ООО «НТЦ ПРОТЕЙ»

УТВЕРЖДЕНО

ПАМР.460018.006.ТП-ЛУ

# РАЗРАБОТКА ТЕХНИЧЕСКОГО ПРОЕКТА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ВЫЗОВА ЭКСТРЕННЫХ ОПЕРАТИВНЫХ СЛУЖБ ПО ЕДИНОМУ НОМЕРУ «112» НА ТЕРРИТОРИИ СВЕРДЛОВСКОЙ ОБЛАСТИ

Пояснительная записка к техническому проекту.

Концепция информационной безопасности. Модель угроз

ПАМР.460018.006.ТП.П11

На 98 листах

| Подп.и дата | |
|---|---|
| Инв.№ дубл. | |
| Взаминв № | |
| Подп.и дата | |
| Инв.№ подл. | |

**Содержание**

**Список сокращений**

| Сокращение | Определение |
|---|---|
| АРМ | автоматизированное рабочее место |
| БД | база данных |
| ДДС | дежурно-диспетчерская служба |
| ЕДДС МО | единая дежурно-диспетчерская служба |
| ИС | информационная система |
| МО | муниципальное образование |
| НДВ | недекларируемые возможности |
| НСД | несанкционированный доступ |
| ПДн | персональные данные |
| ПО | программное обеспечение |
| ПЭВМ | персональная электронно-вычислительная машина |
| РЦОВ | резервный центр обработки вызовов |
| СКЗИ | средства криптографической защиты информации |
| СФ | среда функционирования |
| УСПО-112 | унифицированное специальное программное обеспечение системы-112 |
| ЦОВ | центр обработки вызовов |
| ЦУКС | центр управления в кризисных ситуациях |

# 1 Формирование требований к защите информации, содержащейся в информационной системе

## 1.1 Обоснование необходимости защиты информации, содержащейся в информационной системе

### 1.1.1 Анализ целей создания информационной системы и задач, решаемых этой информационной системой

Система-112 предназначена для информационного обеспечения единых дежурно-диспетчерских служб муниципальных образований.

Вызов экстренных оперативных служб также может быть обеспечен каждому пользователю услугами связи посредством набора номера, предназначенного для вызова соответствующей экстренной оперативной службы.

Основными целями создания системы-112 в Российской Федерации являются:

а) организация вызова экстренных оперативных служб по принципу "одного окна";

б) организация комплекса мер, обеспечивающих ускорение реагирования и улучшение взаимодействия экстренных оперативных служб при вызовах (сообщениях о происшествиях);

в) реализация требований гармонизации способа вызова экстренных оперативных служб в Российской Федерации с законодательством Европейского союза.

4. Система-112 предназначена для решения следующих основных задач:

а) прием по номеру "112" вызовов (сообщений о происшествиях);

б) получение от оператора связи сведений о местонахождении лица, обратившегося по номеру "112", и (или) абонентского устройства, с которого был осуществлен вызов (сообщение о происшествии), а также иных данных, необходимых для обеспечения реагирования по вызову (сообщению о происшествии);

в) анализ поступающей информации о происшествиях;

г) направление информации о происшествиях, в том числе вызовов (сообщений о происшествиях), в дежурно-диспетчерские службы экстренных оперативных служб в соответствии с их компетенцией для организации экстренного реагирования;

д) обеспечение дистанционной психологической поддержки лицу, обратившемуся по номеру "112";

е) автоматическое восстановление соединения с пользовательским (оконечным) оборудованием лица, обратившегося по номеру "112", в случае внезапного прерывания соединения;

ж) регистрация всех входящих и исходящих вызовов (сообщений о происшествиях) по номеру "112";

з) ведение базы данных об основных характеристиках происшествий, о начале, завершении и об основных результатах экстренного реагирования на полученные вызовы (сообщения о происшествиях);

и) возможность приема вызовов (сообщений о происшествиях) на иностранных языках. Субъекты Российской Федерации вправе утверждать перечень муниципальных образований, где с учетом местных условий необходимо обеспечить прием вызовов (сообщений о происшествиях) на государственном языке республики, входящей в состав Российской Федерации, и (или) иных языках народов, проживающих на территории субъекта Российской Федерации.

### 1.1.2 Анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система

При разработке информационной системы должны учитываться требования следующих основных нормативных и регламентирующих документов:

Постановление Правительства РФ от 30.12.2003 N 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (с изменениями на 26 января 2017 года)»

Постановление Правительства РФ от 31.12.2004 N 894 «Об утверждении перечня экстренных оперативных служб, вызов которых круглосуточно и бесплатно обязан обеспечить оператор связи пользователю услугами связи, и о назначении единого номера вызова экстренных оперативных служб (с изменениями на 06.10.2011)»

Распоряжение Правительства РФ от 25.08.2008 N 1240-р «Об одобрении Концепции создания системы обеспечения вызова экстренных оперативных служб через единый номер "112" на базе единых дежурно-диспетчерских служб муниципальных образований»

Указ Президента РФ от 28.12.2010 N 1632 «О совершенствовании системы обеспечения вызова экстренных оперативных служб на территории Российской Федерации»

