандарт содержится в нормативном правовом акте.

В настоящее время ряд национальных стандартов Российской Федерации является обязательным в силу наличия ссылок на них в нормативных правовых актах ФСТЭК России.

Анализ правовых актов и национальных стандартов Российской Федерации выявил ряд проблемных вопросов государственного регулирования в сфере защиты информации в информационных системах в сфере здравоохранения, одним из которых является отсутствие у Минздрава России полномочий по контролю выполнения требований по защите информации в информационных системах в сфере здравоохранения.

Совершенствование и своевременная актуализация правовых актов Российской Федерации позволят минимизировать проблемы регулирования защиты информации в сфере здравоохранения.

2.2.2. Определение основных типов угроз безопасности информации в информационных системах в сфере здравоохранения

При определении основных типов угроз безопасности информации в информационных системах в сфере здравоохранения использованы подходы, установленные методическим документом «Методика оценки угроз безопасности информации» ФСТЭК России[28], с учетом анализа информации об информационных системах в сфере здравоохранения и сведений, содержащихся в банке данных угроз безопасности информации ФСТЭК России.

Угрозы безопасности информации, связанные с преднамеренными и непреднамеренными действиями внутреннего нарушителя

Источниками таких угроз являются пользователи, правомерно обладающие доступом к информационным системам в сфере здравоохранения и обрабатываемой в них информации. К угрозам данного типа относятся:

- ошибочные действия, связанные с непреднамеренным или осознанным нарушением требований нормативной, эксплуатационной и иной документации при работе с информационными системами;

[28] Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 05 февраля 2021 г.

- злоупотребление пользователями предоставленным доступом к информационным системам.

Угрозы данного типа могут привести к самому широкому кругу негативных последствий, связанных с утечкой, искажением, модификацией и удалением информации, нарушением или прекращением функционирования информационной системы. Примерами таких типовых негативных последствий реализации угроз данного типа являются:

- раскрытие, искажение или уничтожение охраняемой информации в результате ошибочных действий пользователей и персонала информационных систем или злоупотребления предоставленными им полномочиями;
- снижение уровня защищенности информационных систем и создание условий, способствующих несанкционированным действиям нарушителей.

Угрозы безопасности информации, связанные с применением методов социальной инженерии

Источником угроз данного типа являются нарушители, использующие средства социальной коммуникации с пользователями информационных систем в сфере здравоохранения.

Методы социальной инженерии используют низкую осведомленность пользователей информационных систем в вопросах информационной безопасности и призваны побудить их совершить нужное нарушителю действие (в том числе непреднамеренное нарушение правил эксплуатации информационной системы): открыть вредоносное вложение, полученное по электронной почте, перейти по вредоносной ссылке, ввести имя и пароль на веб-сайте, имитирующем интерфейс определенной информационной системы в сфере здравоохранения, и т. п.

Примерами типовых негативных последствий реализации угроз данного типа являются:

- раскрытие, искажение или уничтожение охраняемой информации в результате спровоцированных нарушителем действий пользователей и персонала информационных систем;
- получение нарушителем доступа к информационным системам и информационно-телекоммуникационным сетям, создание предпосылок для проведения компьютерных атак на смежные информационные системы и информационно-телекоммуникационные сети.

Угрозы безопасности информации, связанные с уничтожением или блокированием информации вредоносным программным обеспечением

Источником данных угроз могут являться как внешние, так и внутренние нарушители. Угроза может реализоваться в процессе целенаправленной атаки на информационные системы в сфере здравоохранения либо как сопутствующий результат атаки, совершаемой на другие объекты.

Угроза заключается в распространении в инфраструктуре, обеспечивающей функционирование информационной системы, вредоносного программного обеспечения, осуществляющего уничтожение или блокирование (шифрование) информации по заданному признаку (например, файлов определенного формата). Целью нарушителя является временное нарушение или прекращение деятельности организации.

Примерами типовых негативных последствий реализации угроз данного типа являются:

- нарушение штатного режима функционирования информационных систем;
- нарушение процессов деятельности организации, в том числе лечебных процессов;
- причинение вреда жизни и здоровью людей;
- необходимость дополнительных (незапланированных) затрат на восстановление работоспособности информационной системы и деятельности организации.

Угрозы безопасности информации, связанные с передачей информации по каналам связи

Источниками угроз данного типа являются как внутренние нарушители, так и внешние нарушители, получившие несанкционированный доступ к компонентам информационной системы или информационно-телекоммуникационных сетей, обеспечивающих ее функционирование.

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счет деструктивного воздействия на протоколы сетевого (локального) обмена данными. Несанкционированный доступ осуществляется на тех участках маршрута передачи данных, на которых не реализуется комплекс мер технической и криптографической защиты информации.

Примерами типовых негативных последствий реализации угроз данного типа является несанкционированный доступ к информации ограниченного доступа, включая информацию, позволяющую реализовывать иные типы угроз безопасности информации (сведения об уязвимостях компонентов информационных систем, идентификаторы и пароли пользователей и т. п.).

Угрозы безопасности информации, связанные с использованием нарушителем уязвимостей и недекларированных возможностей программного обеспечения

Источниками угроз данного типа являются как внутренние, так и внешние нарушители:

- имеющие санкционированный доступ к компонентам информационной системы и (или) информационно-телекоммуникационных сетей, обеспечивающих ее функционирование;
- получившие несанкционированный доступ к компонентам информационной системы и (или) информационно-телекоммуникационных сетей, обеспечивающих ее функционирование, в результате реализации угроз безопасности информации.

Угроза заключается в преднамеренном повышении привилегий и получении (распространении) доступа к компонентам информационной системы и (или) инфраструктуры, обеспечивающей ее функционирование, с использованием уязвимостей системного и прикладного программного обеспечения. При этом злоумышленник может использовать:

- известные уязвимости серийно выпускаемого программного обеспечения;
- ранее неизвестные уязвимости протоколов сетевого взаимодействия сетевого и прикладного уровней эталонной модели ISO OSI;
- уязвимости веб-интерфейсов программных и аппаратных компонентов информационной системы и инфраструктуры;
- ошибки в настройке программного и аппаратного обеспечения;
- ошибки в архитектуре информационной системы и информационно-телекоммуникационных сетей;
- недекларированные возможности в программном обеспечении.

Угрозы данного типа могут привести к самому широкому кругу негативных последствий, связанных с неправомерным копированием, искажением, модификацией и удалением информации, компрометацией аутентификационных данных, нарушением или прекращением функционирования информационной системы.

Примером типовых негативных последствий угроз данного типа является получение несанкционированного доступа к защищаемой информации в обход реализованных технических мер защиты.

Угрозы безопасности информации, связанные с нарушением функционирования средств, реализующих технологии искусственного интеллекта

Источниками угроз данного типа являются как внутренние нарушители, так и внешние нарушители, получившие несанкционированный доступ к компонентам информационной системы или информационно-телекоммуникационных сетей, обеспечивающих ее функционирование.

К данному типу относятся угрозы, связанные с раскрытием информации о модели машинного обучения, хищением обучающих данных, нарушением функционирования («обходом») средств,

реализующих технологии искусственного интеллекта, модификацией модели машинного обучения путем искажения («отравления») обучающих данных, подменой модели машинного обучения[29].

Примерами типовых негативных последствий реализации угроз данного типа являются:

- нарушение процессов деятельности организации, в том числе лечебных процессов;
- причинение вреда жизни и здоровью людей;
- необходимость дополнительных (незапланированных) затрат на восстановление работоспособности информационной системы и деятельности организации;
- причинение иного финансового ущерба.

Угрозы безопасности информации, связанные с нарушениями предоставления облачных услуг

Источниками угроз данного типа являются как внутренние нарушители, так и внешние нарушители, получившие несанкционированный доступ к облачной инфраструктуре и компонентам, обеспечивающим ее функционирование.

К данному типу относятся угрозы, связанные с нарушением доступности облачных серверов, неопределенностью в распределении ответственности между ролями в облачной инфраструктуре, потерей данных, обрабатываемых в облаке, приостановкой оказания облачных услуг вследствие технических сбоев, и другие угрозы, оказывающие влияние на предоставление облачных услуг[30].

Примерами типовых негативных последствий реализации угроз данного типа является несанкционированный доступ к информации ограниченного доступа, включая информацию, позволяющую реализовывать иные типы угроз безопасности информации (сведения об уязвимостях компонентов информационных систем, идентификаторы и пароли пользователей и т. п.), а также нарушение штатного режима функционирования компонентов облачной инфраструктуры.

Угрозы безопасности информации, связанные с техногенными источниками

К данному типу относятся угрозы, связанные с нарушением функционирования технических и программно-аппаратных средств информационных систем и информационно-телекоммуникационных сетей в результате физических явлений, не зависящих от человеческого фактора (спонтанные отказы программного и аппаратного обеспечения, нарушения электропитания и климатических условий функционирования информационных систем, стихийные бедствия и т. п.).

Примерами типовых негативных последствий реализации угроз данного типа являются:

- нарушение штатного режима функционирования информационных систем;
- нарушение процессов деятельности организации, в том числе лечебных процессов;
- причинение вреда жизни и здоровью людей;
- необходимость дополнительных (незапланированных) затрат на восстановление работоспособности информационной системы и деятельности организации.

2.2.3. Результаты анализа негативных последствий информационной безопасности в информационных системах в сфере здравоохранения, связанных с нарушением или прекращением функционирования информационных систем в сфере здравоохранения, а также защиты информации

По результатам анализа информационных систем в сфере здравоохранения, проектов по цифровизации здравоохранения, а также основных типов угроз безопасности информации в информационных системах в сфере здравоохранения можно выделить ряд негативных последствий, связанных с реализацией угроз безопасности, имеющих критически опасный характер с учетом специфики сферы здравоохранения.

---

[29] См. описание угроз в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).
[30] См. описание угроз в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

Невозможность предоставления медицинских услуг и оказания медицинской помощи, оказание ненадлежащей медицинской помощи

Указанные негативные последствия являются следствием реализации угроз безопасности информации, приводящих в числе прочего к следующему:

- недоступность (блокировка), длительные прерывания, нарушения штатного функционирования работы информационных систем в сфере здравоохранения, а также автоматизированных систем управления технологическим процессом, эксплуатируемых организациями в сфере здравоохранения;
- полная или частичная потеря связи с компонентами информационных систем в сфере здравоохранения, а также с медицинским персоналом при оказании неотложной и экстренной медицинской помощи;
- сбои и ошибки в работе информационных систем в сфере здравоохранения, приводящие к нарушению целостности и достоверности информации, необходимой для предоставления медицинской помощи;
- нештатное функционирование высокотехнологичного медицинского оборудования[31];
- причинение вреда жизни и здоровью пациента.

Невозможность точного определения диагноза и назначения лечения, а также невозможность обеспечения преемственности оказания медицинской помощи

Указанные негативные последствия являются следствием реализации угроз безопасности информации, приводящих в числе прочего к следующему:

- недоступность данных электронной медицинской карты (например, диагноза, плана лечения, характеристики пациента);
- полная или частичная утрата данных электронной медицинской карты;
- нарушение целостности результатов диагностических и лабораторных исследований;
- невозможность осуществления ретроспективного анализа диагностических данных и лабораторных исследований;
- ошибочные результаты диагностических исследований, проводимых с помощью информационных систем и (или) автоматизированных систем управления технологическим процессом;
- нарушение штатного функционирования диагностического оборудования;
- некорректные или ошибочные рекомендации в системе поддержки принятия врачебных решений;
- причинение вреда жизни и здоровью пациента.

Неправомерное использование конфиденциальной информации, обрабатываемой в информационных системах в сфере здравоохранения

Указанные негативные последствия являются следствием реализации угроз безопасности информации, приводящих в числе прочего к следующему:

- разглашение персональных данных граждан, включая специальную категорию персональных данных;
- разглашение сведений, составляющих врачебную тайну;
- разглашение сведений конфиденциального характера;
- нарушение неприкосновенности частной жизни;
- причинение морального вреда;
- причинение вреда деловой репутации;
- нанесение имущественного ущерба, в том числе в результате совершения мошеннических действий;

---

[31] ГОСТ Р 55719-2013 «Изделия медицинские электрические. Требования к содержанию и оформлению технических заданий для конкурсной документации при проведении государственных закупок высокотехнологичного медицинского оборудования».

- нанесение вреда жизни и здоровью пациента.

2.2.4. Определение целей создания системы обеспечения информационной безопасности в сфере здравоохранения

Система обеспечения информационной безопасности в сфере здравоохранения создается в целях координации и планирования деятельности сил обеспечения информационной безопасности в сфере здравоохранения и используемых ими средств защиты информации.

Основными целями системы обеспечения информационной безопасности в сфере здравоохранения являются:

- реализация единых принципов и подходов к обеспечению защиты информации в информационных системах в сфере здравоохранения;
- обеспечение единства организационно-методической политики реализации мер защиты информации;
- координация взаимодействия сил обеспечения информационной безопасности.

Реализация единых принципов и подходов к обеспечению защиты информации в информационных системах в сфере здравоохранения обеспечивается путем разработки, актуализации и внедрения отраслевых стандартов и методических рекомендаций по защите информации.

Единство организационно-методической политики реализации мер защиты информации в информационных системах в сфере здравоохранения обеспечивается путем разработки и утверждения типовых локальных нормативных актов и организационно-распорядительных документов на основе отраслевых стандартов и методических рекомендаций.

Координация взаимодействия сил обеспечения информационной безопасности в сфере здравоохранения обеспечивается путем создания отраслевого центра информационной безопасности Минздрава России, выполняющего в числе прочего функции ведомственного центра ГосСОПКА.

2.2.5. Определение задач, решение которых необходимо для создания системы обеспечения информационной безопасности в сфере здравоохранения

В рамках реализации единых принципов и подходов к обеспечению защиты информации в информационных системах в сфере здравоохранения перед системой обеспечения информационной безопасности в сфере здравоохранения стоят следующие задачи:

- разработка предложений по совершенствованию нормативно-правовой базы Российской Федерации в области защиты информации в информационных системах в сфере здравоохранения;
- разработка и внедрение отраслевых документов стратегического планирования и программ в области обеспечения защиты информации в информационных системах в сфере здравоохранения с учетом их реального состояния и особенностей функционирования;
- создание механизмов оценки соответствия проектов цифровизации сферы здравоохранения требованиям правовых актов Российской Федерации и отраслевых стандартов по защите информации в информационных системах в сфере здравоохранения;
- разработка проектов документов по защите информации, касающихся деятельности Минздрава России, органов государственной власти субъектов Российской Федерации в сфере охраны здоровья и органов местного самоуправления в сфере охраны здоровья;
- реализация требований по технической защите информации, криптографической защите информации и обеспечению безопасности объектов критической информационной инфраструктуры, установленные ФСТЭК России и ФСБ России;
- разработка отраслевых стандартов по защите информации для информационных систем в сфере здравоохранения;
- организация подготовки кадров по обеспечению защиты информации в информационных системах в сфере здравоохранения;

- создание механизмов апробации отраслевых стандартов, методических рекомендаций и проектов документов по защите информации в рамках пилотных зон.

В рамках обеспечения единства организационно-методической политики реализации мер защиты информации перед системой обеспечения информационной безопасности в сфере здравоохранения стоят следующие задачи:

- разработка типовых локальных нормативных актов по защите информации организаций в сфере здравоохранения;
- разработка типовых организационно-распорядительных документов по защите информации организаций в сфере здравоохранения;
- разработка рекомендаций по нормам штатной численности подразделений по защите информации организаций в сфере здравоохранения;
- создание единой базы знаний типовых документов по защите информации в информационных системах в сфере здравоохранения;
- создание библиотеки методических рекомендаций по реализации мер защиты информации.

В рамках координации взаимодействия сил обеспечения информационной безопасности перед системой обеспечения информационной безопасности в сфере здравоохранения стоят следующие задачи:

- создание отраслевого центра информационной безопасности Минздрава России;
- заключение между Минздравом России и ФСБ России соглашения о взаимодействии в области обнаружения, предупреждения и ликвидации компьютерных атак, наделяющего отраслевой центр информационной безопасности Минздрава России функциями ведомственного центра ГосСОПКА;
- разделение полномочий и ответственности между участниками системы обеспечения информационной безопасности в сфере здравоохранения на основе правовых актов Российской Федерации и субъектов Российской Федерации, а также соглашений, заключаемых между участниками системы;
- разработка механизмов взаимодействия между участниками системы обеспечения информационной безопасности в сфере здравоохранения;
- создание единого реестра информационных систем в сфере здравоохранения, включающего в себя сведения о назначении информационных систем, их составе, а также об их аттестации;
- организация взаимодействия с НКЦКИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3. Нормативное правовое регулирование в сфере защиты информации в информационных системах в сфере здравоохранения, основные принципы и подходы к обеспечению защиты информации в информационных системах в сфере здравоохранения

3.1. Перечень нормативных правовых актов Российской Федерации и национальных стандартов Российской Федерации, на основании которых разрабатывается Концепция

Настоящая Концепция разработана на основании следующих нормативных правовых актов и национальных стандартов Российской Федерации:

- документы стратегического планирования:
  - Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400;
  - Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646
  - Основы государственной политики Российской Федерации в области международной информационной безопасности, утвержденные Указом Президента Российской Федерации от 12 апреля 2021 г. № 213;
- федеральные законы и акты Президента Российской Федерации:
  - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
  - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
  - Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
  - Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
  - Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации»;
  - Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации»;
  - Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом Российской Федерации 12.12.2014 № К 1274;
- постановления Правительства Российской Федерации:
  - Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
  - Постановление Правительства Российской Федерации от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»;
  - Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
  - Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
  - Постановление Правительства Российской Федерации от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций

и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями»;
  - Постановление Правительства Российской Федерации от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия»;
  - Постановление Правительства Российской Федерации от 13.02.2019 № 136 «О Центре мониторинга и управления сетью связи общего пользования»;
  - Постановление Правительства Российской Федерации от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения»;
  - Постановление Правительства Российской Федерации от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;
- приказы федеральных органов исполнительной власти:
  - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
  - Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
  - Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
  - Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
  - Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
  - Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;
  - Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
  - Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации

о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;
    - Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;
    - Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
    - совместный Приказ ФСТЭК России № 489 и ФСБ России № 416 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;
    - Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
    - Приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»;
- методические документы и национальные стандарты:
    - методический документ «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11 февраля 2014 г.);
    - ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;
    - ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»;
    - ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;
    - ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;
    - ГОСТ Р 55719-2013 «Изделия медицинские электрические. Требования к содержанию и оформлению технических заданий для конкурсной документации при проведении государственных закупок высокотехнологичного медицинского оборудования»;
- иные нормативные правовые акты:
    - Приказ ФФОМС от 07.04.2011 № 79 «Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования».

3.2. Основные принципы и подходы к обеспечению защиты информации в информационных системах в сфере здравоохранения

3.2.1. Основные принципы и подходы к обеспечению защиты информации при ее обработке в информационных системах в сфере здравоохранения

Обеспечение защиты информации при ее обработке в информационных системах в сфере здравоохранения основывается на следующих принципах:

- законность при обеспечении защиты информации;
- единый подход при организации взаимодействия сил, обеспечивающих защиту информации в сфере здравоохранения;
- унификация подходов к разработке и содержанию локальных нормативных актов и организационно-распорядительных документов в области защиты информации;
- системность обеспечения информационной безопасности;

- приоритетность реализации превентивных мер защиты информации;
- адекватность и эффективность реализуемых мер защиты информации;
- своевременная адаптация реализуемых мер защиты информации;
- непрерывность защиты информации.

3.2.2. Основные принципы и подходы к обеспечению защиты информации в информационных системах в сфере здравоохранения при межведомственном взаимодействии, а также при ее передаче по сетям связи в рамках обмена информацией между информационными системами в сфере здравоохранения

Обеспечение защиты информации в информационных системах в сфере здравоохранения при межведомственном взаимодействии и обеспечении взаимодействия иных информационных систем с информационными системами в сфере здравоохранения основывается на следующих принципах и подходах:

- законность при обеспечении защиты информации в информационных системах в сфере здравоохранения при осуществлении межведомственного взаимодействия и при передаче информации по сетям связи в рамках обмена информацией между информационными системами в сфере здравоохранения;
- соблюдение установленных требований по защите информации, предъявляемых к информационным системам, информационно-телекоммуникационным сетям и сетям передачи данных всеми участниками взаимодействия;
- использование единой системы межведомственного электронного взаимодействия и (или) защищенных сетей передачи данных, функционирующих в сфере здравоохранения для передачи информации ограниченного доступа при межведомственном взаимодействии и при ее передаче в рамках обмена информацией между информационными системами в сфере здравоохранения[32];
- обеспечение целостности и устойчивости функционирования защищенных сетей передачи данных в связи с наличием потенциальных угроз информационной безопасности, которые могут оказать влияние на их работу[33];
- обеспечение непрерывной доступности информационных систем в сфере здравоохранения, участвующих в межведомственном взаимодействии, в соответствии с установленными регламентами функционирования информационных систем;
- соблюдение технологических процессов при реализации межведомственного взаимодействия и при передаче информации по сетям связи в рамках обмена информацией между информационными системами в сфере здравоохранения.

3.2.3. Основные принципы и подходы к обеспечению защиты информации в иных информационных системах, которые могут взаимодействовать с информационными системами в сфере здравоохранения

Обеспечение защиты информации в иных информационных системах, которые могут взаимодействовать с информационными системами в сфере здравоохранения, основывается на следующих принципах и подходах:

- законность при обеспечении защиты информации;
- соблюдение требований по защите информации, установленных правовыми актами Российской Федерации, которое подтверждается аттестацией на соответствие требованиям безопасности информации в случаях, установленных нормативными правовыми актами Российской Федерации;
- учет требований государственных и отраслевых стандартов по защите информации;
- обеспечение постоянного контроля уровня защищенности информации;
- соответствие обработки в иных информационных системах информации, полученной при взаимодействии с информационными системами в сфере здравоохранения, целям,

---

[32] См. Постановление Правительства Российской Федерации от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия».

[33] См. Постановление Правительства Российской Федерации от 13.02.2019 № 136 «О Центре мониторинга и управления сетью связи общего пользования».

задачам и назначению, указанным в заявках на подключение к информационным системам в сфере здравоохранения в соответствии с нормативными правовыми актами Российской Федерации и субъектов Российской Федерации;

- использование единой системы межведомственного электронного взаимодействия и (или) защищенных сетей передачи данных, функционирующих в сфере здравоохранения для передачи информации ограниченного доступа при взаимодействии иных информационных систем с информационными системами в сфере здравоохранения.

3.2.4. Единые подходы к обеспечению безопасности объектов критической информационной инфраструктуры, функционирующих в сфере здравоохранения, и к взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Обеспечение безопасности объектов критической информационной инфраструктуры, функционирующих в сфере здравоохранения, и взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации основываются на следующих принципах и подходах:

- законность;
- соблюдение требований безопасности объектов критической информационной инфраструктуры, установленных правовыми актами Российской Федерации;
- учет требований государственных и отраслевых стандартов по защите информации;
- единство подходов к категорированию объектов критической информационной инфраструктуры в сфере здравоохранения;
- единство подходов при организации взаимодействия сил, обеспечивающих обнаружение компьютерных атак и реагирование на компьютерные атаки и компьютерные инциденты;
- разумная достаточность сил и средств, предназначенных для обеспечения безопасности объектов критической информационной инфраструктуры и предупреждения, обнаружения и ликвидации последствий компьютерных атак;
- реализация единого комплексного подхода к обеспечению безопасности объектов критической информационной инфраструктуры и обнаружению, предупреждению и ликвидации последствий компьютерных атак;
- обеспечение достаточности и рациональности использования сил обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- единство подходов к мониторингу защиты информации в информационных ресурсах в сфере здравоохранения в рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- обеспечение непрерывного взаимодействия с НКЦКИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

4. Архитектура системы обеспечения информационной безопасности в сфере здравоохранения и требования к обеспечению защиты информации в информационных системах в сфере здравоохранения. Эскизные решения

4.1. Взаимосвязь сил и средств обеспечения информационной безопасности в сфере здравоохранения

Минздрав России в пределах своих полномочий выполняет следующие функции в системе обеспечения информационной безопасности в сфере здравоохранения:

- регулирует и контролирует деятельность участников системы обеспечения информационной безопасности в сфере здравоохранения;
- создает на базе подведомственного учреждения отраслевой центр информационной безопасности;
- в случаях, установленных законодательством Российской Федерации, осуществляет согласование с ФСТЭК России, ФСБ России проектов отраслевых стандартов и методических рекомендаций по защите информации в информационных системах в сфере здравоохранения, дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, учитывающих особенности функционирования значимых объектов критической информационной инфраструктуры в сфере здравоохранения;
- утверждает отраслевые стандарты и методические рекомендации по защите информации в информационных системах в сфере здравоохранения, дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, учитывающих особенности функционирования значимых объектов критической информационной инфраструктуры в сфере здравоохранения;
- координирует и контролирует выполнение субъектами критической информационной инфраструктуры в сфере здравоохранения требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры и по обеспечению их функционирования;
- устанавливает дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, учитывающие особенности функционирования значимых объектов критической информационной инфраструктуры в сфере здравоохранения;
- согласовывает перечень объектов критической информационной инфраструктуры в сфере здравоохранения в части подведомственных субъектов критической информационной инфраструктуры[34].

В целях обеспечения единых подходов к управлению системой обеспечения информационной безопасности в сфере здравоохранения отраслевой центр информационной безопасности в пределах своих полномочий выполняет следующие функции:

- организует и координирует деятельность участников системы обеспечения информационной безопасности в сфере здравоохранения;
- привлекается к осуществлению ведомственного контроля выполнения требований по защите информации в информационных системах в сфере здравоохранения, заказчиками и (или) операторами которых являются Минздрав России или подведомственные ему организации;
- привлекается к осуществлению контроля выполнение субъектами критической информационной инфраструктуры в сфере здравоохранения требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры и по обеспечению их функционирования;
- разрабатывает проекты дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, учитывающих

[34] См. Правила категорирования объектов критической информационной инфраструктуры, утвержденные постановлением Правительства Российской Федерации от 08 февраля 2018 г. № 127, п. 15

особенности функционирования значимых объектов критической информационной инфраструктуры в сфере здравоохранения;

- разрабатывает проекты отраслевых стандартов и методических рекомендаций по защите информации в информационных системах в сфере здравоохранения;
- осуществляет функции ведомственного центра ГосСОПКА в отношении объектов КИИ Минздрава России, а также объектов КИИ подведомственных учреждений и иных организаций, перечень которых определяется Минздравом России, и выполняет функции, определенные соглашением с НКЦКИ;
- осуществляет функции отраслевого центра ГосСОПКА в сфере здравоохранения, координирует силы и средства обеспечения информационной безопасности в сфере здравоохранения при обнаружении компьютерных атак, реагировании на инциденты, ликвидации их последствий, а при необходимости — принимает участие в мероприятиях по ликвидации последствий инцидентов в информационных системах в сфере здравоохранения;
- осуществляет непрерывное взаимодействие с НКЦКИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак на объекты критической информационной инфраструктуры Минздрава России;
- осуществляет функции отраслевого центра компетенции по вопросам обеспечения информационной безопасности в сфере здравоохранения, реагирования на компьютерные инциденты, связанные с нарушением или прекращением их функционирования, ликвидации последствий таких инцидентов;
- координирует вопросы организации функционирования защищенных сетей передачи данных, используемых для взаимодействия информационных систем в сфере здравоохранения;
- взаимодействует с ФСТЭК России и ФСБ России по вопросам обеспечения защиты информации в информационных системах в сфере здравоохранения, в том числе в рамках осуществления ими государственного контроля (надзора) в организациях, являющихся операторами информационных систем в сфере здравоохранения;
- оказывает методическую и практическую помощь участникам системы обеспечения информационной безопасности в сфере здравоохранения по вопросам защиты информации;
- осуществляет организацию и контроль качества подготовки кадров по информационной безопасности для сферы здравоохранения.

Ситуационный центр Минздрава России обеспечивает деятельность руководства Минздрава России и сотрудников профильных департаментов Минздрава России при реализации функций оценки, анализа и прогнозирования ситуации, стратегического, текущего и оперативного планирования, мониторинга и контроля исполнения управленческих решений в сфере здравоохранения.

Ситуационный центр Минздрава России является организационным ядром системы распределенных ситуационных центров сферы здравоохранения на федеральном и региональном уровне. Отраслевой центр информационной безопасности Минздрава России является для ситуационного центра Минздрава России источником оперативной и аналитической информации, необходимой для принятия комплексных управленческих решений в сфере здравоохранения.

Органы государственной власти субъектов Российской Федерации в сфере охраны здоровья и органы местного самоуправления в сфере охраны здоровья в пределах своих полномочий выполняют функции по обеспечению информационной безопасности в информационных системах в сфере здравоохранения, в том числе:

- обеспечивают выполнение требований по защите информации в информационных системах в сфере здравоохранения;
- осуществляют контроль за выполнением требований по защите информации в информационных системах в сфере здравоохранения.

В целях решения задач по обеспечению информационной безопасности в информационных системах в сфере здравоохранения и контроля за выполнением требований безопасности органы

государственной власти субъектов Российской Федерации в сфере охраны здоровья и органы местного самоуправления в сфере охраны здоровья при необходимости могут привлекать отраслевой центр информационной безопасности Минздрава России.

В рамках системы обеспечения информационной безопасности в сфере здравоохранения Минздрав России и подведомственные организации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования, органы государственной власти субъектов Российской Федерации в сфере охраны здоровья, органы местного самоуправления в сфере охраны здоровья, медицинские и фармацевтические организации могут выступать как в роли заказчиков информационных систем, так и в роли операторов информационных систем.

Заказчики информационных систем в сфере здравоохранения:

- принимают решения о необходимости защиты информации, содержащейся в информационной системе в сфере здравоохранения;
- классифицируют информационные системы в сфере здравоохранения по требованиям защиты информации;
- определяют угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации, и разрабатывают на их основе и с учетом отраслевых стандартов модели угроз безопасности информации для информационных систем в сфере здравоохранения;
- определяют требования к системам защиты информации для информационных систем в сфере здравоохранения;
- организуют разработку и внедрение систем защиты информации информационных систем в сфере здравоохранения.

Операторы информационных систем в сфере здравоохранения обеспечивают защиту информации в ходе эксплуатации информационных систем и при выводе их из эксплуатации в соответствии с нормативными правовыми актами Российской Федерации и, при наличии, в соответствии с дополнительными требованиями, установленными заказчиками информационных систем.

Для проведения работ по защите информации в ходе создания и эксплуатации информационных систем в сфере здравоохранения заказчиками и операторами в соответствии с законодательством Российской Федерации при необходимости могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации[35].

Организации, являющиеся операторами иных информационных систем, которые могут взаимодействовать с информационными системами в сфере здравоохранения, и организации, информационные ресурсы и (или) инфраструктура которых используются в сфере здравоохранения, обеспечивают информационную безопасность принадлежащих им информационных систем, информационных ресурсов и инфраструктуры в соответствии с правовыми актами Российской Федерации.

Информационная безопасность в информационных системах в сфере здравоохранения обеспечивается путем реализации в информационных системах (включая информационно-телекоммуникационные сети и защищенные сети передачи данных) мер защиты информации в соответствии с требованиями, установленными заказчиками информационных систем на основании правовых актов Российской Федерации. Выполнение требований к мерам защиты подтверждается:

- результатами приемочных испытаний информационных систем на соответствие техническому заданию на создание или модернизацию информационной системы;
- результатами аттестации по требованиям безопасности информации в случаях, установленных правовыми актами;
- результатами периодического контроля за обеспечением уровня защищенности (оценки эффективности мер защиты информации, контроля за обеспечением безопасности) информационных систем в сфере здравоохранения.

---

[35] См. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные Приказом ФСТЭК России от 11.02.2013 № 17.

Безопасность информации в защищенных сетях передачи данных федерального, регионального и муниципального уровня, используемых для взаимодействия информационных систем в сфере здравоохранения, должна обеспечиваться на основе требований правовых актов Российской Федерации. Безопасность информации в защищенных сетях передачи данных должна обеспечиваться на основе следующих принципов:

- законность;
- централизованный подход и стандартизация создания, функционирования, модернизации и управления защищенной сети передачи данных и ее компонентов;
- единство подходов к управлению доступом к защищенным сетям передачи данных;
- стандартизация требований по защите информации в инфраструктуре защищенной сети передачи данных и подключаемых конечных точках;
- резервирование каналов связи;
- реализация эшелонированной защиты защищенной сети передачи данных;
- регулярность, своевременность и полнота проводимых мероприятий по обеспечению информационной безопасности;
- осуществление взаимодействия в электронной форме, в том числе с гражданами и организациями в соответствии с правилами и принципами, установленными национальными стандартами Российской Федерации в области криптографической защиты информации;
- применение средств криптографической защиты информации, сертифицированных ФСБ России.

4.2. Требования к обеспечению защиты информации в информационных системах в сфере здравоохранения

Информационные системы в сфере здравоохранения применяются для обработки информации, необходимой для обеспечения критических процессов, и (или) для управления, контроля критических процессов, связанных с оказанием медицинской помощи. Нарушение или прекращение функционирования таких информационных систем может привести к причинению ущерба жизни и здоровью граждан[36]. Такие системы в соответствии с законодательством Российской Федерации относятся к значимым объектам критической информационной инфраструктуры и подлежат защите в соответствии с требованиями правовых актов Российской Федерации в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.

К силам обеспечения безопасности оператора информационной системы в сфере здравоохранения относятся:

- подразделения (работники) оператора, ответственные за обеспечение безопасности информационных систем;
- подразделения (работники) оператора, эксплуатирующие информационные системы;
- подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) технических средств информационных систем;
- иные подразделения (работники), участвующие в обеспечении безопасности информационных систем и (или) информационно-телекоммуникационных систем оператора.

Общее руководство по вопросам обеспечения информационной безопасности осуществляет руководитель организации сферы здравоохранения или его заместитель.

Руководитель организации, являющейся оператором информационной системы в сфере здравоохранения, определяет структурное подразделение, ответственное за защиту информации в информационных системах в сфере здравоохранения (структурное подразделение по информационной безопасности), или назначает отдельных работников, ответственных за защиту информации в информационных системах в сфере здравоохранения (специалистов

---

[36] См. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

по информационной безопасности). В соответствии с требованиями правовых актов Российской Федерации структурное подразделение по информационной безопасности, специалисты по информационной безопасности должны осуществлять следующие функции:

- разрабатывать предложения по совершенствованию организационно-распорядительных документов по защите информации в информационных системах и информационно-телекоммуникационных сетях, находящихся в эксплуатации у оператора, представлять их руководителю оператора;
- проводить анализ угроз безопасности информации в отношении информационных систем и информационно-телекоммуникационных сетей, находящихся в эксплуатации у оператора, выявлять уязвимости в них;
- обеспечивать реализацию требований по защите информации в информационных системах и информационно-телекоммуникационных сетях оператора в соответствии с законодательством Российской Федерации;
- обеспечивать в соответствии с требованиями по защите информации реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;
- осуществлять реагирование на компьютерные инциденты в соответствии с нормативными правовыми актами Российской Федерации и организационно-распорядительными документами оператора;
- организовывать проведение оценки соответствия информационных систем в сфере здравоохранения требованиям по защите информации;
- готовить предложения по совершенствованию функционирования систем защиты информации информационных систем в сфере здравоохранения;
- обеспечивать обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты;
- осуществлять развитие сил и средств в соответствии с правовыми актами в области обнаружения, предупреждения или ликвидации последствий компьютерных атак и компьютерных инцидентов.

Структурное подразделение по информационной безопасности, специалисты по информационной безопасности реализуют указанные функции во взаимодействии с подразделениями (работниками), эксплуатирующими информационные системы в сфере здравоохранения, и подразделениями (работниками), обеспечивающими функционирование информационных систем в сфере здравоохранения.

Подразделения (работники), обеспечивающие функционирование информационных систем в сфере здравоохранения, должны обеспечивать безопасность информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, в следующем объеме:

- осуществлять поддержку функционирования информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, в соответствии с эксплуатационной документацией;
- выполнять требования по обеспечению информационной безопасности, закрепленные в организационно-распорядительных документах по обеспечению информационной безопасности информационных систем в сфере здравоохранения, при поддержке функционирования информационных систем в сфере здравоохранения (при администрировании, наладке, регламентных работах);
- осуществлять контроль за конфигурацией информационных систем в сфере здравоохранения и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, и поддерживать ее неизменность с учетом функционирующей системы защиты информации;
- осуществлять взаимодействие с подразделением по информационной безопасности, специалистом по информационной безопасности в части информирования о нештатных ситуациях и инцидентах, выявленных в процессе выполнения работ по поддержке функционирования информационных систем в сфере здравоохранения и информационно-телекоммуникационных сетей, обеспечивающих их функционирование;

- осуществлять взаимодействие с подразделением по информационной безопасности, специалистом по информационной безопасности в части информирования о планируемых и (или) произошедших изменениях в конфигурации информационных систем в сфере здравоохранения и информационно-телекоммуникационных сетей, обеспечивающих их функционирование;
- осуществлять взаимодействие с подразделением по информационной безопасности, специалистом по информационной безопасности в части выявления сбоев в функционировании средств защиты информации в информационных системах в сфере здравоохранения и информационно-телекоммуникационных сетях, обеспечивающих их функционирование;
- осуществлять взаимодействие с подразделением, эксплуатирующим информационные системы в сфере здравоохранения, по вопросам возникновения в процессе эксплуатации информационных систем в сфере здравоохранения нештатных ситуаций и инцидентов;
- осуществлять внутренний контроль за соблюдением установленных для информационных систем в сфере здравоохранения правил и процедур обработки и защиты информации;
- оказывать содействие подразделению по информационной безопасности, специалисту по информационной безопасности в части выполнения мероприятий по реагированию на инциденты информационной безопасности и принимать непосредственное участие в этих мероприятиях в объеме, предусмотренном в организационно-распорядительных документах по обеспечению информационной безопасности информационных систем в сфере здравоохранения.