Постановление Правительства РФ от 21.11.2011 N 958 «О системе обеспечения вызова экстренных оперативных служб по единому номеру "112" (с изменениями на 6 марта 2015 года)»

Постановление Правительства РФ от 06.07.2015 N 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 (с изменениями на 11 мая 2017 года)

Приказ Мининформсвязи России от 17.11.2006 N 142 «Об утверждении и введении в действие Российской системы и плана нумерации» (с изменениями на 5 апреля 2016 года)

Приказ Мининформсвязи России от 27.09.2007 N 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования»

Приказ Минкомсвязи России от 25.08.2009 N 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»

ГОСТ Р 22.7.01-2016 Безопасность в чрезвычайных ситуациях. Единая дежурно-диспетчерская служба. Основные положения (Применяется с 01.06.2017. Заменяет ГОСТ Р 22.7.01-99).

Основные документы по безопасности Государства и населения:

Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (с изменениями на 8 марта 2015 года)

Федеральный закон от 21.12.1994 N 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (с изменениями на 23 июня 2016 года)

Федеральный закон от 07.07.2003 N 126-ФЗ «О связи» (с изменениями на 6 июля 2016 года).

Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 19 декабря 2016 года) (редакция, действующая с 1 января 2017 года)

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (с изменениями на 22 февраля 2017 года)

Федеральный закон от 22.07.2008 N 123-ФЗ «Технический регламент о требованиях пожарной безопасности» (с изменениями на 3 июля 2016 года)

Федеральный закон от 30.12.2009 N 384-ФЗ «Технический регламент о безопасности зданий и сооружений» (с изменениями на 2 июля 2013 года)

Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями на 30 ноября 2016 года)

Указ Президента РФ от 06.03.1997 N 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 13 июля 2015 года)

Указ Президента РФ от 28.08.2003 N 991 «О совершенствовании единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» (с изменениями на 29 июня 2013 года)

Указ Президента РФ от 17.05.2007 N 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации»

Указ Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (с изменениями на 22 мая 2015 года)

Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Постановление Правительства РФ от 30.12.2003 N 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций» (с изменениями на 26 января 2017 года)

Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСБ России от 10 июля 2014 г. N 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».

ГОСТ Р 53110-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения».

ГОСТ Р 53111-2009 «Устойчивость функционирования сети связи общего пользования. Требования и методы проверки».

ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

Методический документ «Меры защиты информации в государственных информационных системах», утверждённые ФСТЭК России 11.02.2014;

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная Заместителем директора ФСТЭК России 15.02.2008;

«Методика определения актуальных угроз персональных данных при их обработке в информационных системах персональных данных», утвержденная Заместителем директора ФСЭК России от 14.02.2008;

Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992.

Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992.

Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», утверждено решением председателя Гостехкомиссии России от 30.03.1992.

Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992.

Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25.07.1997.

Руководящий документ «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114.

### 1.1.3 Цели и задачи защиты информации в информационной системе

Подсистема обеспечения информационной безопасности (ПОИБ) системы-112 предназначена для защиты для защиты информации и средств ее обработки в системе-112.

Целью реализации ПОИБ является снижение вероятного ущерба от реализации угроз ИБ и выполнение требований законодательства Российской Федерации в части защиты информации, в том числе персональных данных.

### 1.1.4 Основные этапы создания системы защиты информации

Этапы создания системы защиты информации должны соответсовать требованиям ГОСТ 34.601-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. В ходе работ по созданию ПОИБ системы-112 должно быть выполнено следующее:

формирование требований к защите информации, содержащейся в информационной системе;

в составе технического проекта по созданию системы-112 разработка разделов по созданию подсистемы обеспечения информационной безопаснотси системы-112;

внедрение ПОИБ (монтажные и пусконаладочные работы) при создании системы-112;

аттестация ПОИБ системы-112 по требованиям защиты информации и ввод в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

### 1.1.5 Перечень объектов защиты информационной системы

Объектами защиты информационной системы-112 являются:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- помещения, в которых размещены компоненты системы-112.

Обработка персональных данных осуществляется:

- в Центре обработки вызовов или (и) Резервном Центре обработки вызовов системы-112 субъекта РФ (ЦОВ-АЦ/РЦОВ);
- в помещениях центров обработки вызовов единой дежурно-диспетчерской службы муниципальных образований субъекта РФ (ЦОВ-ЕДДС);
- в помещениях, в которых установлены автоматизированные рабочие места дежурно-диспетчерских служб (ДДС);
- в помещениях, в которых установлены автоматизированные рабочие места центра управления в кризисных ситуациях (ЦУКС).

## 1.2 Классификация информационной системы по требованиям защиты информации

Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Система-112 имеет региональный масштаб, поскольку она функционирует на территории всех муниципальных образований Свердловской области.

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или

иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Величину (степень) ущерба, в соответствии следует оценивать качественно по вербальной шкале.

Нарушения безопасности информации, обрабатываемой в ГИС, могут приводить к ущербу в социальной, политической, международной, экономической, финансовой или иных областях деятельности, причем в каждой из этих областей деятельности возможно причинение одного из следующих видов ущерба: финансового, экономического, материального, экологического, социального, морального и их сочетаний. Как правило, экономический и материальный ущербы могут быть пересчитаны в финансовый и поэтому далее как самостоятельные виды ущерба не рассматриваются.

Остальные виды ущерба могут быть охарактеризованы следующим образом.

Финансовый ущерб, в основном, обусловлен:

возможностью потерь финансовых средств, в том числе неполучением ожидаемой прибыли;

необходимостью дополнительных затрат на выплату штрафов (неустоек) и компенсаций гражданам (клиентам, сотрудникам);

необходимостью дополнительного финансирования запланированных работ и работ, связанных с ликвидацией последствий нарушений безопасности информации в ГИС (в том числе закупка и/или разработка программного и/или аппаратного обеспечения, модернизация системы защиты информации).

Экологический ущерб обусловлен возможностью возникновения ситуаций, при которых создается опасность жизни и здоровью граждан вследствие загрязнения окружающей среды радиоактивными, токсическими или болезнетворными биологическими материалами.

Социальный ущерб может быть обусловлен возможностью возникновения (нарастания) социальной напряженности в обществе, которая проявляется в возрастании количества жалоб в органы власти и местного самоуправления, в появлении публикаций с критикой организаций и органов власти, в активизации выступлений общественных организаций и политических партий, в проведении демонстраций, организации и осуществлении акций гражданского неповиновения.

Моральный ущерб, в основном, обусловлен возможностью:

снижения государственного престижа на международном уровне;

снижения престижа федеральных органов власти, органов власти субъектов Российской Федерации и органов местного самоуправления;

дискредитации руководителей государственных структур;

нарушения деловой репутации государственных организаций;

нанесения морального вреда (оскорбление, публикация ложных сведений об организации, органе власти, сведений личного характера, персональных данных) гражданам, сотрудникам государственных организаций и органов власти.

Оценка финансового ущерба произведена с учетом характера информации ограниченного доступа, содержания несанкционированных действий с защищаемой информацией и уровня последствий от нарушения защищаемой информации в ГИС (федерального, регионального, объектового). При этом информация ограниченного доступа подразделяется на финансово-экономическую, административно-управленческую и технологическую. Для каждой такой информации выявляются возможные несанкционированные действия и далее для каждого действия оценивается возможный ущерб. Финансовый ущерб для системы-112 может заключаться в необходимости дополнительных затрат на выплату штрафов (неустоек) и компенсаций гражданам в случае разглашения персональных данных, а также возможности дополнительного финансирования работ, связанных с ликвидацией последствий нарушений безопасности информации в системе-112 и модернизации ПОИБ.

Оценка финансового ущерба для системы-112 приведена в таблице 1.

Таблица 1 – Оценка финансового ущерба для системы-112

| Содержание несанкционированных действий с защищаемой информацией | Вид защищаемой информации | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Информация ограниченного доступа | | | | | | | | | Иная защищаемая информация | | |
| | Финансово-экономического характера | | | Административно-управленческого характера | | | Технологического характера | | | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне |
| | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне | | | |
| Нарушение конфиденциальности информации | Низкий | Средний | Минимальный | Низкий | Средний | Минимальный | Минимальный | Средний | Минимальный | Минимальный | Средний | Минимальный |
| Нарушение целостности информации | Средний | Средний | Минимальный | Срдений | Срдений | Минимальный | Срдений | Срдений | Минимальный | Минимальный | Срдений | Минимальный |
| Нарушение доступности информации | Срдений | Средний | Минимальный | Срдений | Срдений | Минимальный | Срдений | Срдений | Минимальный | Минимальный | Срдений | Минимальный |

Экологический ущерб оценивается в том случае, когда вследствие нарушений доступности или целостности системного, специального и прикладного программного обеспечения или используемых данных может произойти нарушение функционирования ГИС и с развитием чрезвычайной ситуации, связанной с гибелью людей или нарушением условий их жизнедеятельности. Оценка экологического ущерба приведена в таблице 2.

Таблица 2 Оценка экологического ущерба для системы-112

| Последствия от реализации угроз безопасности информации | Масштаб чрезвычайной ситуации | Возможный экологический ущерб |
|---|---|---|
| Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей, не выходит за пределы территории объекта и количество людей, которые могут погибнуть или получит ущерб здоррвью не может превысить 10 человек | Чрезвычайная ситуация локального характера | Средний |
| Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей, не выходит за пределы территории одного поселения или внутригородской территориигорода федерального значения и количество людей, которые могут погнибнуть или получить ущшерб здоровью не может превысить 50 человек | Чрезвычайная ситуация муниципального характера | Средний |
| Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей, не выходит за пределы территории одного субъекта Российской Федерации, при этом количество пострадавших может составить свыше 50 человек, но не более 500 человек | Чрезвычайная ситуация регионального характера | Средний |

| | | |
|---|---|---|
| Территория, на которой может сложиться чрезвычайная ситуация и будут нарушены условия жизнедеятельности людей выходит за пределы одного субъекта Российской Федерации и будут нарушены условия жизнедеятельности более чем 500 человек | Чрезвычайная ситуация федерального характера | Низкий |