Подразделения (работники), эксплуатирующие информационные системы в сфере здравоохранения, должны обеспечивать безопасность эксплуатируемых информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, в следующем объеме:

- осуществлять эксплуатацию информационных систем и информационно-телекоммуникационных сетей, обеспечивающих их функционирование, в соответствии с эксплуатационной документацией;
- выполнять требования по обеспечению информационной безопасности, закрепленные в организационно-распорядительных документах по обеспечению информационной безопасности информационных систем в сфере здравоохранения, при эксплуатации информационных систем в сфере здравоохранения;
- осуществлять взаимодействие с подразделением по информационной безопасности, специалистом по информационной безопасности в части информирования о нештатных ситуациях и инцидентах, выявленных в процессе эксплуатации информационных систем в сфере здравоохранения;
- осуществлять внутренний контроль за соблюдением установленных для эксплуатируемых подразделением информационных систем в сфере здравоохранения правил и процедур обработки и защиты информации;
- оказывать содействие подразделению по информационной безопасности, специалисту по информационной безопасности в части выполнения мероприятий по реагированию на инциденты информационной безопасности в объеме, предусмотренном в организационно-распорядительных документах по обеспечению информационной безопасности информационных систем в сфере здравоохранения.

Оператор информационных систем в сфере здравоохранения должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности информационных систем в сфере здравоохранения и о возможных угрозах безопасности информации.

Нормативные правовые акты ФСТЭК России устанавливают требования к составу и содержанию мер защиты информации для следующих видов объектов защиты:

- государственные информационные системы в сфере здравоохранения;
- информационные системы персональных данных;

- значимые объекты критической информационной инфраструктуры Российской Федерации.

Требования к реализации мер защиты устанавливаются в соответствии с правовыми актами Российской Федерации для информационных систем в сфере здравоохранения (включая информационно-телекоммуникационные сети и защищенные сети передачи данных). Использование для функционирования информационных систем в сфере здравоохранения информационных ресурсов и инфраструктуры сторонних организаций допускается только при выполнении требований по защите информации, установленных для информационных систем.

В случае если на информационную систему одновременно распространяются требования двух или более нормативных правовых актов, при реализации мер защиты информации должны быть учтены требования всех этих актов.

Правовые акты Российской Федерации определяют базовые меры защиты информационной системы и (или) информационно-телекоммуникационной сети. Выбор мер защиты, которые должны быть реализованы, производится обладателем информации по следующим правилам:

- на основании класса защищенности государственной информационной системы, уровня защищенности персональных данных и (или) категории значимости объекта критической информационной инфраструктуры в соответствии с требованиями соответствующего правового акта ФСТЭК России формируется базовый набор мер защиты информации;
- из базового набора могут исключаться меры защиты, непосредственно связанные с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе (процедура адаптации базового набора мер защиты);
- если адаптированный базовый набор мер защиты информации не обеспечивает блокирование или нейтрализацию всех угроз, включенных в модель угроз безопасности информации, в него включаются недостающие меры защиты информации, необходимые для противодействия угрозам (процедура уточнения адаптированного базового набора мер защиты информации).

Если уточненный адаптированный базовый набор мер защиты информации не обеспечивает полное соответствие требованиям о защите информации, установленным иными нормативными актами, в него также включаются дополнительные меры защиты информации (процедура дополнения уточненного адаптированного базового набора мер защиты информации). Требования к каждой выбранной мере защиты информации определяются в соответствии с правовыми актами ФСТЭК России[37].

4.3. Эскизные решения по реализации мер защиты информации в информационных системах в сфере здравоохранения

Настоящая Концепция определяет эскизные решения по реализации мер защиты информации в информационных системах в сфере здравоохранения. Эскизные решения по реализации мер защиты информации в информационных системах в сфере здравоохранения предназначены для разработки проектных решений по созданию и модернизации систем защиты информации в информационных системах в сфере здравоохранения.

На этапе проектирования системы защиты информации эскизные решения подлежат уточнению с учетом основных структурно-функциональных характеристик информационных систем, информационных технологий и особенностей функционирования информационных систем в сфере здравоохранения.

В эскизных решениях приведена реализация организационных и технических мер защиты информации, в том числе применение следующих средств защиты информации:

- средства управления доступом;
- средства доверенной загрузки;
- средства криптографической защиты информации;

---

[37] Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 г.

- средства межсетевого экранирования;
- средства сбора и анализа событий информационной безопасности;
- средства антивирусной защиты;
- средства обнаружения вторжений;
- средства анализа защищенности;
- средства резервного копирования и восстановления данных;
- средства защиты среды виртуализации.

Средства защиты информации от несанкционированного доступа (СрЗИ НСД) могут иметь программную или программно-аппаратную реализацию и обеспечивают предотвращение или существенное затруднение несанкционированного доступа к информации[38].

Средства доверенной загрузки (СДВ) могут иметь программную или программно-аппаратную реализацию и обеспечивают предотвращение несанкционированного доступа к программным и (или) техническим ресурсам средств вычислительной техники информационных систем в сфере здравоохранения на этапе их загрузки[39].

Средства криптографической защиты информации – это шифровальные (криптографические) средства защиты информации конфиденциального характера[40]. Средства криптографической защиты информации могут иметь программную или программно-аппаратную реализацию. В рамках эскизных решений рассматриваются следующие виды средств криптографической защиты:

- средства шифрования и средства имитозащиты, предназначенные для защиты каналов связи;
- средства электронной подписи.

Средства межсетевого экранирования (СМЭ) могут быть реализованы в виде локальных (однокомпонентных) или функционально-распределенных программных (программно-аппаратных) средств и обеспечивают контроль и фильтрацию в соответствии с заданными правилами проходящих через них информационных потоков[41].

Средства сбора и анализа событий информационной безопасности (ССИБ) обеспечивают централизованный автоматизированный сбор, первичную аналитическую обработку и хранение информации о событиях информационной безопасности.

Средства антивирусной защиты (САВЗ) представляют собой программные средства, реализующие функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации[42].

Система обнаружения вторжений (СОВ) представляет собой программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности[43].

Средства анализа защищенности (САЗ) предназначены для сбора и обработки сведений об уязвимостях и недостатках в настройке программного обеспечения, используемого в информационных системах в сфере здравоохранения.

---

[38] ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

[39] В соответствии с Требованиями к средствам доверенной загрузки, утвержденными Приказом ФСТЭК России от 27.09.2013 № 119.

[40] В соответствии с Приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

[41] В соответствии с Требованиями к межсетевым экранам, утвержденными Приказом ФСТЭК России от 09.02.2016 № 9.

[42] В соответствии с Требованиями к средствам антивирусной защиты, утвержденными Приказом ФСТЭК России от 20.03.2012 № 28.

[43] ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

Средства резервного копирования и восстановления данных (СРК) предназначены для копирования информации на резервный носитель информации в информационных системах в сфере здравоохранения и восстановления данных в случае аварийных ситуаций.

Средства защиты среды виртуализации (СЗСВ) предназначены для защиты виртуальных устройств обработки, хранения и (или) передачи данных, а также необходимых для их работы аппаратных и (или) программных средств[44].

Эскизные решения по реализации мер защиты информации в информационных системах в сфере здравоохранения приведены в приложении II.

[44] ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».

5. Основные принципы и подходы к выбору и (или) разработке программного обеспечения информационных систем в сфере здравоохранения

Информационные системы в сфере здравоохранения применяются для обработки информации, необходимой для обеспечения критических процессов, и (или) для управления, контроля критических процессов, связанных с оказанием медицинской помощи. Нарушение или прекращение функционирования таких информационных систем может привести к причинению ущерба жизни и здоровья граждан[45]. Такие системы в соответствии с законодательством Российской Федерации относятся к значимым объектам критической информационной инфраструктуры и подлежат защите в соответствии с требованиями правовых актов Российской Федерации в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Таким образом, на все информационные системы в сфере здравоохранения распространяются требования по безопасной разработке прикладного программного обеспечения, установленные правовыми актами ФСТЭК России:

- требования по безопасной разработке программного обеспечения;
- требования к испытаниям по выявлению уязвимостей в программном обеспечении;
- требования к поддержке безопасности программного обеспечения.

Требования по безопасной разработке программного обеспечения подразумевают:

- наличие руководства по безопасной разработке программного обеспечения;
- проведение анализа угроз безопасности информации программного обеспечения;
- наличие описания структуры программного обеспечения на уровне подсистем и результатов сопоставления функций программного обеспечения и интерфейсов, описанных в функциональной спецификации, с его подсистемами (для программного обеспечения, планируемого к применению в значимых объектах 1-й категории значимости).

Требования к проведению испытаний по выявлению уязвимостей в программном обеспечении подразумевают:

- проведение статического анализа исходного кода программы;
- проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей;
- проведение динамического анализа кода программы (для программного обеспечения, планируемого к применению в значимых объектах 1-й категории значимости).

Требования к поддержке безопасности программного обеспечения подразумевают:

- наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения;
- определение способов и сроков доведения разработчиком (производителем) программного обеспечения до его пользователей информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями программного обеспечения его обновлений, проверки их целостности и подлинности;
- наличие процедур информирования субъекта критической информационной инфраструктуры об окончании производства и (или) поддержки программного обеспечения (для программного обеспечения, планируемого к применению в значимых объектах 1-й категории значимости).

Указанные требования направлены на своевременное выявление и устранение ошибок и недостатков, приводящих к появлению уязвимостей в прикладном программном обеспечении информационных систем в сфере здравоохранения. Выполнение этих требований позволит минимизировать риски, связанные с использованием нарушителями таких уязвимостей.

---

[45] См. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Требования к безопасной разработке должны включаться в техническое задание при выборе, закупке, разработке и модернизации прикладного программного обеспечения для информационных систем в сфере здравоохранения. Выполнение требований по безопасной разработке оценивается на этапе проектирования системы и подтверждается при приемке информационной системы.

Прикладное программное обеспечение информационных систем в сфере здравоохранения, в котором реализованы функции безопасности, используемые при реализации мер защиты информации, является для защищаемых объектов средством защиты информации. Для такого программного обеспечения должна проводиться оценка соответствия требованиям к функциям безопасности в форме сертификации, испытаний или приемки. В случаях, установленных законодательством Российской Федерации, при выборе программного обеспечения информационной системы в сфере здравоохранения преимущественно должно использоваться российское программное обеспечение и оборудования, соответствующие требованиям безопасности, в том числе:

- требованиям по защите автоматизированного рабочего места разработчиков программного обеспечения
- требованиям по проверке наличия программных уязвимостей и ошибок конфигурации мобильных приложений, влияющих на информационную безопасность
- требованиям по применению дополнительных программных и программно-аппаратных защитных механизмов, в том числе установка необходимых обновлений для используемого программного обеспечения.

6. Основные принципы и подходы к мониторингу защиты информации в информационных системах в сфере здравоохранения. Обнаружение компьютерных атак и реагирование на инциденты информационной безопасности в информационных системах и объектах критической информационной инфраструктуры в сфере здравоохранения. Архитектура, эскизные решения

6.1. Основные принципы и подходы к мониторингу защиты информации в информационных системах в сфере здравоохранения. Обнаружение компьютерных атак и реагирование на инциденты информационной безопасности в информационных системах и объектах критической информационной инфраструктуры в сфере здравоохранения

Мониторинг защиты информации является неотъемлемой частью функционирования системы обеспечения информационной безопасности в сфере здравоохранения. Мониторинг защиты информации должен осуществляться на постоянной основе на двух уровнях:

- в рамках подсистемы защиты информации информационной системы (системы обеспечения безопасности значимого объекта критической информационной инфраструктуры);
- в рамках взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Мониторинг защиты информации в рамках подстистемы защиты информации информационной системы (системы обеспечения безопасности значимого объекта критической информационной инфраструктуры) осуществляется в соответствии с требованиями нормативных правовых актов ФСТЭК России путем реализации предусмотренных ими мер защиты информации.

Мониторинг защиты информации в рамках взаимодействия с ГосСОПКА в соответствии с требованиями правовых актов ФСБ России и Национального координационного центра по компьютерным инцидентам (НКЦКИ) путем установки средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак. При этом средства защиты, используемые для мониторинга защиты информации в рамках подсистемы защиты информации информационной системы (системы обеспечения безопасности значимого объекта критической информационной инфраструктуры), являются источниками данных для средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В целях реализации настоящей Концепции в правовых актах Минздрава России и отраслевых стандартах могут быть установлены дополнительные требования к мониторингу защиты информации.

Мониторинг защиты информации в информационных системах в сфере здравоохранения должен осуществляться на основе следующих принципов и подходов:

- осуществление мониторинга защиты информации на основе нормативной правовой базы Российской Федерации;
- разделение функций по осуществлению мониторинга между участниками системы обеспечения информационной безопасности в сфере здравоохранения;
- единство координации, контроля реализации, научно-технической и организационно-методической политики комплекса технических и организационных мер обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения;
- достаточность и рациональность использования сил обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Осуществление мониторинга защиты информации на основе нормативной правовой базы Российской Федерации

Мониторинг защиты информации в информационных системах в сфере здравоохранения должен осуществляться в соответствии с:

- требованиями правовых актов ФСБ России и НКЦКИ в области обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- требованиями правовых актов ФСТЭК России, устанавливающих состав и содержание мер защиты информации в информационных системах.

Мониторинг защиты информации в информационных системах в сфере здравоохранения должен быть основан на следующих подходах:

- события безопасности должны регистрироваться всеми источниками событий[46];
- состав данных о событиях безопасности, регистрируемых в информационных системах в сфере здравоохранения и информационно-телекоммуникационных сетях, обеспечивающих их функционирование, определяется отраслевыми стандартами, согласованными с ФСБ России;
- данные о событиях безопасности должны предоставляться в отраслевой центр мониторинга информационной безопасности в порядке, установленном Минздравом России;
- контроль эффективности мер защиты информации и внесение своевременных изменений в обеспечение защиты информации в информационных системах в сфере здравоохранения должны осуществляться в числе прочего на основе анализа данных о событиях безопасности;
- отраслевой центр информационной безопасности Минздрава России на основе анализа данных о событиях безопасности осуществляет корректирующие воздействий на уровне системы обеспечения информационной безопасности в сфере здравоохранения;
- меры по обнаружению, предупреждению и ликвидации последствий компьютерных атак и компьютерных инцидентов реализуются операторами информационных систем самостоятельно или с привлечением центров ГосСОПКА;
- центры ГосСОПКА привлекаются операторами информационных систем в сфере здравоохранения к реализации мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак и компьютерных инцидентов на основании заключаемых соглашений;
- отраслевой центр информационной безопасности Минздрава России является центром компетенции по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и компьютерных инцидентов в информационных системах в сфере здравоохранения.

Мониторинг защиты информации в информационных системах в сфере здравоохранения может включать в себя следующие способы контроля:

- контроль учетных записей операторов и администраторов систем, а также анализ парольной политики и стойкости аутентификационных данных администраторов и пользователей»;
- проверка наличия уязвимостей для выявления возможностей нарушителя и их подтверждения (в том числе повышение привилегий, создание учетных записей, внедрение дополнительных функциональных модулей и модулей управления, извлечение паролей и хэш-значений паролей, подмена размещенной информации и т.д.);
- защиту от утечек данных пользователей
- периодическое тестирование на выявление уязвимостей в средствах защиты информации.

[46] См. Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, утвержденными Приказом ФСБ России от 06.05.2019 № 196.

Разделение функций по осуществлению мониторинга между участниками системы обеспечения информационной безопасности в сфере здравоохранения

Деятельность по мониторингу защиты информации в информационных системах в сфере здравоохранения осуществляется следующими участниками системы обеспечения информационной безопасности:

- операторы информационных систем в сфере здравоохранения (субъекты критической информационной инфраструктуры);
- ведомственные и корпоративные центры ГосСОПКА;
- отраслевой центр информационной безопасности Минздрава России.

Операторы информационных систем в сфере здравоохранения:

- реализуют в информационных системах меры по мониторингу защиты информации, установленные требованиями правовых актов ФСТЭК России, и применяют для этого необходимые средства защиты информации;
- применяют в информационных системах и информационно-телекоммуникационных сетях средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в порядке, установленном законодательством Российской Федерации;
- информируют НКЦКИ и отраслевой центр информационной безопасности Минздрава России о компьютерных инцидентах в порядке, установленном правовыми актами и методическими документами ФСБ России, НКЦКИ и Минздрава России;
- предоставляют в отраслевой центр информационной безопасности Минздрава России инвентаризационную и иную информацию об информационных системах в сфере здравоохранения, а также информацию о событиях безопасности в порядке и в сроки, установленные Минздравом России.

Ведомственные и корпоративные центры ГосСОПКА:

- выполняют функции по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения в соответствии с требованиями правовых актов и методических рекомендаций ФСБ России и НКЦКИ;
- выполняют функции мониторинга защиты информации в информационных системах в сфере здравоохранения на основе соглашений, заключенных с операторами информационных систем;
- предоставляют операторам информационных систем средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак в случаях, предусмотренных заключенными соглашениями;
- предоставляют в НКЦКИ инвентаризационную информацию об информационных системах в сфере здравоохранения, находящихся в зоне их ответственности, в порядке и в сроки, установленные соглашениями, заключенными между центрами ГосСОПКА и НКЦКИ.

Отраслевой центр информационной безопасности Минздрава России:

- выполняет функции ведомственного центра ГосСОПКА в отношении информационных систем и иных объектов критической информационной инфраструктуры, включенных в зону его ответственности по решению Минздрава России;
- информирует операторов информационных систем и центры ГосСОПКА о выявленных уязвимостях критического уровня опасности, выявленных в прикладном программном обеспечении предназначенном для реализации функций назначения информационных систем в сфере здравоохранения;
- осуществляет контроль выполнения требований по защите информации в информационных системах в сфере здравоохранения и защищенных сетях передачи данных в пределах установленных полномочий;

- осуществляет сбор и обработку сведений, не составляющих государственную тайну, о состоянии защищенности информационных систем в сфере здравоохранения в пределах установленных полномочий;
- разрабатывает рекомендации по штатным нормативам структурных подразделений медицинской организаций, осуществляющих деятельность по обнаружению, предупреждению и ликвидации последствий компьютерных атак и компьютерных инцидентов.

Единство координации, контроля реализации, научно-технической и организационно-методической политики комплекса технических и организационных мер обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения

Деятельность по обнаружению, предупреждению и ликвидации последствий компьютерных атак осуществляется в соответствии с правовыми актами ФСБ России и методическими документами НКЦКИ.

Отраслевой центр информационной безопасности Минздрава России в ходе своей деятельности:

- принимает участие в определении и прогнозировании угроз безопасности информации, связанных с особенностями применения информационных технологий в сфере здравоохранения и реализации проектов по цифровизации сфере здравоохранения;
- разрабатывает и согласовывает с НКЦКИ проекты отраслевых стандартов и методических рекомендаций по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения.

Отраслевые стандарты по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения утверждаются Минздравом России и обязательны к применению операторами информационных систем в сфере здравоохранения и центрами ГосСОПКА в дополнение к методическим документам НКЦКИ.