Оценка величины (степени) социального ущерба основывается на определении возможного уровня социальной напряженности, вызванной сбоями или недостатками в работе органа власти или организации (предприятия), влияющими на жизнь людей, обеспечение их прав и свобод, или связанной с незаконным распространением персональных данных людей и иной подлежащей защите информации без согласия физических и юридических лиц. Непосредственными причинами сбоев и недостатков являются:

нарушение функционирования ГИС или уничтожение информации и связанное с этим существенное замедление работы органа власти, организации (предприятия);

несанкционированное изменение данных, хранящихся в ГИС, и выдача гражданам или организациям неверных данных;

кража и несанкционированное распространение информации, обладателями которой являются физические или юридические лица.

Величина (степень) социального ущерба определяется в зависимости от последствий, к которым может привести реализация угроз безопасности информации и от уровня (предприятие, муниципальные органы, органы власти субъектов Российской Федерации, федеральные органы власти), на котором могут проявиться эти последствия в результате реализации угроз безопасности информации в ГИС.

Оценка возможного социального ущерба от реализации угроз безопасности в системе-112 приведена в таблице 3.

Таблица 3 - Оценка возможного социального ущерба от реализации угроз безопасности в системе-112

| | | | | |
|---|---|---|---|---|
| Возможные выступления населения в виде пикетов и демонстраций, проведений акций гражданского неповиновения | Последствия проявляются на федеральном уровне | Минимальный | Минимальный | Минимальный |
| | Последствия проявляются на региональном уровне | Минимальный | Минимальный | Минимальный |
| | Последствия проявляются на объектовом уровне | Минимальный | Минимальный | Минимальный |
| Возможное поделючение к разрешению | Последствия проявляются на федеральном уровне | Минимальный | Минимальный | Минимальный |

| | | | | |
|---|---|---|---|---|
| Содержание несанкционированных действий с защищаемой информацией | Возможное недовольство населения, выражаемое в жалобах в органы власти и публикациях в прессе | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне |
| Неправомерные доступ, копирование, предоставление или распространение информации (нарушение конфиденциальности информации) | Минимальный | Средний | Минимальный | Минимальный |
| Неправомерное уничтожение или модифицирование информации (нарушение целостности информации) | Минимальный | Средний | Минимальный | Минимальный |
| Неправомерное блокирование информации (нарушение доступности информации) | Минимальный | Средний | Минимальный | Минимальный |

Оценка величины (степени) морального ущерба основывается на определении того, чьи интересы могут быть затронуты в результате утечки информации (в том числе персональных данных), нарушения ее целостности и доступности или нарушения функционирования ГИС в целом с существенным затруднением выполнения органом власти или организации своих функций. Величина (степень) морального ущерба зависит от вида и масштаба последствий реализации угроз безопасности информации. Оценка возможного морального ущерба от реализации угроз безопасности информации в системе-112 приведена в стблице 4.

Таблица 4 – Оценка возможного морального ущерба от реализации угроз безопасности информации в системе-112

| | | |
|---|---|---|
| Содрежание несанкционированных действий с защищаемой инофрмацией | Снижение престижа организации, органа власти или государства в целом | Дискредитация или нарушение деловой репутации должностных лиц. Причинение морального вреда гражданам, сотрудникам государственных организаций и органов власти (оскорбление, публикация ложных сведений, сведений личного хараткера) |

| | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне | Последствия проявляются на объектовом уровне | Последствия проявляются на региональном уровне | Последствия проявляются на федеральном уровне |
|---|---|---|---|---|---|---|
| Неправомерные доступ, копирование, предоставление или распространение информации (нарушение конфиденциальности информации) | Минимальный | Средний | Минимальный | Минимальный | Минимальный | Минимальный |
| Неправомерное унитожение или модифицирование информации (нарушение целостности информации) | Минимальный | Средний | Минимальный | Минимальный | Минимальный | Минимальный |
| Неправомерное блокирование информации (нарушение доступности информации) | Минимальный | Средний | Минимальный | Минимальный | Минимальный | Минимальный |

Поскольку для системы -112 степень возможного ущерба принимается средней, нет ни одного свойства, для которого определена высокая степень ущерба уровень значимости информации принимается УЗ 2.

В соответствии с Приложением N 2 к Приказу ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями на 15 февраля 2017 года) класс защищенности системы-112 определен как К2.

### 1.3 Определение уровня защищенности персональных данных

В соответствии с Законом №152-ФЗ персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПДн). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПДн. Категории и перечень персональных данных, обрабатываемых в системе-112, представлены в таблице 5:

Таблица 5 – Категории и перечень ПДн, обрабатываемых в системе-112

| Категория ПДн | Перечень ПДн | Обоснование |
|---|---|---|
| Иные | − фамилия, имя отчество (заявителя, владельца пользовательского оборудования, разыскиваемого, больного и т.д.);<br>− номер пользовательского оборудования, с которого поступил вызов (сообщение);<br>− информация о месте нахождения пользовательского оборудования;<br>− адрес проживания заявителя;<br>− язык общения заявителя;<br>− информация о транспортном средстве, участвовавшем в ДТП;<br>− пол;<br>− степень родства заявителя;<br>− возраст;<br>− дата рождения. | В соответствии со статьей 8 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных (с изменениями на 29 июля 2017 года)» в общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных |
| Специальные | - данные о состоянии здоровья; | В соответствии со статьей 10 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных (с изменениями на 29 июля 2017 года)» к специальным категориям персональных данных относятся персональные данные, касающихся расовой, национальной |

| Категория ПДн | Перечень ПДн | Обоснование |
|---|---|---|
| | | принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. В соответствии с п.п. 4 данной статьи к данным о состоянии здоровья в т.ч. относятся сведения, сообщаемые для в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг. При этом обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну. Данные заносятся диспетчером ДДС-03 в дополнительные поля карточки диспетчера ДДС-03 системы-112. |

| Категория ПДн | Перечень ПДн | Обоснование |
|---|---|---|
| Биометрические | − пол подозреваемого в совершении правонарушения;<br>− возраст подозреваемого в совершении правонарушения;<br>− рост подозреваемого в совершении правонарушения;<br>− телосложение подозреваемого в совершении правонарушения;<br>− особые приметы подозреваемого в совершении правонарушения;<br>− пол разыскиваемого;<br>− фамилия, имя, отчество разыскиваемого;<br>− дата рождения разыскиваемого;<br>− возраст разыскиваемого;<br>− рост разыскиваемого;<br>− телосложение разыскиваемого;<br>− особые приметы разыскиваемого. | В соответствии со статьей 11 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных (с изменениями на 29 июля 2017 года)» обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской |

| Категория ПДн | Перечень ПДн | Обоснование |
|---|---|---|
| | | Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации. Данные заносятся диспетчером ДДС-02 в дополнительные поля карточки диспетчера ДДС-02 системы-112. |

В системе-112 не обрабатываются персональные данные сотрудников оператора.

В соответствии с таблицей 5 система-112 является информационной системой, обрабатывающей специальные категории персональных данных.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Недекларированные возможности – функциональные возможности программных средств и средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В качестве общесистемного программного обеспечения используются программные средства приобретаемые централизовано у доверенного вендора, с соблюдением авторских прав и лицензионности. Разработку УСПО-112 осуществило МЧС России, пусконаладочные работы УСПО-112 (БД ПДн) осуществляет доверенная организация. Соглашение о конфиденциальности, заключаемое с сотрудниками, реализующими данные функции, и реализованная система защиты информации позволяют судить о маловероятности наличия НДВ в системном и прикладном ПО системы-112.

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» системы-112 являются актуальными угрозы 3 типа – не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.

Поскольку для системы-112 актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора для системы-112 необходимо обеспечить 2-ой уровень защищенности персональных данных.

## 1.4 Модель угроз безопасности

### 1.4.1 Определение уровня исходной защищенности системы-112

Исходная защищенность информационной системы (системы-112) оценивается по «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. Заместителем директора ФСТЭК России от 14.02.2008). Согласно Методике уровень исходной защищенности определяется по показателям, приведенным в таблице 6.

Таблица 6 – Показатели исходной защищенности информационной системы

| Технические и эксплуатационные характеристики ИС | Уровень защищенности | | |
|---|---|---|---|
| | высокий | средний | низкий |
| 1. По территориальному размещению: | | | |
| − распределенная ИС, которая охватывает несколько областей; | – | – | + |
| − городская ИС, охватывающая не более одного населенного пункта; | – | – | + |
| − корпоративная ИС, охватывающая не более одной организации; | – | + | – |
| − кампусная ИС из близкорасположенных зданий; | – | + | – |
| − локальная ИС в пределах одного здания | + | – | – |
| 2. По наличию соединения с сетями общего пользования: | | | |
| − многоточечный выход; | – | – | + |
| − одноточечный выход; | – | + | – |
| − отсутствие выхода | + | – | – |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: | | | |
| − чтение, поиск; | + | – | – |
| − запись, удаление, сортировка; | – | + | – |
| − модификация, передача | – | – | + |
| 4. По разграничению доступа к персональным данным: | | | |
| − имеют доступ определенный перечень сотрудников; | – | + | – |
| − имеют доступ сотрудники одной организации; | – | – | + |
| − имеют доступ все (общедоступные данные) | – | – | + |
| 5. По наличию соединений с другими базами данных иных ИС: | | | |
| − используется несколько БД; | – | – | + |
| − используется одна БД | + | – | – |

| Технические и эксплуатационные характеристики ИС | Уровень защищенности | | |
|---|---|---|---|
| | высокий | средний | низкий |
| 6. По уровню обобщения (обезличивания) ПДн: | | | |
| − используются только обезличенные данные; | + | – | – |
| − данные обезличиваются при передаче в другие организации; | – | + | – |
| − используются не обезличенные данные | – | – | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям без предварительной обработки: | | | |
| − предоставляется вся БД; | – | – | + |
| − предоставляется часть БД; | – | + | – |
| − информация не предоставляется | + | – | – |

ИС имеет высокий исходный уровень защищенности, если не менее 70% показателей соответствуют уровню «высокий», а остальные «среднему». В этом случаеY1=0.