Достаточность и рациональность использования сил обнаружения, предупреждения и ликвидации последствий компьютерных атак

Достаточность и рациональность использования сил обнаружения, предупреждения и ликвидации последствий компьютерных атак обеспечивается применением следующих подходов:

- силы обеспечения информационной безопасности операторов информационных системы в сфере здравоохранения решают задачи по обнаружению компьютерных атак и компьютерных инцидентов в порядке и объеме, предусмотренном эксплуатационной документацией информационных систем, планами действий в нештатных ситуациях и планами действий по реагированию на компьютерные атаки и ликвидации последствий компьютерных инцидентов;
- кадровый состав сил обеспечения информационной безопасности определяет оператор информационной системы с учетом рекомендуемых штатных нормативов, утвержденных Минздравом России;
- при обнаружении нештатных ситуаций, компьютерных атак и компьютерных инцидентов, не предусмотренных эксплуатационной документацией и планами реагирования, оператор информационной системы на основании заключенного соглашения привлекает силы центра ГосСОПКА;
- кадровый состав сил обнаружения, предупреждения и ликвидации последствий компьютерных атак центра ГосСОПКА определяется в соответствии с правовыми актами и методическими рекомендациями НКЦКИ;
- операторы информационных систем в сфере здравоохранения привлекают к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделения и должностных лиц ФСБ России в соответствии с планами реагирования на компьютерные инциденты

и принятия мер по ликвидации последствий компьютерных атак, согласованными с ФСБ России[47].

6.2. Архитектура, эскизные решения построения системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

Система реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения представляет собой совокупность сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, и используемых ими технических, программных, программно-аппаратных и иных средств.

Архитектура системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения приведена в приложении III.

К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся подразделения и должностные лица, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, следующих категорий участников системы реагирования на компьютерные атаки и инциденты информационной безопасности информационных систем в сфере здравоохранения:

- операторы информационных систем в сфере здравоохранения (субъекты критической информационной инфраструктуры);
- ведомственные и корпоративные центры ГосСОПКА;
- отраслевой центр информационной безопасности Минздрава России;
- главный центр ГосСОПКА.

К средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся:

- средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, которые применяются операторами в информационных системах в сфере здравоохранения и информационно-телекоммуникационных системах, обеспечивающих их функционирование;
- средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, применяемые центрами ГосСОПКА, отраслевым центром информационной безопасности Минздрава России, главным центром ГосСОПКА.

Технические средства, программные средства и средства защиты информации информационных систем в сфере здравоохранения применяются для реализации мер защиты информации в информационных системах и служат источниками данных для обнаружения и предупреждения компьютерных атак. К таким средствам относятся:

- средства защиты информации от несанкционированного доступа;
- средства криптографической защиты информации;
- средства межсетевого экранирования;
- средства антивирусной защиты;
- средства обнаружения вторжений;
- средства анализа защищенности;
- средства резервного копирования и восстановления данных;
- средства защиты среды виртуализации;
- средства сбора и обработки событий безопасности;
- программные, программно-технические средства информационных систем.

---

[47] См. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный Приказом ФСБ России от 19.06.2019 № 282.

Центры ГосСОПКА, отраслевой центр информационной безопасности Минздрава России и операторы информационных систем в сфере здравоохранения применяют следующие средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и инцидентов информационной безопасности:

- технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак, обеспечивающие:
  - сбор и обработку событий информационной безопасности;
  - автоматический анализ событий информационной безопасности и выявление инцидентов информационной безопасности;
  - повторный анализ ранее зарегистрированных событий информационной безопасности и выявление на основе такого анализа не обнаруженных ранее инцидентов информационной безопасности;
- технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак, обеспечивающие:
  - сбор и обработку сведений об инфраструктуре контролируемых информационных ресурсов;
  - сбор и обработку сведений об уязвимостях и недостатках в настройке программного обеспечения, используемого в контролируемых информационных ресурсах, и формирование рекомендаций по минимизации угроз безопасности информации;
  - учет угроз безопасности информации;
- технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак, обеспечивающие:
  - учет и обработку инцидентов информационной безопасности;
  - взаимодействие с НКЦКИ и с операторами информационных систем в сфере здравоохранения;
- технические, программные, программно-аппаратные и иные средства обмена информацией, необходимой при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак;
- криптографические средства защиты информации, необходимой при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Назначение каждого из указанных средств и эскизные решения по их применению приведены в приложении IV.

7. Основные этапы реализации концепции

Первоочередными направлениями реализации настоящей Концепции являются:

- обеспечение защиты информации в информационных системах и безопасности значимых объектов критической информационной инфраструктуры в сфере здравоохранения;
- совершенствование нормативно-правовой базы Российской Федерации в области защиты информации в информационных системах в сфере здравоохранения;
- создание отраслевого центра обеспечения информационной безопасности Минздрава России и централизация сил обеспечения информационной безопасности в сфере здравоохранения;
- разработка единых подходов и требований к созданию и развитию защищенных сетей передачи данных, функционирующих в сфере здравоохранения;
- развитие отраслевого сегмента ГосСОПКА, включающего в себя всех участников системы обеспечения информационной безопасности в сфере здравоохранения.

Совершенствование нормативно-правовой базы Российской Федерации в области защиты информации в информационных системах в сфере здравоохранения включает в себя:

- разработку перечня правовых актов Российской Федерации и предложений по их актуализации, необходимых для реализации настоящей Концепции;
- разработку отраслевых документов стратегического планирования в области защиты информации в сфере здравоохранения;
- разработку проектов правовых актов Российской Федерации, устанавливающих полномочия, права, обязанности и разграничение ответственности участников системы обеспечения информационной безопасности в сфере здравоохранения;
- разработку и утверждение правовых актов, устанавливающих порядок осуществления ведомственного контроля за выполнением требований по защите информации в информационных системах в сфере здравоохранения.

Создание отраслевого центра обеспечения информационной безопасности Минздрава России и централизация сил обеспечения информационной безопасности в сфере здравоохранения включают в себя:

- принятие решения о создании отраслевого центра информационной безопасности Минздрава России
- утверждение положения об отраслевом центре информационной безопасности Минздрава России;
- создание на базе отраслевого центра информационной безопасности Минздрава России органа по аттестации;
- заключение между Минздравом России и ФСБ России соглашения о взаимодействии в области обнаружения, предупреждения и ликвидации компьютерных атак, наделяющего отраслевой центр информационной безопасности Минздрава России функциями ведомственного центра ГосСОПКА.

Разработка единых подходов и требований к созданию и развитию защищенных сетей передачи данных, функционирующих в сфере здравоохранения, включает в себя:

- разработку, согласование и утверждение отраслевых стандартов и методических рекомендаций по защите информации в защищенных сетях передачи данных в сфере здравоохранения;
- создание и (или) модернизацию защищенных сетей передачи данных в соответствии с отраслевыми стандартами и методическими рекомендациями по защите информации.

Развитие отраслевого сегмента ГосСОПКА, объединяющего всех участников системы обеспечения информационной безопасности в сфере здравоохранения, включает в себя:

- разработку, согласование и утверждение правовых актов Российской Федерации, определяющих полномочия отраслевого центра информационной безопасности Минздрава России в рамках отраслевого сегмента ГосСОПКА по координации сил и средств обеспечения информационной безопасности в сфере здравоохранения при

обнаружении компьютерных атак, реагировании на инциденты, ликвидации их последствий;

- разработку, согласование и утверждение правовых актов Российской Федерации, устанавливающих состав сведений, предоставляемых участниками системы обеспечения информационной безопасности в сфере здравоохранения отраслевому центру информационной безопасности Минздрава России, порядок и сроки их предоставления;
- реализацию операторами информационных систем в сфере здравоохранения и центрами ГосСОПКА в соответствии с правовыми актами Российской Федерации мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы в сфере здравоохранения.

Реализация настоящей Концепции по указанным направлениям осуществляется в три этапа:

- разработка программы развития системы обеспечения информационной безопасности в сфере здравоохранения, создание отраслевого центра информационной безопасности Минздрава России;
- апробация программы развития системы обеспечения информационной безопасности в сфере здравоохранения в рамках пилотной зоны;
- реализация программы развития системы обеспечения информационной безопасности в сфере здравоохранения с охватом всех участников системы обеспечения информационной безопасности в сфере здравоохранения на федеральном уровне, уровне субъектов Российской Федерации и муниципальном уровне.

На этапе разработки программы развития системы обеспечения информационной безопасности в сфере здравоохранения, создания отраслевого центра информационной безопасности Минздрава России осуществляются:

- разработка, согласование и утверждение проектных решений по техническому, программному, информационному, нормативному, кадровому обеспечению, необходимых для осуществления деятельности отраслевого центра информационной безопасности;
- закупка и внедрение технического, программного обеспечения и средств защиты, необходимых для организации деятельности отраслевого центра информационной безопасности в соответствии с проектными решениями;
- организация подготовки кадров, необходимых для осуществления деятельности отраслевого центра информационной безопасности Минздрава России;
- разработка проектов системообразующих правовых актов Российской Федерации и проектов отраслевых стандартов по защите информации.

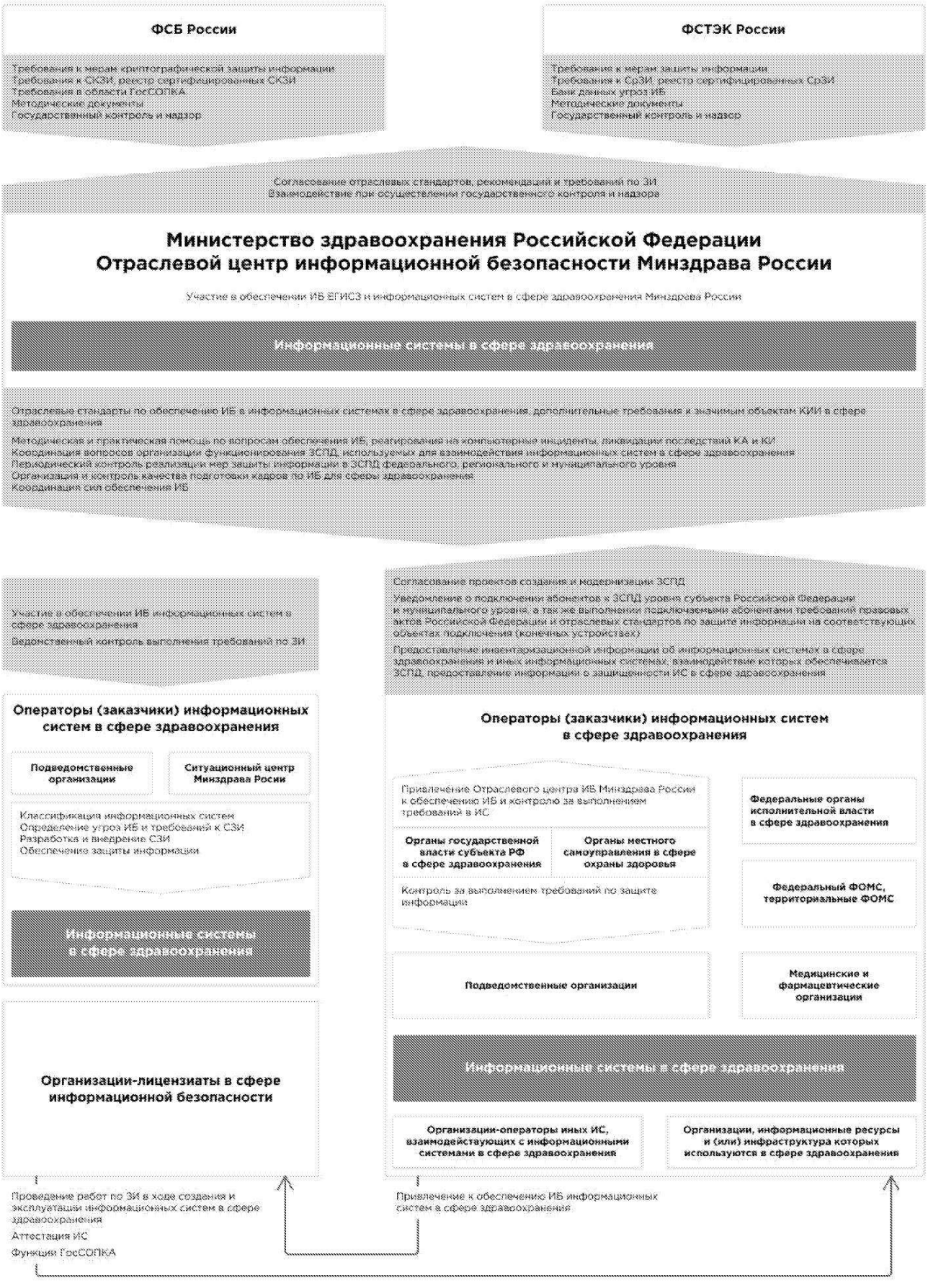
Апробация программы развития системы обеспечения информационной безопасности в сфере здравоохранения осуществляется в рамках пилотной зоны, определяемой решением Минздрава России. На этапе апробации производится реализация участниками системы обеспечения информационной безопасности в сфере здравоохранения, входящими в пилотную зону, мероприятий и технических решений, предусмотренных проектами правовых актов Российской Федерации и отраслевых стандартов Минздрава России, разработанными на этапе разработки программы развития системы обеспечения информационной безопасности в сфере здравоохранения.

Реализация программы развития системы обеспечения информационной безопасности в сфере здравоохранения на федеральном уровне, уровне субъектов Российской Федерации и муниципальном уровне включает в себя:

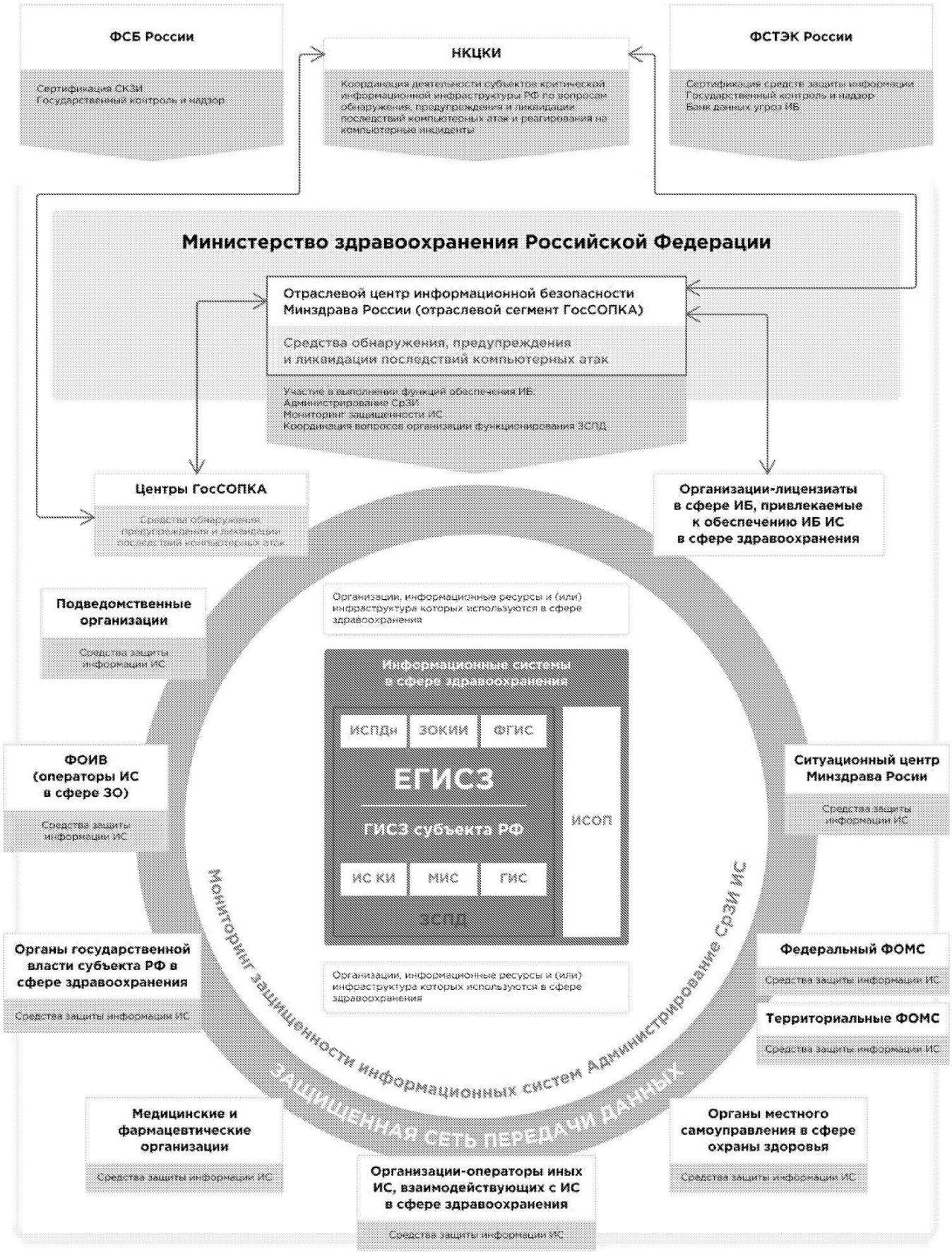
- актуализацию документов стратегического планирования на основе результатов апробации программ создания системы обеспечения информационной безопасности в сфере здравоохранения;
- реализацию программ создания системы обеспечения информационной безопасности в сфере здравоохранения в соответствии с актуализированными документами стратегического планирования.

Приложение I

Архитектура системы обеспечения информационной безопасности в сфере здравоохранения. Организационная схема



Архитектура системы обеспечения информационной безопасности в сфере здравоохранения. Функциональная схема



Приложение II
Эскизные решения по реализации мер защиты информации в информационных системах в сфере здравоохранения

1. Порядок реализации мер защиты информации в информационных системах в сфере здравоохранения

В таблице приведены порядок реализации мер защиты информации в информационных системах в сфере здравоохранения и результаты на каждом этапе реализации.

№ п/п	Мероприятия по реализации мер защиты	Способ реализации (результат)		
		ГИС	**ИСПДн**	**ЗОКИИ**
	Принятие решения о необходимости защиты информации, содержащейся в информационной системе в сфере здравоохранения	Концепция создания системы[48]		
		Приказ о создании системы защиты информации информационной системы		
	Назначение лица, ответственного за организацию и контроль обеспечения ИБ в информационной системе в сфере здравоохранения	Приказ о назначении лица, ответственного за организацию обеспечения ИБ в информационной системе в сфере здравоохранения на уровне не ниже заместителя руководителя		
	Назначение структурного подразделения либо должностного лица, ответственного за обеспечение ИБ в информационной системе в сфере здравоохранения	Приказ о создании структурного подразделения либо о назначении должностного лица, ответственного за обеспечение ИБ в информационной системе в сфере здравоохранения Положение о структурном подразделении (инструкция) ответственного за обеспечение ИБ		
	Проведение классификации информационной системы Проведение категорирования объектов КИИ Определение уровня защищенности персональных данных при их обработке в информационной системе	Акт классификации информационной системы по требованиям защиты информации	Акт определения уровня защищенности персональных данных при их обработке в информационной системе	Приказ о создании постоянно действующей комиссии по категорированию объектов КИИ Положение о постоянно действующей комиссии по категорированию объектов КИИ Письмо во ФСТЭК России о направлении перечня объектов критической информационной инфраструктуры, подлежащих категорированию Перечень объектов критической информационной инфраструктуры, подлежащих категорированию Акт категорирования объекта КИИ Письмо во ФСТЭК России о направлении сведений о результатах присвоения объекту критической информационной

[48] В соответствии с Постановлением Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

№ п/п	Мероприятия по реализации мер защиты	Способ реализации (результат)		
		ГИС	**ИСПДн**	**ЗОКИИ**
				инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий
	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработка на их основе модели угроз безопасности информации	Модель угроз безопасности информации информационной системы, согласованная со ФСТЭК России и ФСБ России в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации (в случае, если реализация мероприятий по созданию информационной системы или системы защиты осуществляется федеральным органом исполнительной власти или органом исполнительной власти субъекта Российской Федерации[49])	Модель угроз безопасности информации информационной системы	Модель угроз безопасности информации информационной системы
	Определение (формирование) требований по защите информации в информационной системе в сфере здравоохранения	Техническое задание на создание системы защиты информации информационной системы в сфере здравоохранения, согласованное со ФСТЭК России и ФСБ России в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации (в случае, если реализация мероприятий по созданию информационной системы или системы защиты осуществляется федеральным органом исполнительной власти или органом исполнительной власти субъекта Российской Федерации[49])	Техническое задание на создание системы защиты информации информационной системы в сфере здравоохранения	Техническое задание на создание системы защиты информации информационной системы в сфере здравоохранения
	Разработка системы защиты информации информационной системы в сфере здравоохранения	Проектная документация (эскизный (технический) проект и рабочая документация) на информационную систему (систему защиты информации информационной системы), разрабатываемая с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» Эксплуатационная документация на систему защиты информации информационной системы		
	Внедрение системы защиты информации информационной системы в сфере здравоохранения	Акты и протоколы установки и настройки средств защиты информации в информационной системе Организационно-распорядительные документы по защите информации Программа и методика предварительных испытаний Протокол предварительных испытаний Акт приемки информационной системы (системы защиты информации) в опытную эксплуатацию Программа опытной эксплуатации Протокол проведения анализа уязвимостей информационной системы Программа и методика приемочных испытаний Протокол приемочных испытаний		

[49] В соответствии с Постановлением Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

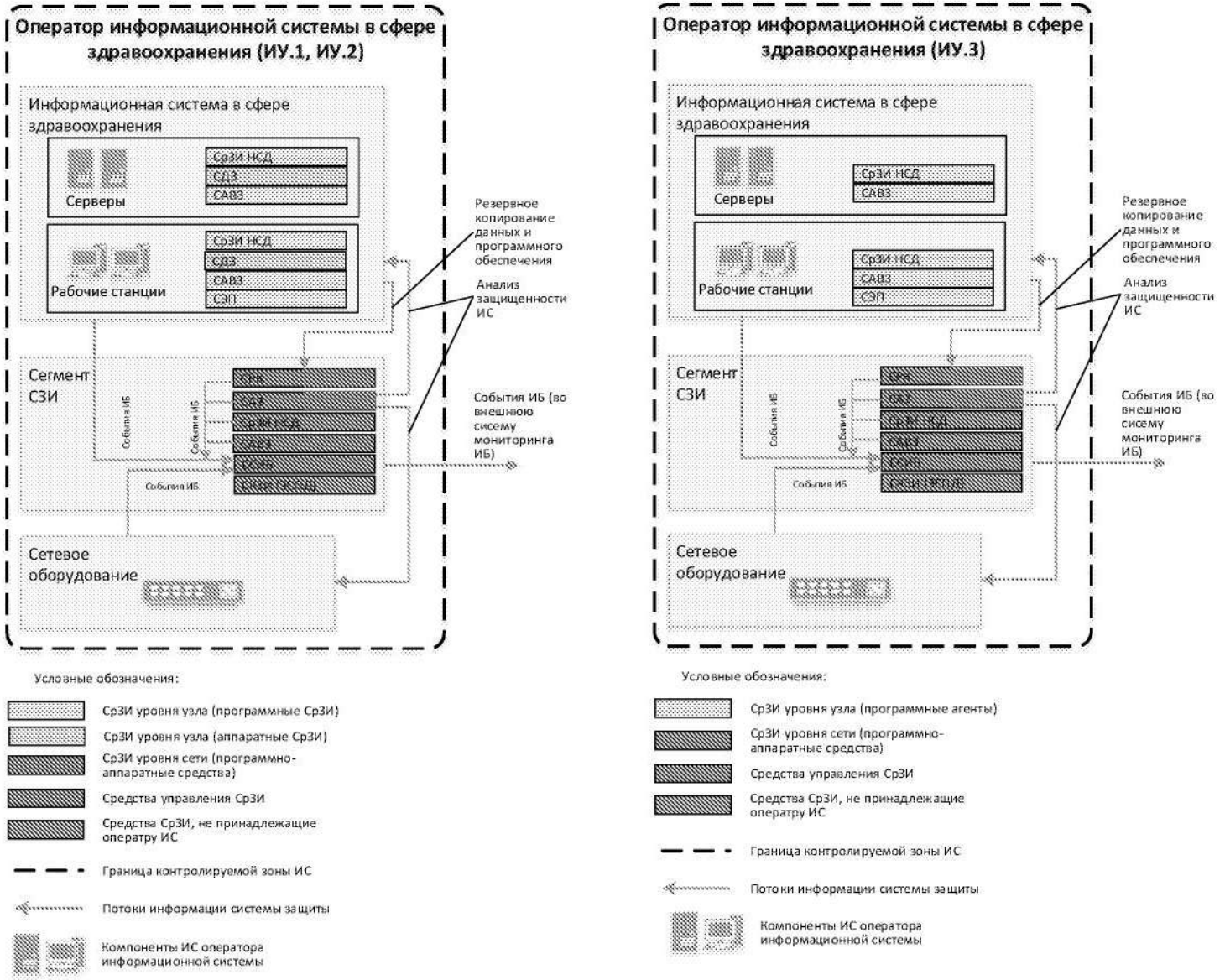
№ п/п	Мероприятия по реализации мер защиты	Способ реализации (результат)		
		ГИС	**ИСПДн**	**ЗОКИИ**
	Аттестация информационной системы в сфере здравоохранения	Программа и методики аттестационных испытаний[50]* Аттестат соответствия Заключение Протоколы испытаний		
	Ввод в эксплуатацию системы защиты информационной системы в сфере здравоохранения	Акт о вводе системы защиты в эксплуатацию		
	Обеспечение защиты информации в ходе эксплуатации информационной системы в сфере здравоохранения	В соответствии перечнем организационных мероприятий по обеспечению информационной безопасности (п. 2 Приложения II)		
	Обеспечение защиты информации при выводе из эксплуатации информационной системы в сфере здравоохранения или после принятия решения об окончании обработки информации	Акт о выводе системы из эксплуатации Документы (акты, протоколы), подтверждающие архивирование информации ИС и (или) уничтожение информации в ИС Документы (акты, протоколы), подтверждающие уничтожение носителей информации в ИС	Акт о выводе системы из эксплуатации Документы (акты, протоколы), подтверждающие архивирование ПДн в ИС и (или) уничтожение ПДн в ИС Документы (акты, протоколы), подтверждающие уничтожение носителей ПДн в ИС	Акт о выводе системы из эксплуатации Документы (акты, протоколы), подтверждающие архивирование информации ИС и (или) уничтожение информации в ИС Документы (акты, протоколы), подтверждающие уничтожение носителей информации в ИС

[50] См. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29.04.2021 № 77

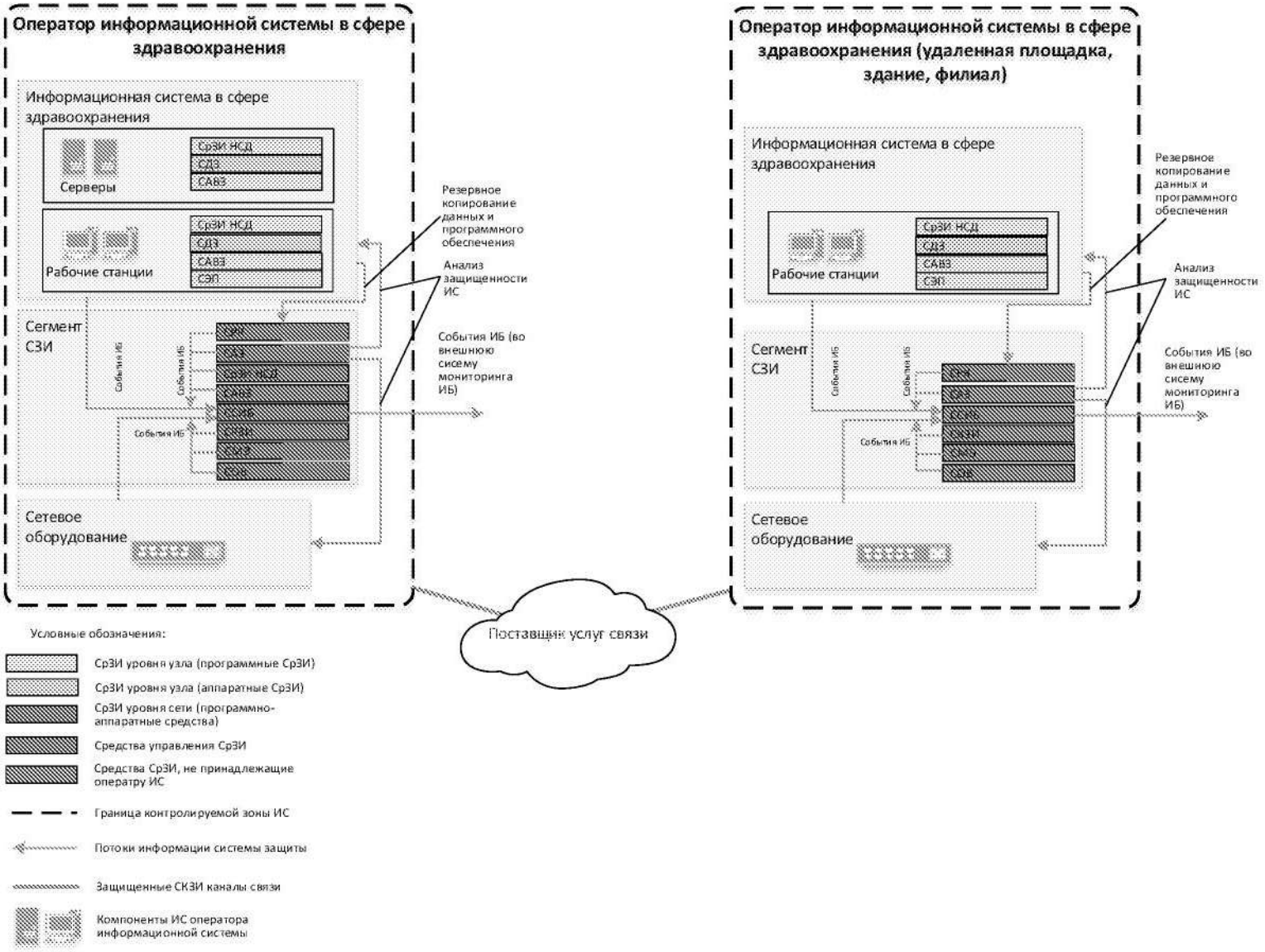
2. Необходимость использования оператором средств защиты информации

Средства защиты	Архитектура / унифицированный класс защиты ИС											
	Инфраструктура оператора (все компоненты информационной системы и каналы связи расположены в пределах контролируемой зоны оператора информационной системы)			Инфраструктура как услуга (часть компонентов информационной системы, а также каналы связи предоставляются поставщиком услуг в качестве сервисов и выходят за пределы контролируемой зоны оператора информационной системы)			Платформа как услуга (часть компонентов информационной системы, включая связующее программное обеспечение, а также каналы связи предоставляются поставщиком услуг в качестве сервисов и выходят за пределы контролируемой зоны оператора)			Программное обеспечение как услуга (компоненты информационной системы, включая программное обеспечение, предоставляются поставщиком услуг в качестве сервисов, доступ к которым осуществляется через тонкие клиенты по каналам связи, выходящим за пределы контролируемой зоны оператора информационной системы)		
	ИО.1	**ИО.2**	**ИО.3**	**ИУ.1**	**ИУ.2**	**ИУ.3**	**ПУ.1**	**ПУ.2**	**ПУ.3**	**ПОУ.1**	**ПОУ.2**	**ПОУ.3**
СрЗИ НСД	Необходимо использовать									Не требуются		
СДЗ	Необходимо использовать		Не требуются	Необходимо использовать		Не требуются	Необходимо использовать		Не требуются	Не требуются		
СЭП	Требуются при необходимости использования ЭП											
СМЭ	Необходимо использовать при сопряжении с другими ИС оператора и (или) с внешними сетями, включая сеть Интернет			Необходимо использовать								
СКЗИ	Не требуются			Необходимо использовать						Необходимо использовать		
ССИБ	Необходимо использовать											
САВЗ	Необходимо использовать											
СОВ	Необходимо использовать при сопряжении с другими ИС оператора и (или) с внешними сетями, включая сеть Интернет		Не требуются	Необходимо использовать		Не требуются	Необходимо использовать		Не требуются	Необходимо использовать		Не требуются
САЗ	Необходимо использовать											
СРК	Необходимо использовать									Не требуются		
СЗСВ	Требуются при использовании в ИС средств виртуализации									Не требуются (не применяются технологии виртуализации в инфраструктуре оператора ИС)		

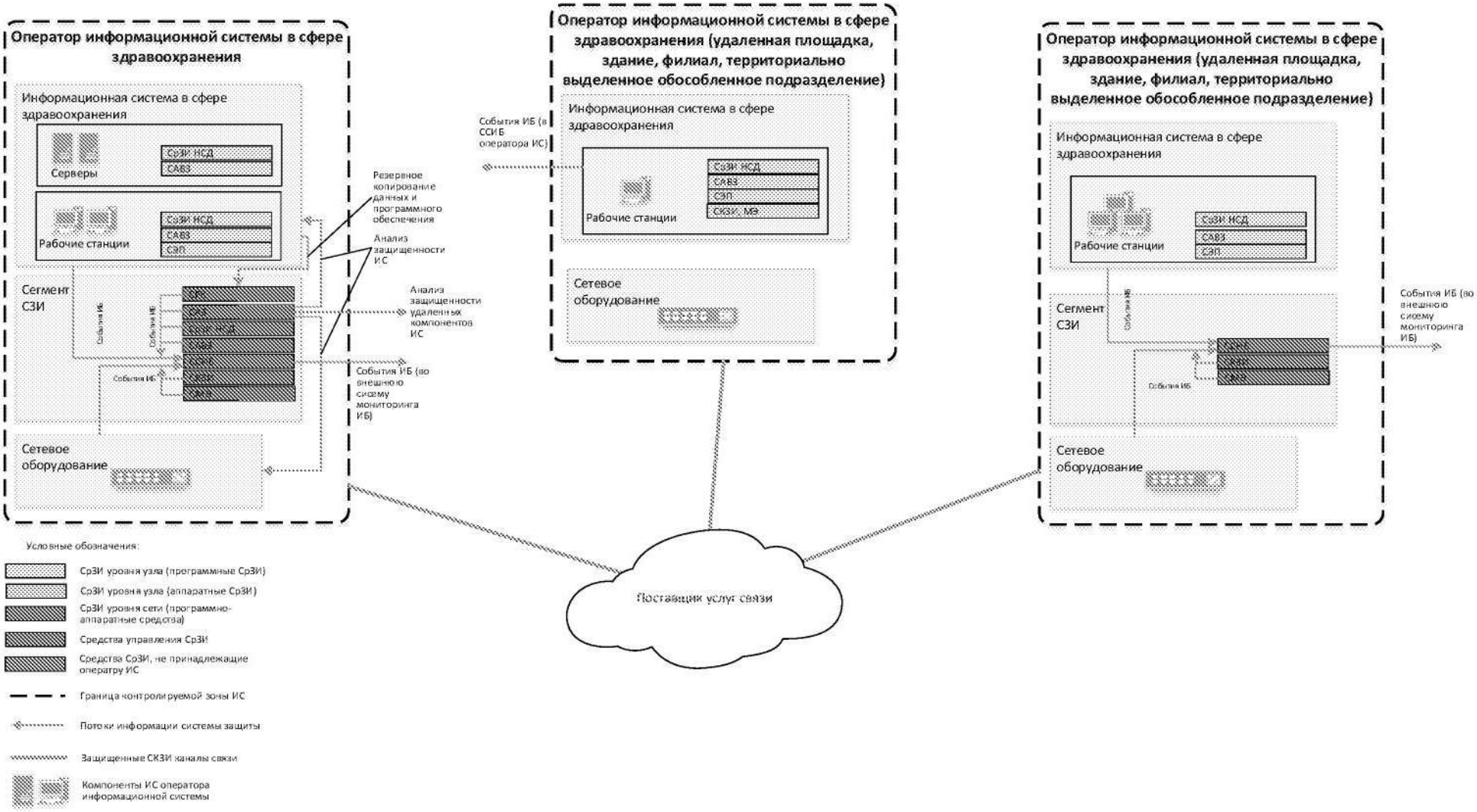
2.1. Эскизные решения для информационных систем при размещении всех технических средств в инфраструктуре оператора информационной системы