ИС имеет средний исходный уровень защищенности, если «высоких» и «средних» оценок не менее 70% («низких» оценок не более 30%). В этом случае Y1=5.

Во всех остальных случаях ИС имеет низкий исходный уровень защищенности, Y1=10.

Характеристики исходной защищенности системы-112, полученные в результате сопоставления параметров этой системы с показателями исходной защищенности ИС, рассмотренными выше, приведены в таблице 7.

Таблица 7 – Показатели исходной защищенности системы-112

| Технические и эксплуатационные характеристики системы-112 | Уровни защищенности | | |
|---|---|---|---|
| | высокий | средний | низкий |
| По территориальному размещению:<br>распределенная ИС, которая охватывает несколько областей | | | + |
| По наличию соединения с сетями общего пользования:<br>ИС, имеющая многоточечный выход в сеть общего пользования | | | + |
| По встроенным (легальным) операциям с записями баз данных:<br>модификация, передача | | | + |
| По разграничению доступа к информации:<br>ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект данных | | + | |
| По наличию соединений с другими базами данных иных ИС:<br>используется несколько БД | | | + |
| По уровню обобщения (обезличивания) ПДн:<br>ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | | | + |
| По объему данных, которые предоставляются сторонним пользователям ИС без предварительной обработки:<br>ИС, предоставляющая часть данных | | + | |

| | | | |
|---|---|---|---|
| Процентное соотношение | 0 | 28.57 | 71.43 |

Система-112 имеет низкий уровень исходной защищенности, т.к. менее 70% характеристик ИС соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений).

При составлении перечня актуальных угроз информации низкому уровню исходной защищенности ставится в соответствие числовой коэффициент Y1 равный 10.

### 1.4.2 Вероятность реализации угроз информационной безопасности

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для ИС в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны (Y2 = 5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности информации не приняты (Y2 = 10).

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

Возможность реализации угрозы считается:

«низкой» при $0 \le Y \le 0,3$;

«средней» при $0,3 < Y \le 0,6$;

«высокой» при $0,6 \le Y \le 0,8$;

«очень высокой» при $0,8 < Y$.

С учетом оценок уровня защищенности для системы-112 Y1=10.

Оценка опасности угроз информационной безопасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

Низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов.

Средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов.

Высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов.

### 1.4.3 Классификация угроз безопасности информации по методическим документам ФСТЭК России

Состав и содержание угроз определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к информации.

Совокупность таких условий и факторов формируется с учетом характеристик ИС, свойств среды (пути) распространения информационных сигналов, содержащих защищаемую информацию и возможностей источников угроз.

Угрозы классифицируются в соответствии с перечисленными ниже признаками.

По видам возможных источников угроз:

– угрозы, связанные с действиями лиц, имеющих доступ к ИС (внутренний нарушитель);

– угрозы, связанные с действиями лиц, не имеющих доступ к ИС (внешний нарушитель).

По структуре системы-112, на которую направлена реализация угроз:

– угрозы системе-112 на базе АРМ;

– угрозы системе-112 на базе локальных информационных систем;

– угрозы системе-112 на базе распределенных информационных систем.

По виду несанкционированных действий, осуществляемых с информацией:

– угрозы, приводящие к нарушению конфиденциальности информации (нет непосредственного воздействия на информацию);

– угрозы, приводящие к несанкционированному воздействию на содержание информации (изменение или уничтожение информации);

– угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы системы-112 (блокирование информации).

По способам реализации угроз:

– угрозы, реализуемые в системе-112 при ее подключении к сетям связи общего пользования;

– угрозы, реализуемые в системе-112 при ее подключении к сетям международного информационного обмена;

– угрозы, реализуемые в системе-112, не имеющих подключений к сетям связи общего пользования и сетям международного информационного обмена.

По виду каналов, с использование которых реализуется угроза:

– угрозы, реализуемые через технические каналы утечки;

– угрозы, реализуемые за счет НСД к информации.

### 1.4.4 Угрозы, реализуемые по техническим каналам утечки информации

Угрозы утечки информации по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки информации.

Источниками угрозы являются физические лица, не имеющие доступа к системе-112.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.

Носителем информации является пользователь ИС, акустическая система, воспроизводящая информацию, а также технические средства ИС и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке информации в ИС возможно возникновение угроз за счет реализации следующих технических каналов утечки информации:

– канал утечки акустической (речевой) информации;

– канал утечки видовой информации;

– канал утечки информации за счет ПЭМИН.

***Угроза, реализуемая за счет утечки акустической (речевой) информации***

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Угроза, реализуемая за счет утечки видовой информации***

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС.

Необходимое условие осуществления просмотра (регистрации) информации является наличие прямой видимости между средством наблюдения и носителем информации.

Угрозы утечки видовой информации в системе-112 маловероятны, так как в ИС исключен просмотр выводимой текстовой информации в помещениях ИС установлены жалюзи на окнах. Посетители в помещения, в которых расположены ТС системы-112, не допускаются без сопровождения лиц, допущенных в КЗ. Размещение экранов мониторов специальным образом исключает несанкционированный просмотр информации. Серверное оборудование не имеет постоянно функционирующих средств отображения информации.

Все оборудование, необходимое для функционирования Системы-112, находится в пределах КЗ. Приняты организационные меры, при которых неконтролируемое пребывание посторонних лиц в служебных помещениях.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Угроза, реализуемая за счет утечки информации по каналам ПЭМИН***

Угроза утечки информации по каналам ПЭМИН реализуется за счет перехвата техническими средствами побочных (не связанных с прямыми функциональными значениями элементов ИС) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации техническими средствами ИС.

В данных помещениях функционирует множество ВТСС (телефонные средства; средства и системы охранной и пожарной сигнализации; средства и системы оповещения и сигнализации; средства и системы кондиционирования и т.д.), создающие электромагнитные помехи.

Угрозы утечки информации по каналам ПЭМИН, связанные с действиями лиц, не имеющих доступ к ИС (внешний нарушитель), маловероятны, так как использование данного канала утечки не является эффективным (малое количество информации) и очень трудоемким (дорогостоящая специализированная аппаратура, длительное время на настройку и обработку данных). Реализация данной угрозы может привести только к нарушению конфиденциальности информации (копирование, неправомерное распространение).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

### 1.4.5 Угрозы, реализуемые за счет несанкционированного доступа к информации

Угрозы, связанные с несанкционированным доступом (далее – НСД), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИС, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий.

Угрозы НСД в ИС с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространение), целостности (уничтожения, изменения) и доступности (блокирования) информации, и включают в себя:

– угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ

общего применения);

– угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.д.;

– угрозы внедрения вредоносных программ (программно-математического воздействия).

Угрозы, реализуемые за счет несанкционированного доступа к информации с использованием штатного программного обеспечения, разделяются на угрозы уничтожения, хищения аппаратных средств ИС путем физического доступа к элементам ИС, а также на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

***Источники угрозы НСД в системе-112***

Источниками угрозы НСД в ИС могут быть:

***Нарушители:***

Нарушители, не имеющие доступ к системе-112, реализующие угрозы из внешних сетей общего пользования и (или) сетей международного информационного обмена (внешние нарушители) – к данным нарушителям можно отнести лиц, использующих несанкционированный доступ к системе-112 через сеть общего пользования (Интернет) (существует низкая вероятность подобных действий).

Нарушители, имеющие доступ к системе-112, включая пользователей системы-112, реализующие угрозы непосредственно в системе-112 (внутренние нарушители):

– зарегистрированные пользователи системы-112, осуществляющие ограниченный доступ к ресурсам системы-112 с рабочего места;

– зарегистрированные пользователи системы-112, осуществляющие удаленный доступ к информации по локальным и (или) распределенным информационным системам;

– зарегистрированные пользователи системы-112 с полномочиями системного администратора системы-112;

– зарегистрированные пользователи системы-112 с полномочиями администратора безопасности системы-112.

***Вредоносные программы:***

Программные закладки – актуальны, но маловероятны.

Программные вирусы – не актуальны, т.к. установлено программное средство антивирусной защиты Dr.Web Enterprise Security Suite.

Вредоносные программы, распространяющиеся по сети – актуальны.

Другие вредоносные программы, предназначенные для осуществления НСД – актуальны.

***Уязвимости в системе-112***

К уязвимостям в системе-112 относятся:

Уязвимости программного обеспечения – актуальны.

Уязвимости, вызванные наличием в ИС программно-аппаратной закладки – актуальны, но маловероятны.

Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных – актуальны.

Уязвимости, вызванные недостатками организации ТЗИ от НСД – актуальны.

Уязвимости в СЗИ – актуальны, но маловероятны.

Уязвимости программно-аппаратных средств ИС в результате сбоев в работе, отказов этих средств – актуальны.

***Объекты воздействия на систему-112***

Информация, обрабатывающаяся на АРМ (узле) вычислительной сети:

в средствах (портах) ввода/вывода информации – средства в АРМ и серверах системы-112.

Информация в средствах, реализующих сетевое взаимодействие, и каналах передачи данных и активное сетевое оборудование.

### 1.4.6 Угрозы уничтожения, хищения аппаратных средств путем физического доступа к элементам системы-112

***Кража ПЭВМ***

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы системы-112.

На объектах информатизации, которые входят в состав системы-112, обеспечивается круглосуточная физическая охрана, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Кража носителей информации***

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

На объектах информатизации, которые входят состав системы-112, обеспечивается круглосуточная физическая охрана, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Кража, модификация, уничтожение информации***

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИС и средства защиты, а также происходит работа пользователей.

На объектах информатизации, которые подключены к системе-112, обеспечивается круглосуточная физическая охрана, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Вывод из строя узлов ПЭВМ и каналов связи***

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИС и проходят каналы связи.