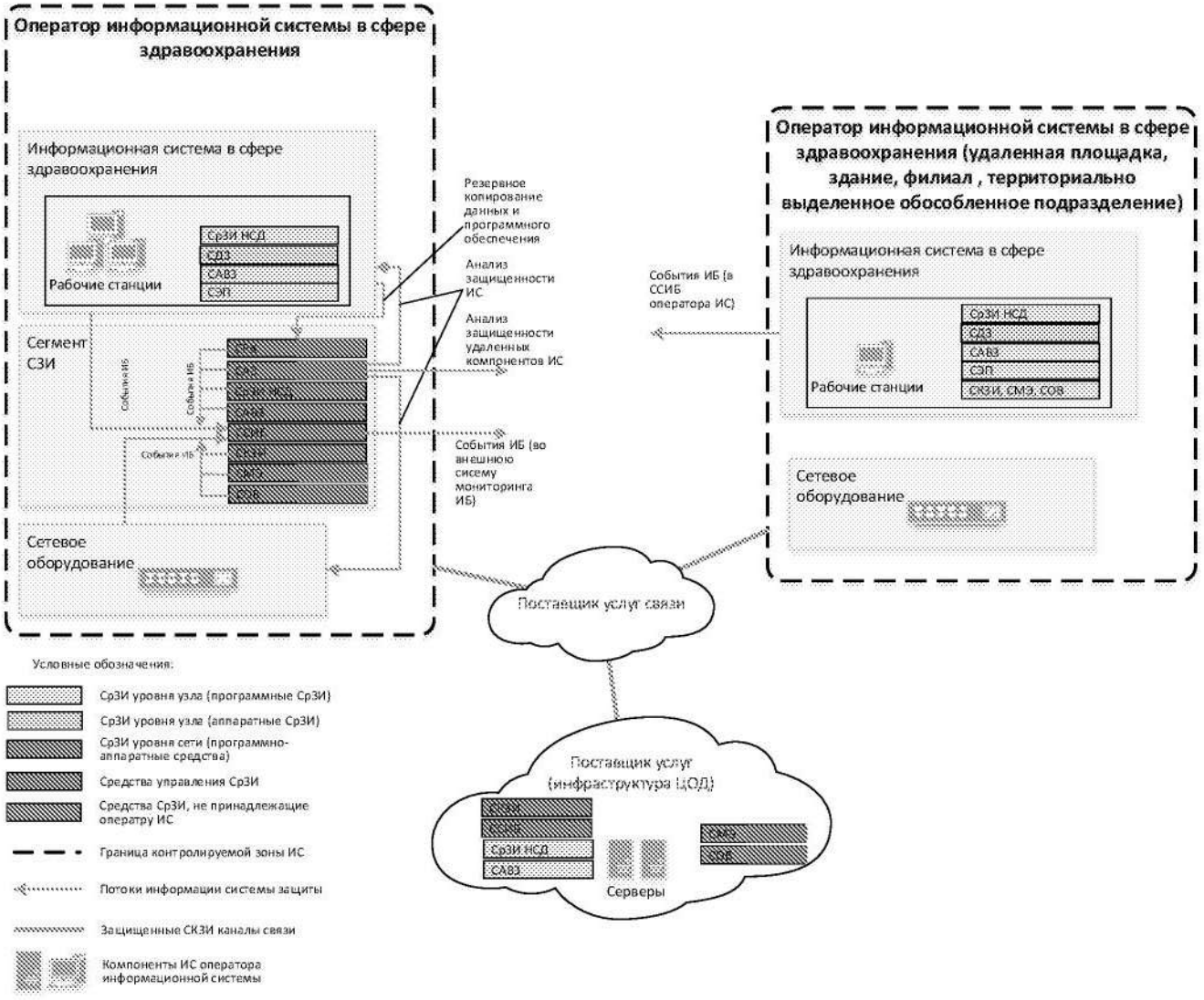
2.2. Эскизные решения для информационных систем классов защищенности 2 и 1 при использовании облачных услуг по модели «инфраструктура как услуга»



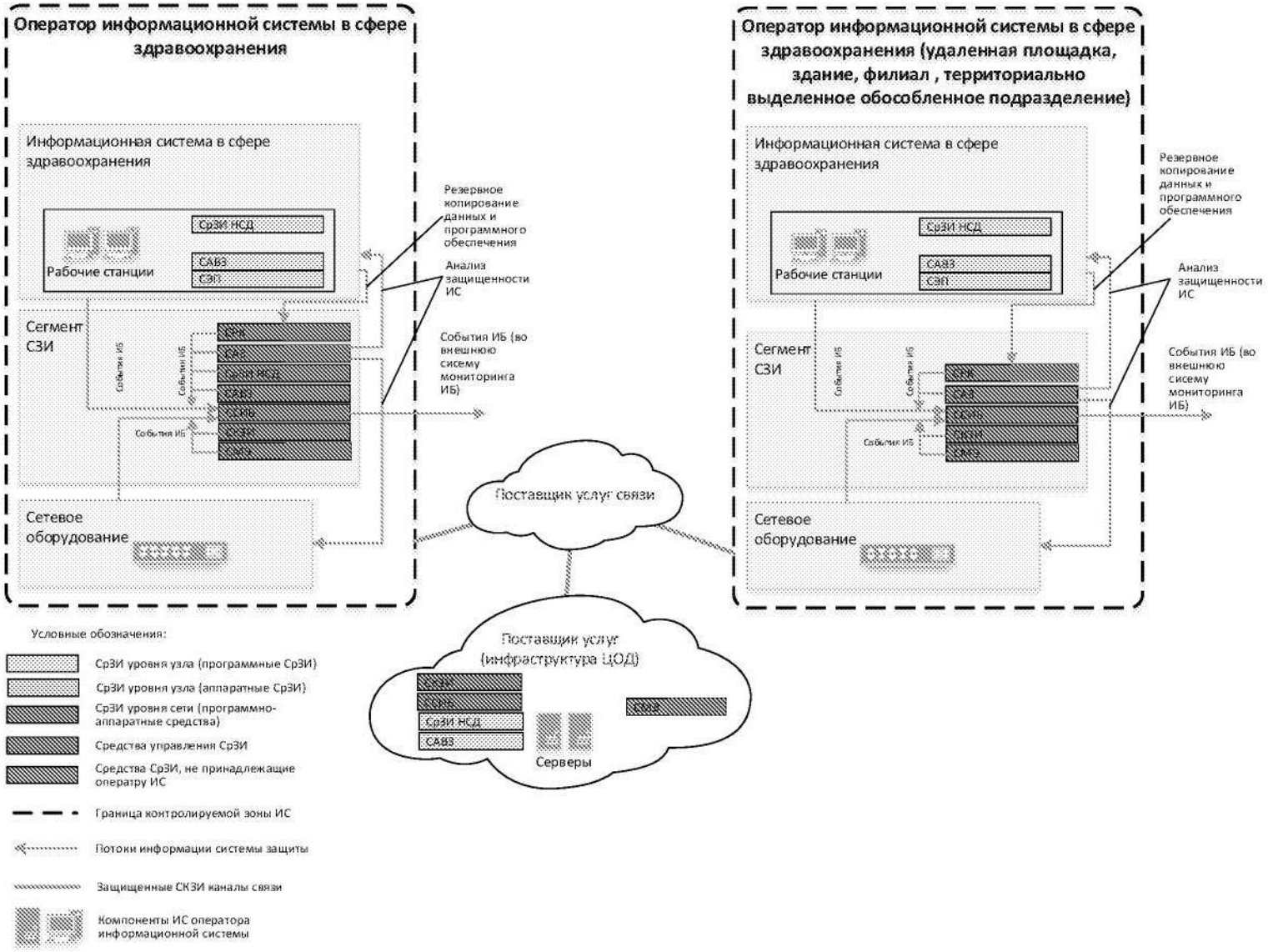
2.3. Эскизные решения для информационных систем класса защищенности 3 при использовании облачных услуг по модели «инфраструктура как услуга»



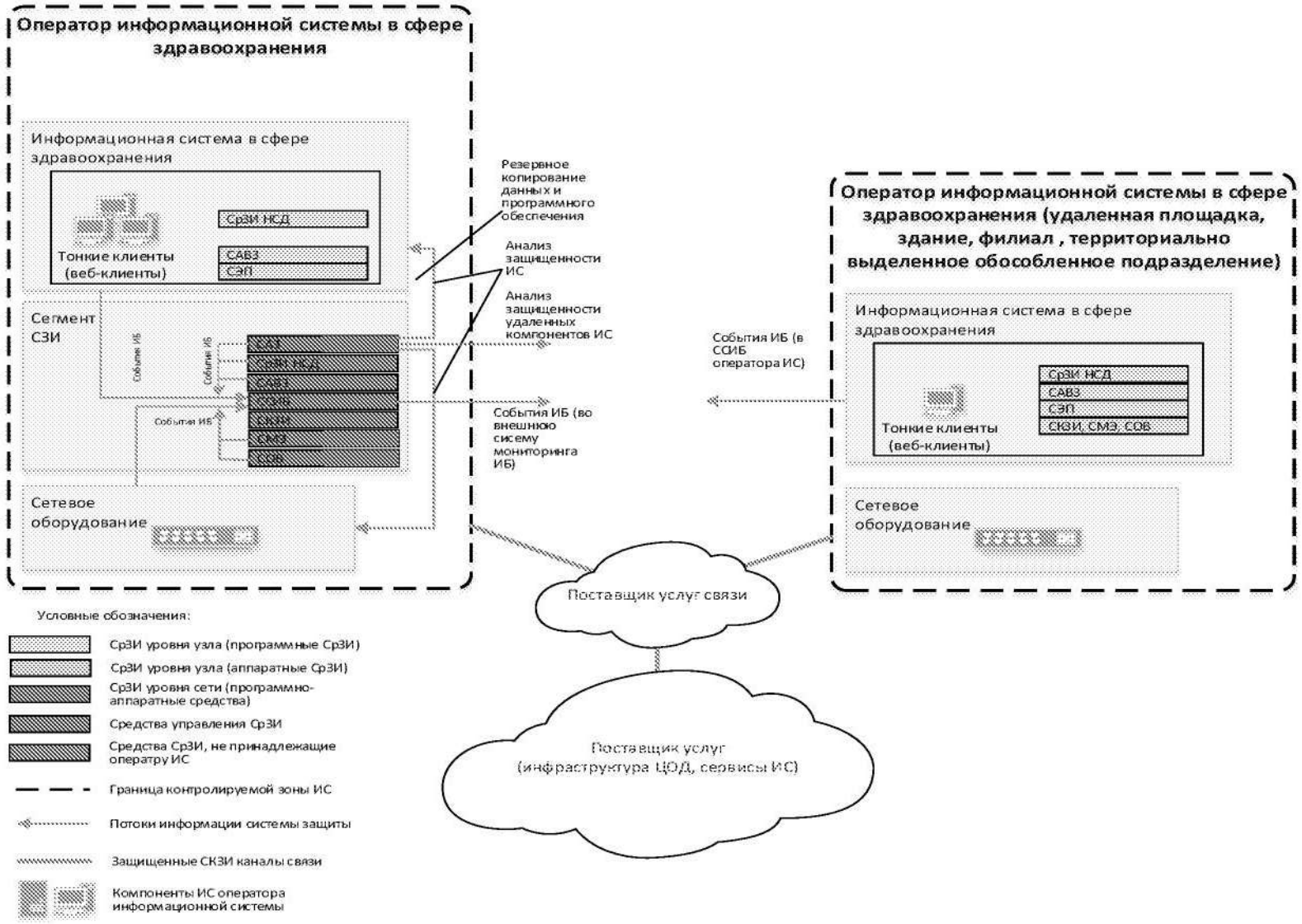
2.4. Эскизные решения для информационных систем классов защищенности 2 и 1 при использовании облачных услуг по модели «платформа как услуга»



2.5. Эскизные решения для информационных систем класса защищенности 3 при использовании облачных услуг по модели «платформа как услуга»



2.6. Эскизные решения для информационных систем при использовании облачных услуг по модели «программное обеспечение как услуга»



3. Решения по организационно-техническим мероприятиям

Реализация мер защиты информации информационных систем включает, помимо применения технических средств защиты, выполнение организационных мероприятий. К организационным мероприятиям по обеспечению защиты информации в информационных системах относится разработка локальных нормативных актов, инструкций, правил, регламентов и других организационно-распорядительных документов, касающихся организации защиты информации, утверждаемых руководителем организации или уполномоченным им должностным лицом. Контроль выполнения организационных мероприятий по обеспечению информационной безопасности должен быть возложен на уполномоченное лицо, назначенное приказом руководителя организации.

Перечень организационных мероприятий по обеспечению информационной безопасности в организации для информационных систем в сфере здравоохранения представлен в таблице.

№	Название мероприятия	Результат мероприятия	Примечание
1.	**Мероприятия по обеспечению безопасности ПДн**	**Организационно-распорядительная документация и локальные нормативные акты по обеспечению безопасности ПДн**	Мероприятия проводятся, если в информационной системе обрабатываются ПДн
1.1	Назначение ответственного за организацию обработки ПДн	Приказ о назначении ответственного за организацию обработки ПДн Инструкция ответственного за организацию обработки ПДн	Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)
1.2	Разработка документа, определяющего политику оператора информационной системы в отношении обработки персональных данных	Политика оператора информационной системы в отношении обработки персональных данных обработки персональных данных	
1.3	Разработка положения по организации и проведению работ обеспечению безопасности ПДн	Приказ об утверждении положения по организации и проведению работ обеспечению безопасности ПДн Положение по организации и проведению работ обеспечению безопасности ПДн	
1.4	Разработка правил рассмотрения запросов субъектов персональных данных или их представителей	Правила рассмотрения запросов субъектов персональных данных или их представителей	Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)
1.5	Разработка правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)
1.6	Разработка правил работы с обезличенными данными в случае обезличивания персональных данных	Правила работы с обезличенными данными в случае обезличивания персональных данных	Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)
1.7	Определение перечня должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных	Приказ об утверждении перечня должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных	Разрабатывается в том случае, если оператор информационной системы в сфере здравоохранения является государственным или муниципальным органом Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)

№	Название мероприятия	Результат мероприятия	Примечание
1.8	Разработка типового обязательства служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей	Типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей	Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)
1.9	Разработка типовой формы согласия на обработку персональных данных, а также типовой формы разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные	Типовая форма согласия на обработку персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные	Мероприятие проводится при создании информационной системы (до начала создания системы защиты информации)
1.1	Разработка типовой формы согласия на обработку общедоступных персональных данных	Типовая форма согласия на обработку общедоступных персональных данных	
1.1	Выделение помещения (помещений), в котором производится обработка ПДн	Приказ о выделении помещения (помещений), в котором производится обработка ПДн	
1.1	Формирование комиссии по определению уровня защищенности ПДн при их обработке в информационной системе	Приказ о составе комиссии по определению уровня защищенности ПДн при их обработке в информационной системе Положение о комиссии по определению уровня защищенности ПДн при их обработке в информационной системе	
1.1	Разработка плана мероприятий по защите ПДн в ИС	План мероприятий по защите ПДн в ИС	
1.1	Определение уровня защищенности персональных данных при их обработке в информационной системе	Акт определения уровня защищенности персональных данных при их обработке в информационной системе	
1.1	Определение перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	Приказ об утверждении перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	
1.1	Разработка и утверждение правил доступа в помещения, в которых производится обработка конфиденциальной информации, в том числе ПДн, в рабочее и нерабочее время, а также в нештатных ситуациях	Правила доступа в помещения, в которых производится обработка конфиденциальной информации, в том числе ПДн, в рабочее и нерабочее время, а также в нештатных ситуациях	
1.1	Утверждение списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии	Приказ об утверждении списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии	Для ИС 1-го и 2-го унифицированных классов защиты
1.1	Назначение лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям	Приказ о назначении лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям	Для ИС 1-го унифицированного класса защиты
1.1	Определение и утверждение мест хранения материальных носителей персональных данных	Приказ об утверждении мест хранения материальных носителей персональных данных	
1.2	Формирование комиссии по уничтожению документов с ПДн	Приказ о назначении комиссии по уничтожению документов с ПДн Положение о комиссии по уничтожению документов с ПДн	

№	Название мероприятия	Результат мероприятия	Примечание
1.2	Организация охраны, внутриобъектового режима и порядка допуска лиц в помещения, в которых ведется обработка персональных данных	Приказ об утверждении инструкции, определяющей порядок охраны, внутриобъектовый режим и порядок допуска лиц в помещения, в которых ведется обработка персональных данных Инструкция, определяющая порядок охраны, внутриобъектовый режим и порядок допуска лиц в помещения, в которых ведется обработка персональных данных	
1.2	Организация охраны, внутриобъектового режима и порядка допуска лиц в помещения, в которых установлены СКЗИ или хранятся ключевые документы	Приказ об утверждении инструкции, определяющей порядок охраны, внутриобъектовый режим и порядок допуска лиц в помещения, в которых установлены СКЗИ или хранятся ключевые документы Инструкция, определяющая порядок охраны, внутриобъектовый режим и порядок допуска лиц в помещения, в которых установлены СКЗИ или хранятся ключевые документы	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.2	Определение перечня лиц, имеющих право доступа в помещения с элементами ИСПДн	Приказ об утверждении перечня лиц, имеющих право доступа в помещения с элементами ИСПДн Перечень лиц, имеющих право доступа в помещения с элементами ИСПДн	
1.2	Определение перечня ПДн, обрабатываемых в информационной системе	Приказ об утверждении перечня ПДн, обрабатываемых в информационной системе Перечень ПДн, обрабатываемых в информационной системе	
1.2	Определение перечня ИСПДн в организации	Приказ об утверждении перечня ИСПДн Перечень ИСПДн	
1.2	Разработка и утверждение правил доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ	Правила доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.2	Разработка журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.2	Назначение ответственного за организацию работ по криптографической защите информации	Приказ о назначении ответственного за организацию работ по криптографической защите информации Инструкция ответственного за организацию работ по криптографической защите информации	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.2	Разработка инструкции пользователя СКЗИ	Инструкция пользователя СКЗИ	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.3	Разработка инструкции по обращению со средствами криптографической защиты информации СКЗИ	Инструкция по обращению со средствами криптографической защиты информации СКЗИ	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.3	Разработка перечня пользователей, допущенных к работе с СКЗИ	Перечень пользователей, допущенных к работе с СКЗИ	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.3	Разработка технического (аппаратного) журнала СКЗИ	Технический (аппаратный) журнал СКЗИ	Мероприятие проводится в случае применения оператором информационной системы СКЗИ
1.3	Разработка журнала учета носителей персональных	Журнал учета носителей персональных данных	

№	Название мероприятия	Результат мероприятия	Примечание
2.	**Мероприятия по обеспечению безопасности значимых объектов КИИ**	**Организационно-распорядительная документация и локальные нормативные акты по обеспечению безопасности значимых объектов КИИ**	
2.1.	Формирование постоянно действующей комиссии по категорированию объектов КИИ	Приказ о создании постоянно действующей комиссии по категорированию объектов КИИ Положение о постоянно действующей комиссии по категорированию объектов КИИ	Требуется, если категорирование объектов КИИ осуществляется организацией (оператором ИС) самостоятельно
2.2.	Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию	Письмо во ФСТЭК России о направлении перечня объектов критической информационной инфраструктуры, подлежащих категорированию Перечень объектов критической информационной инфраструктуры, подлежащих категорированию	Требуется, если категорирование объектов КИИ осуществляется организацией (оператором ИС) самостоятельно
2.3.	Категорирование объекта КИИ	Акт категорирования объекта КИИ	Требуется, если категорирование объектов КИИ осуществляется организацией (оператором ИС) самостоятельно
2.4.	Подготовка сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	Письмо во ФСТЭК России о направлении сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	Требуется, если категорирование объектов КИИ осуществляется организацией (оператором ИС) самостоятельно
2.5.	Разработка политики обеспечения безопасности значимых объектов КИИ	Политика обеспечения безопасности значимых объектов КИИ	
2.6.	Разработка плана мероприятий обеспечения безопасности значимых объектов КИИ	План мероприятий обеспечения безопасности объектов КИИ	Должен составляться ежегодно
2.7.	Назначение лиц, ответственных за управление (администрирование) подсистемой безопасности значимого объекта КИИ	Приказ о назначении лиц, ответственных за управление (администрирование) подсистемой безопасности значимого объекта КИИ	
2.8.	Назначение лиц, которым разрешены действия по внесению изменений в конфигурацию значимого объекта и его подсистемы безопасности	Приказ о назначении лиц, которым разрешены действия по внесению изменений в конфигурацию значимого объекта и его подсистемы безопасности	
2.9.	Разработка и утверждение регламента информирования ФСБ России (НКЦКИ) о компьютерных инцидентах	Регламент информирования ФСБ России (НКЦКИ) о компьютерных инцидентах	
2.10	Разработка плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак	План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак	
2.11	Определение порядка контроля выполнения мероприятий по обеспечению безопасности значимого объекта	Порядок контроля выполнения мероприятий по обеспечению безопасности значимого объекта	
2.12	Определение компонентов значимого объекта КИИ, подлежащих изменению и контролю	Приказ об утверждении перечня компонентов значимого объекта КИИ, подлежащих изменению и контролю Перечень компонентов значимого объекта КИИ, подлежащих изменению и контролю	
3.	**Мероприятия по обеспечению безопасности государственных ИС**	**Организационно-распорядительная документация и локальные нормативные акты по защите информации в информационной системе**	

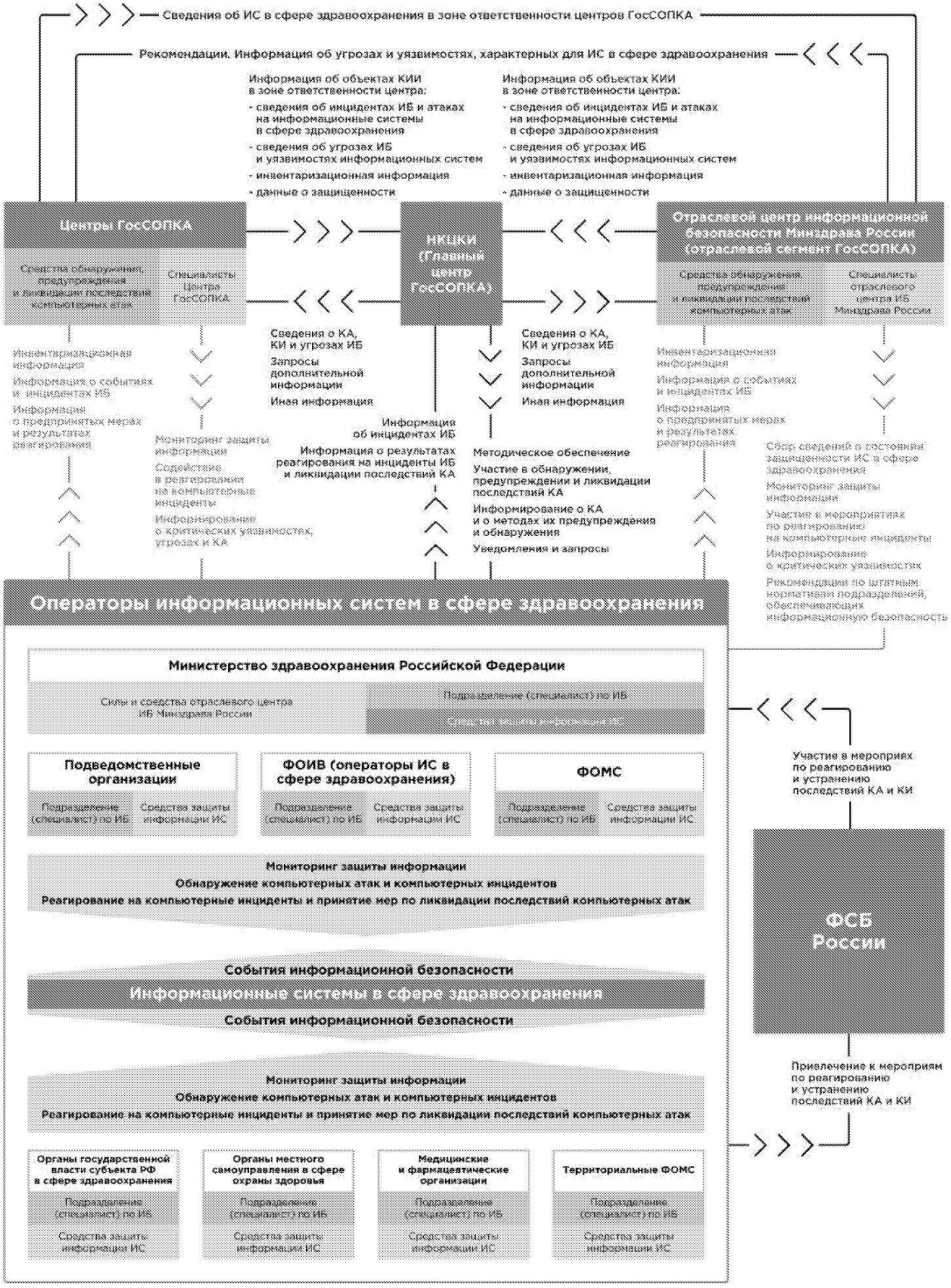
№	Название мероприятия	Результат мероприятия	Примечание
3.1.	Назначение лиц, ответственных за управление (администрирование) системой защиты информации информационной системы	Приказ о назначении лиц, ответственных за управление (администрирование) системой защиты информации информационной системы	Включает перечень лиц, ответственных за управление (администрирование) системой защиты информации информационной системы
3.2.	Разработка перечня ИС организации	Перечень ИС организации	
3.3.	Разработка перечня сведений конфиденциального характера, обрабатываемых в ИС	Перечень сведений конфиденциального характера, обрабатываемых в ИС	
3.4.	Формирование комиссии по классификации ИС	Приказ о составе комиссии по классификации ИС Положение о комиссии по классификации информационной системы	
3.5.	Классификация информационной системы	Акт классификации ИС	
3.6.	Разработка политики обеспечения информационной безопасности в организации	Политика обеспечения информационной безопасности в организации	
3.7.	Назначение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий	Приказ о назначении лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий	Включает перечень лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий
3.8.	Назначение лиц, ответственных за выявление инцидентов и реагирование на них	Приказ о назначении лиц, ответственных за выявление инцидентов и реагирование на них	Включает перечень лиц, ответственных за выявление инцидентов и реагирование на них
3.9.	Разработка порядка контроля выполнения мероприятий по обеспечению защиты информации в информационной системе	Порядок контроля выполнения мероприятий по обеспечению защиты информации в информационной системе	Включает перечень лиц, ответственных за планирование и контроль мероприятий по защите информации в информационной системе
3.10	Разработка плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак	План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак	
4.	**Мероприятия по обеспечению безопасности коммерческой тайны**	**Организационно-распорядительная документация и локальные нормативные акты по обеспечению защиты коммерческой тайны**	Разрабатываются при наличии в ИС организации информации, составляющей коммерческую тайну
4.1.	Введение режима коммерческой тайны в организации	Приказ о введении режима коммерческой тайны в организации	
4.2.	Назначение ответственного за обеспечение безопасности коммерческой тайны	Приказ о назначении ответственного за обеспечение безопасности коммерческой тайны	
4.3.	Разработка перечня сведений, составляющих коммерческую тайну	Перечень сведений, составляющих коммерческую тайну	
4.4.	Разработка положения о защите коммерческой тайны	Положение о защите коммерческой тайны	
5.	**Общие мероприятия по обеспечению безопасности защищаемых ИС**		
5.1.	Разработка правил и процедур идентификации и аутентификации в ИС	Раздел в инструкцию пользователя ИС в части описания правил и процедур идентификации и аутентификации в ИС Раздел в инструкцию администратора ИС в части описания правил и процедур идентификации и аутентификации в ИС	
5.2.	Разработка правил и процедур управления доступом к информационным ресурсам ИС	Раздел в инструкцию пользователя ИС в части описания правил и процедур управления доступом к информационным ресурсам ИС	

№	Название мероприятия	Результат мероприятия	Примечание
		Раздел в инструкцию администратора ИС в части описания правил и процедур управления доступом к информационным ресурсам ИС Матрица доступа пользователей к защищаемым информационным ресурсам информационной системы	
5.3.	Регламентация правил и процедур ограничения программной среды	Раздел в инструкцию пользователя ИС в части описания правил и процедур правил и процедур ограничения программной среды Раздел в инструкцию администратора ИС в части описания правил и процедур ограничения программной среды	Для ИС 1-го и 2-го унифицированных классов защиты
5.4.	Разработка правил и процедур защиты машинных носителей информации	Инструкция по порядку учета, хранения и уничтожения съемных носителей конфиденциальной информации, журналы учета машинных носителей информации	
5.5.	Регламентация правил и процедур аудита безопасности	Регламент аудита безопасности	
5.6.	Разработка правил и процедур антивирусной защиты	Инструкция по антивирусной защите в ИС	
5.7.	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)	Регламент предотвращения вторжений (компьютерных атак)	
5.8.	Разработка правил и процедур обеспечения целостности	Раздел в инструкцию пользователя ИС в части описания правил и процедур обеспечения целостности Раздел в инструкцию администратора ИС в части описания правил и процедур обеспечения целостности	
5.9.	Регламентация правил и процедур обеспечения доступности	Регламент резервного копирования и восстановления информации	
5.10	Регламентация правил и процедур защиты технических средств и систем	Приказ об утверждении границы контролируемой зоны информационной системы	
5.11	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	Регламент защиты виртуальной инфраструктуры	
5.12	Регламентация правил и процедур реагирования на компьютерные инциденты	Регламент управления инцидентами информационной безопасности	
5.13	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	Регламент управления конфигурацией информационной (автоматизированной) системы	
5.14	Регламентация правил и процедур управления обновлениями программного обеспечения	Регламент управления обновлениями программного обеспечения	
5.15	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	Регламент планирования мероприятий по обеспечению защиты информации	
5.16	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	Регламент обеспечения действий в нештатных ситуациях	
5.17	Регламентация правил и процедур информирования и обучения персонала	Регламент информирования и обучения персонала в области информационной безопасности	

Перечень приведенных в настоящем приложении организационных мероприятий по обеспечению информационной безопасности в организации для информационных систем в сфере здравоохранения может уточняться оператором информационной системы при уточнении выбранного эскизного решения по реализации мер защиты информации.

Приложение III

Архитектура системы реагирования на компьютерные атаки и инциденты информационной безопасности в сфере здравоохранения



Приложение IV
Эскизные решения построения системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

В настоящем приложении приводится описание технической реализации функций и порядок взаимодействия сторон в рамках системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения.

1. Требования к технической реализации функций системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

Технические и программно-аппаратные средства отраслевого центра информационной безопасности Минздрава России, информационных систем в сфере здравоохранения и систем защиты информации данных информационных систем, а также средства центров ГосСОПКА, в зону ответственности которых включаются информационные ресурсы организаций в сфере здравоохранения, должны полностью обеспечивать выполнение следующих функций системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения:

- предупреждение компьютерных атак;
- обнаружение компьютерных атак;
- ликвидация последствий компьютерных атак и инцидентов информационной безопасности.

1.1. Предупреждение компьютерных атак

1.1.1 Сбор и обработка сведений об инфраструктуре информационных систем в сфере здравоохранения

Целью сбора и обработки сведений об инфраструктуре информационной системы в сфере здравоохранения (инвентаризации) является получение и поддержание в актуальном состоянии сведений об информационных системах в сфере здравоохранения и информационно-телекоммуникационных сетях, обеспечивающих их функционирование, необходимых для выполнения функций по обнаружению, предупреждению и ликвидации последствий компьютерных атак. К таким сведениям относятся:

- сведения об архитектуре и объектах информационной системы в сфере здравоохранения (сетевые адреса и имена, наименования и версии используемого ПО);
- сведения о выполняющихся на объектах информационной системы в сфере здравоохранения сетевых службах;
- сведения об источниках событий информационной безопасности.

Инвентаризацию необходимо проводить для всех компонентов, входящих в каждый объект защиты. Сбор такого объема сведений с необходимой степенью детализации требует применения соответствующих инструментальных средств: специализированных средств инвентаризации (configuration management database, CMDB) или средств анализа защищенности, в которых реализована функция инвентаризации информационных ресурсов.

1.1.2 Сбор и обработка сведений об уязвимостях и недостатках в настройке программного обеспечения, используемого в информационной системе в сфере здравоохранения

Основным методом предупреждения компьютерных атак является устранение уязвимостей, которые могут быть использованы нарушителем для проведения атаки. Таким образом, целью анализа уязвимостей является выявление недостатков в обеспечении безопасности информационных ресурсов, которые могут быть использованы для осуществления компьютерных атак.

Для выявления уязвимостей могут использоваться следующие способы:

- сканирование компонентов объекта защиты средствами анализа защищенности;
- сравнение текущих параметров конфигурации компонентов объекта защиты с рекомендациями и руководствами по их безопасной настройке;

- лабораторное исследование программного и аппаратного обеспечения (фаззинг, статический анализ исходного кода, динамический анализ исходного кода);
- тестирование на проникновение[51].

В качестве инструментов выявления уязвимостей должны применяться средства анализа защищенности (сканеры уязвимостей).

1.2. Обнаружение компьютерных атак

1.2.1 Прием сообщений об инцидентах информационной безопасности от персонала и пользователей информационной системы в сфере здравоохранения

Источниками сообщений о возможных событиях и инцидентах информационной безопасности могут являться:

- пользователи объекта защиты;
- уполномоченные лица центра ГосСОПКА;
- надзорные органы;
- прочие лица (например, исследователи, обнаружившие уязвимость общедоступного компонента информационной системы, или смежные организации, если инцидент, связанный с объектом защиты, сказывается на функционировании взаимодействующих с ним информационных систем).

При приеме сообщений о возможном инциденте и уточнении полученной информации рекомендуется ориентироваться на следующий состав сведений об инциденте:

- контактные данные;
- сведения об информационной системе в сфере здравоохранения, в которой произошел инцидент;
- дата и время обнаружения инцидента;
- описание инцидента;
- информация о принятых мерах по реагированию на инцидент.

При получении сообщения проводится проверка содержащихся в нем сведений. При подтверждении инцидента производится его регистрация и реагирование на него.

Для приема сообщений об инцидентах от пользователей и персонала информационных систем в сфере здравоохранения используются как общедоступные средства связи (почтовая связь, телефонная связь, электронная почта), так и специализированные программно-технические средства, входящие в инфраструктуру отраслевого центра информационной безопасности Минздрава России или центра ГосСОПКА. К таким средствам относятся средства учета и обработки инцидентов информационной безопасности, а также средства взаимодействия.

1.2.2 Сбор событий информационной безопасности

Сбор событий, связанных с нарушением информационной безопасности, необходим для осуществления анализа связанной с ними информации и выявления на основании полученных данных инцидентов информационной безопасности. События информационной безопасности регистрируются средствами операционных систем, средствами защиты информации, телекоммуникационным оборудованием и средствами и системами его мониторинга и управления, прикладными сервисами, а также иными средствами, эксплуатируемыми в составе информационных систем в сфере здравоохранения и информационно-телекоммуникационных систем, обеспечивающих их функционирование (далее — источники событий информационной безопасности).

Сбор событий производится путем сбора данных из журналов регистрации событий на источниках событий. В силу большого количества источников событий, а также собираемых данных их сбор требует применения автоматизированных средств (систем security information and event management, SIEM-систем). Такие средства сбора событий информационной безопасности должны включаться в состав системы защиты ИС в сфере здравоохранения.

---

[51] В случае если в ходе теста на проникновение удалось реализовать одну или несколько угроз, побочным результатом теста являются сведения об уязвимостях, которые для этого использовались.

1.2.3 Анализ событий информационной безопасности

В ходе анализа событий информационной безопасности осуществляются:

- отбор и фильтрация событий информационной безопасности;
- выявление последовательностей разнородных событий информационной безопасности, имеющих логическую связь, которые могут быть значимы для выявления возможных нарушений безопасности информации (корреляция) и объединения однородных данных о событиях информационной безопасности (агрегация);
- выявление компьютерных инцидентов, регистрация методов (способов) их обнаружения.

Анализ событий производится путем их агрегирования и сопоставления (корреляции) на основе правил, разрабатываемых в ходе анализа угроз. В силу большого потока таких событий их анализ требует применения автоматизированных средств (систем security information and event management, SIEM-систем). Такие средства должны включаться в состав отраслевого центра информационной безопасности Минздрава, а также центров ГосСОПКА.

При анализе событий информационной безопасности должны учитываться данные о существующих и потенциальных угрозах информационной безопасности и о способах их обнаружения. Получение таких данных, их обработку, накопление (хранение) и учет в составе отраслевого центра информационной безопасности и центров ГосСОПКА обеспечивают средства анализа и учета угроз информационной безопасности (threat intelligence).

1.3. Ликвидация последствий компьютерных атак

1.3.1 Учет и обработка инцидентов, взаимодействие с НКЦКИ и с операторами ИС

Учет и обработка инцидентов осуществляются с использованием автоматизированных средств учета и обработки инцидентов, соответствующих требованиям НКЦКИ. После проверки сведений о возможном инциденте (сообщение от персонала или пользователей информационной системы, предупреждения о срабатывании правил корреляции средств анализа событий информационной безопасности) производится их первичная проверка.

В случае если сведения о возможном инциденте подтверждаются хотя бы одним из лиц, ответственных за функционирование хотя бы одного из информационных ресурсов, инцидент признается подтвержденным и принимаются меры реагирования.

Реагирование на инцидент включает в себя:

- фиксацию состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент;
- фиксацию и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент;
- определение причин инцидента и возможных его последствий для информационного ресурса;
- локализацию инцидента;
- сбор сведений для последующего установления причин инцидента;
- планирование мер по ликвидации последствий инцидента;
- ликвидацию последствий инцидента;
- контроль ликвидации последствий.

Определение причин инцидента проводится персоналом операторов информационных систем, специалистами центра ГосСОПКА. При необходимости для определения причин инцидента информационной безопасности могут привлекаться специалисты отраслевого центра информационной безопасности Минздрава России.

Сведения о подтвержденном инциденте направляются в НКЦКИ и ведомственный центр ГосСОПКА.

Для автоматизации процедур учета и обработки инцидентов информационной безопасности используются специализированные программно-технические средства, входящие в инфраструктуру отраслевого центра информационной безопасности и центров ГосСОПКА. К таким средствам

относятся средства учета и обработки инцидентов, средства взаимодействия с ГосСОПКА и средства взаимодействия с операторами ИС в сфере здравоохранения.

Схема, представленная на рис. 2, в общем виде дает представление о составе и месте средств в системе реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения, а также о направлениях и сути взаимодействия между отраслевым центром информационной безопасности Минздрава России и участниками системы.

Сегменты архитектуры системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения для центра ГосСОПКА, в зону ответственности которого входят информационные системы в сфере здравоохранения, и для оператора информационной системы в сфере здравоохранения представлены на рис. 3 и 4 соответственно.

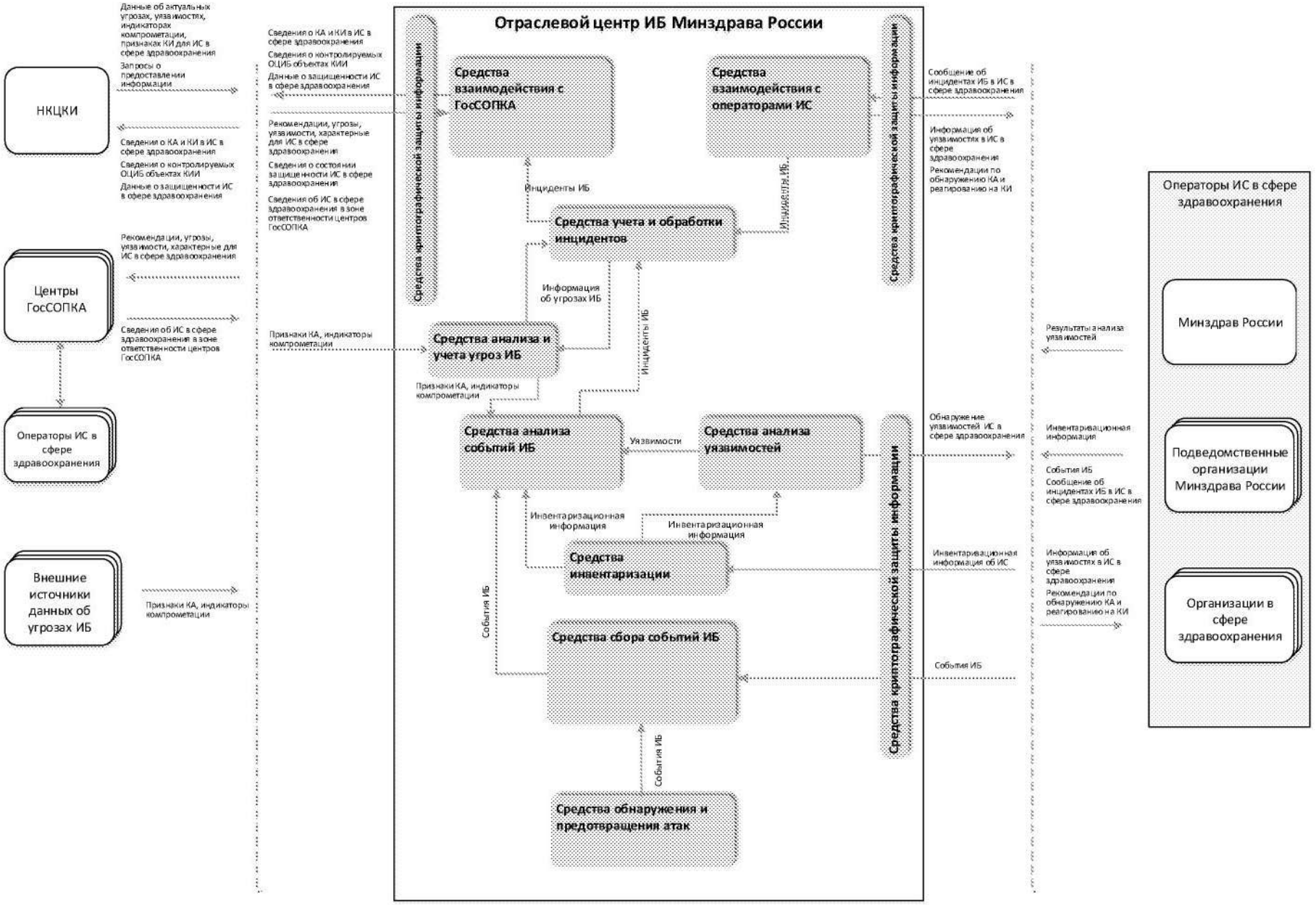


Рисунок 2. Архитектура системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

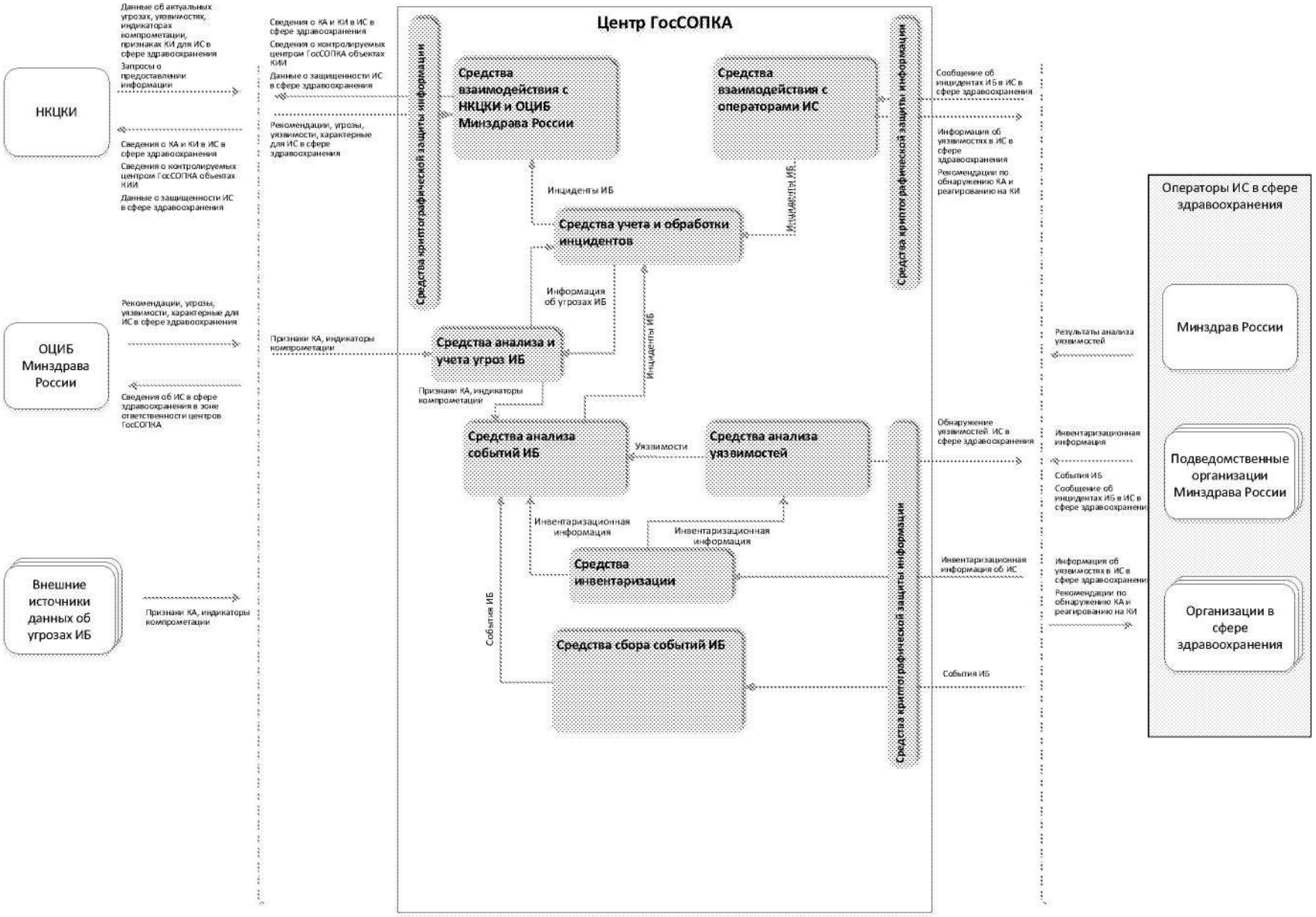


Рисунок 3. Архитектура сегмента центра ГосСОПКА системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

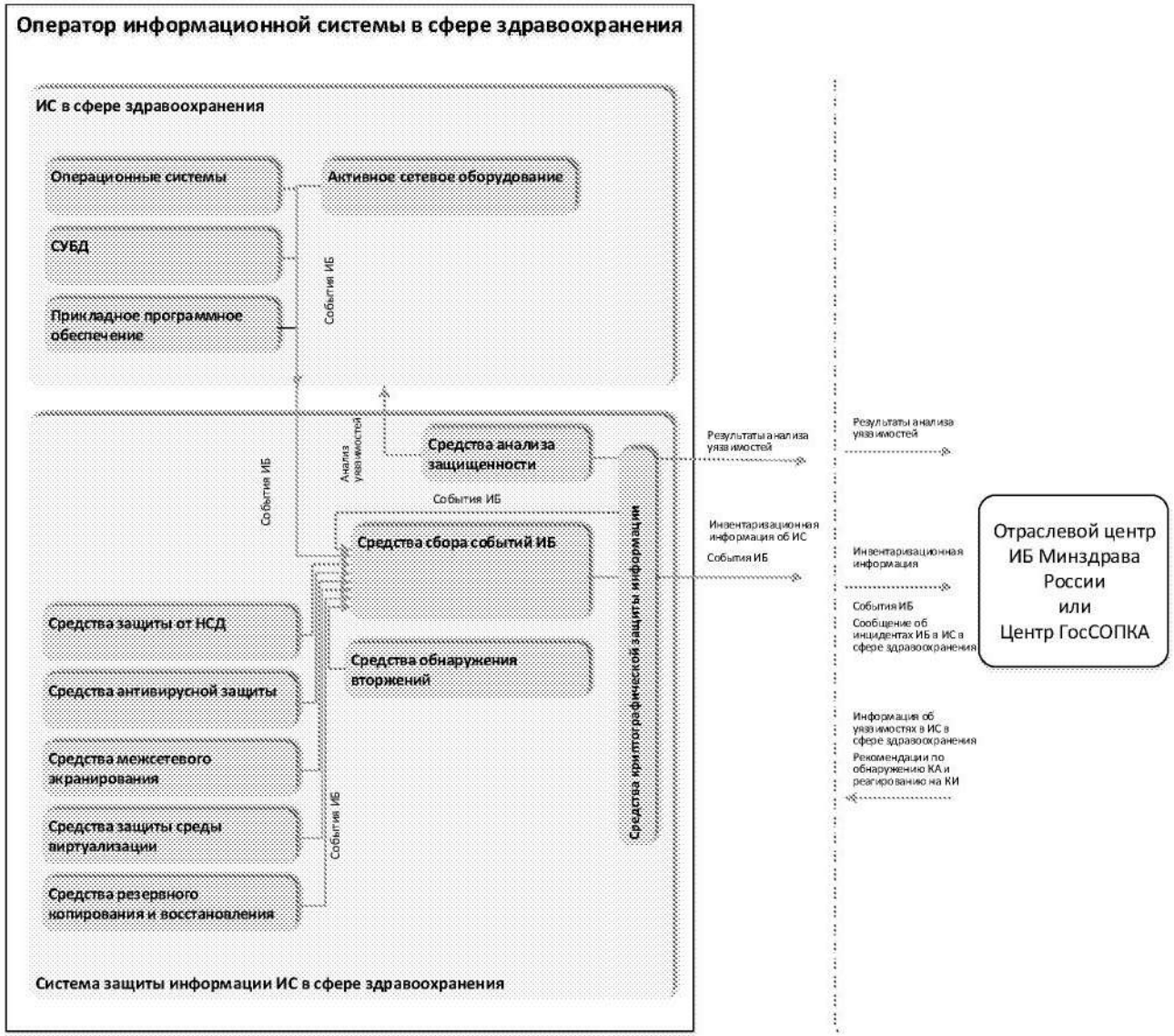


Рисунок 4. Архитектура сегмента оператора информационной системы в сфере здравоохранения системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

2. Взаимодействие сторон в рамках системы реагирования на компьютерные атаки и инциденты информационной безопасности в информационных системах в сфере здравоохранения

2.1. Взаимодействие отраслевого центра информационной безопасности Минздрава России и центров ГосСОПКА с организациями в сфере здравоохранения

Взаимодействие отраслевого центра информационной безопасности Минздрава России с организациями, являющимися операторами информационных систем в сфере здравоохранения, входящих в зону ответственности отраслевого центра информационной безопасности, в общем случае включает следующие функции:

- для отраслевого центра информационной безопасности:
  - прием от организации сведений о составе и характеристиках информационных ресурсов, включенных в зону ответственности отраслевого центра информационной безопасности;
  - прием информации от организации об инцидентах информационной безопасности;
  - доведение до организации информации об угрозах безопасности информации и необходимых мерах по противодействию им;
  - доведение до организации информации о проведении компьютерных атак и о методах их предупреждения, обнаружения и противодействия;
  - оказание содействия в реагировании на компьютерные инциденты, обеспечение методической и экспертной поддержки по вопросам реагирования на компьютерные инциденты;
  - обнаружение уязвимостей информационных систем в сфере здравоохранения организации;
- для организации:
  - предоставление в отраслевой центр информационной безопасности сведений о составе и характеристиках информационных систем в сфере здравоохранения, а также актуализация таких сведений;
  - предоставление в отраслевой центр информационной безопасности сведений о выявляемых компьютерных атаках и компьютерных инцидентах в информационных системах в сфере здравоохранения, а также информации о принятых мерах и результатах реагирования на такие инциденты;
  - прием от отраслевого центра информационной безопасности информации об актуальных угрозах безопасности и признаках компьютерных инцидентов в информационных ресурсах в сфере здравоохранения и принятие мер по противодействию данным угрозам.

Функции и порядок взаимодействия отраслевого центра информационной безопасности и организаций, являющихся операторами информационных систем в сфере здравоохранения, определяются уровнем информатизации (информационной инфраструктуры) и наличием у таких организаций информационных систем, принадлежащих им на праве собственности или ином законном основании. В том случае, если в организации используется исключительно клиентский доступ к централизованным информационным системам в сфере здравоохранения, основные функции взаимодействия с отраслевым центром информационной безопасности включают:

- для отраслевого центра информационной безопасности:
  - сбор сведений об информационных ресурсах организации;
  - прием информации от организации об инцидентах информационной безопасности;
  - участие в осуществлении мероприятий по реагированию на компьютерные инциденты и устранению последствий компьютерных атак;
- для организации:
  - предоставление в отраслевой центр информационной безопасности сведений о выявляемых компьютерных атаках и инцидентах информационной безопасности в инфраструктуре организации.

Взаимодействие между отраслевым центром информационной безопасности и организацией осуществляется:

- по инициативе одной из сторон;
- в виде ответа на запрос;
- в соответствии с установленной периодичностью, согласованной сторонами;
- в автоматизированном режиме с использованием технической инфраструктуры отраслевого центра информационной безопасности.

Информационное взаимодействие отраслевого центра информационной безопасности и организаций, являющихся операторами информационных систем в сфере здравоохранения, может осуществляться в следующих формах:

- по телекоммуникационным каналам сети Интернет:
  - с использованием автоматизированных средств технической инфраструктуры отраслевого центра информационной безопасности;
  - направлением электронного письма;
- в письменном в виде с приложением электронных носителей информации (при необходимости);
- телефонным звонком на номера операторов отраслевого центра информационной безопасности и организации соответственно.

В целях выполнения требований Приказа ФСБ России от 19.06.2019 № 282 «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» в случае включения организаций, являющихся операторами информационных систем в сфере здравоохранения, в зону ответственности отраслевого центра информационной безопасности информация об инцидентах информационной безопасности на объектах организации передается в отраслевой центр информационной безопасности независимо от формы и способов передачи в следующие сроки:

- для значимых объектов КИИ организации — не позднее 3 ч. с момента обнаружения инцидента информационной безопасности;
- для остальных объектов КИИ организации — не позднее 24 ч. с момента обнаружения инцидента информационной безопасности.

Информация о результатах мероприятий по реагированию на инциденты информационной безопасности и принятию мер по ликвидации последствий компьютерных атак на значимые объекты КИИ организаций, являющихся операторами информационных систем в сфере здравоохранения, должна передаваться в отраслевой центр информационной безопасности независимо от формы и способов передачи не позднее 48 часов после завершения таких мероприятий.

Порядок и способы взаимодействия между отраслевым центром информационной безопасности и организациями, являющимися операторами информационных систем в сфере здравоохранения, а также формы и типы передаваемой информации определяются до начала взаимодействия и документально оформляются в установленном порядке.

Функции и порядок взаимодействия центра ГосСОПКА, созданного субъектом Российской Федерации или специализированной организацией, с операторами информационных систем в сфере здравоохранения, входящих в зону ответственности центра ГосСОПКА, определяются в соответствии с подписанным соглашением о взаимодействии и осуществляются в соответствии с требованиями ФСБ России и НКЦКИ.

2.2. Взаимодействие отраслевого центра информационной безопасности Минздрава России с НКЦКИ

Функции взаимодействия отраслевого центра информационной безопасности Минздрава России с НКЦКИ осуществляются в соответствии с заключенным между Минздравом России и НКЦКИ соглашением.

Взаимодействие отраслевого центра информационной безопасности с НКЦКИ осуществляется с помощью специальных средств взаимодействия, предусмотренных для реализации технических решений при создании отраслевого центра информационной безопасности. При взаимодействии по незащищенным каналам связи дополнительно используются средства криптографической защиты информации, сертифицированные в системе сертификации ФСБ России.

Порядок взаимодействия отраслевого центра информационной безопасности с НКЦКИ включает выполнение следующих действий:

- предоставление сведений НКЦКИ;
- получение и обработка информационных сообщений НКЦКИ.

Отраслевой центр информационной безопасности поддерживает следующие регламенты взаимодействия:

- по инициативе одной из сторон;
- в виде ответа на запрос;
- в соответствии с установленной периодичностью, согласованной сторонами;
- в автоматизированном режиме с использованием технической инфраструктуры НКЦКИ.

Отраслевой центр информационной безопасности при взаимодействии с НКЦКИ принимает следующую информацию:

- сведения об актуальных угрозах информационных систем в сфере здравоохранения, входящих в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- сведения об актуальных уязвимостях информационных систем в сфере здравоохранения, входящих в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- сведения о признаках компьютерных инцидентов и индикаторах компрометации, связанных с компьютерными атаками на информационные системы в сфере здравоохранения, входящие в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- запросы на предоставление дополнительной информации по компьютерным инцидентам и другим событиям информационной безопасности в информационных системах в сфере здравоохранения, входящих в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- иную информацию, предусмотренную нормативно-правовыми актами Российской Федерации в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Отраслевой центр информационной безопасности при взаимодействии с НКЦКИ передает следующую информацию:

- инвентаризационные сведения об информационных системах в сфере здравоохранения, входящих в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- сведения об инцидентах и атаках на информационные системы в сфере здравоохранения, входящие в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- сведения об угрозах безопасности информации и уязвимостях информационных систем в сфере здравоохранения, входящих в зону ответственности отраслевого центра информационной безопасности Минздрава России, и ИТКС, обеспечивающих их функционирование;
- иную информацию, предусмотренную нормативно-правовыми актами Российской Федерации в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

2.3. Взаимодействие отраслевого центра информационной безопасности Министерства здравоохранения Российской Федерации с центрами ГосСОПКА

Функции взаимодействия отраслевого центра информационной безопасности Минздрава России с центрами ГосСОПКА, созданными субъектами Российской Федерации или

специализированными организациями, определяются нормативными правовыми актами ФСБ России, НКЦКИ, Минздрава России и субъектов Российской Федерации и осуществляются в соответствии с заключенным между оператором информационных систем в сфере здравоохранения и центром ГосСОПКА соглашением.

Взаимодействие отраслевого центра информационной безопасности Минздрава России с центрами ГосСОПКА осуществляется с помощью специальных программно-технических средств взаимодействия, предусмотренных для реализации технических решений при создании отраслевого центра информационной безопасности. При взаимодействии по незащищенным каналам связи дополнительно используются средства криптографической защиты информации, сертифицированные в системе сертификации ФСБ России.