В организации введен контроль доступа в контролируемую зону, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ***

Угроза осуществляется путем НСД к информации при проведении ремонта и уничтожения носителей информации.

В системе-112, носители информации, располагаются только в серверном сегменте.

В организации введен контроль доступа в контролируемую зону, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Несанкционированное отключение средств защиты***

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИС.

В организации введен контроль доступа в контролируемую зону, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Угрозы, реализуемые за счет непосредственного доступа***

Эти угрозы могут быть реализованы в случае получения физического доступа к ИС или, по крайней мере, к средствам ввода/вывода информации в ИС. Их можно объединить в три группы:

– угрозы, реализуемые в ходе загрузки ОС;

– угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем;

– угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.

***Угрозы, реализуемые в ходе загрузки ОС***

Эти угрозы направлены на перехват паролей и идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехвата управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду АРМ. Чаще всего такие угрозы реализуются с использованием отчужденных носителей информации.

Реализацией данной угрозы могут заниматься внутренние нарушители, т.е. зарегистрированные пользователи, осуществляющие ограниченный доступ к серверной части системы-112 с рабочего места, с целью получения доступа к информации.

Реализация данной угрозы не приводит к негативным последствиям для субъектов данных, т.к. направлена на получение доступа в операционную среду АРМ. В системе введено разграничение прав пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО.

Частота (вероятность) реализации угрозы – низкая вероятность (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем***

Эти угрозы направлены на выполнение непосредственно несанкционированного доступа к информации.

При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями ОС или какой-либо прикладной программой общего пользования, так и специально созданными для выполнения несанкционированного доступа программами.

Работа пользователей осуществляется на АРМ исключительно с при помощи специализированного программного обеспечения УСПО-112.

Виды нарушений безопасности в случае реализации угрозы:

нарушение конфиденциальности информации (копирование, неправомерное распространение).

Реализация данной угрозы может привести к негативным последствиям для субъектов данных, ущерб может проявляться в виде несанкционированного доступа к информации посторонних лиц, а также возможного распространения информации.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – средняя.

Вероятность реализации угрозы признается низкой, доступ из УСПО-112 к серверу ИСПДн организуется с использованием личных логинов и паролей сотрудников, допущенных к работе с УСПО.

***Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ***

Эти угрозы направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться какой-либо прикладной программой общего пользования.

Виды нарушений безопасности, в случае реализации угрозы, и непосредственный ущерб совпадают с видами и ущербом для предыдущей угрозы.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – средняя.

***Угрозы, реализуемые за счет удаленного доступа***

Угрозы удаленного доступа, реализуемые с использованием протоколов межсетевого взаимодействия:

- анализ сетевого трафика;
- сканирование сети;
- подмена доверенного объекта сети;
- навязывание ложного маршрута сети;
- внедрение ложного объекта сети;
- перехват за пределами КЗ;
- удаленный запуск приложений;
- внедрение по сети вредоносных программ;
- угроза выявления пароля.

***Анализ сетевого трафика***

Угроза реализуется с помощью специальной программы анализатора пакетов, перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передается идентификатор пользователя и его пароль.

В системе-112 пользователи не имеют прав на изменение параметров системы и не могут запускать многие приложения, в том числе и программы анализатора пакетов.

Возможные последствия:

Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей.

Реализация данной угрозы не приводит к негативным последствиям для субъектов данных, т.к. информационный обмен в систему-112 осуществляется посредством защищенной сети оператора связи.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Сканирование сети***

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИС и анализе ответов от них.

Возможные последствия:

Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Реализация данной угрозы не приводит к негативным последствиям для субъектов данных, для нарушения безопасности информации необходимо реализовывать последующие угрозы НСД.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Подмена доверенного объекта***

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы - с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных. В результате реализации угрозы нарушитель получает права доступа к техническому средству ИС.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Навязывание ложного маршрута сети***

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИС. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Внедрение ложного объекта сети***

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются

различные протоколы удаленного поиска (например, ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Перехват за пределами контролируемой зоны***

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Удаленный запуск приложений***

Угроза заключается в стремлении запустить на хосте ИС различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

распространение файлов, содержащих несанкционированный исполняемый код;

удаленный запуск приложения путем переполнения буфера приложений серверов;

удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним.

Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде документа, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса, нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Внедрение по сети вредоносных программ***

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

– программы подбора и вскрытия паролей;
– программы, реализующие угрозы;
– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИС;
– программы-генераторы компьютерных вирусов;
– программы, демонстрирующие уязвимости средств защиты информации и др.

На АРМ и серверах системы-112 установлены средства антивирусной защиты.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Угроза выявления пароля***

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Реализуется с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена объекта сети (IP-адресов) и перехват пакетов.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Отказ в обслуживании***

Угроза основана на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда ОС оказывается не в состоянии обрабатывать поступающие пакеты.

Разновидности угроз «Отказ в обслуживании»:

Скрытый отказ в обслуживании, вызванный частичным исчерпанием ресурсов ИС на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов.

Возможные последствия:

Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

Явный отказ в обслуживании, вызванный исчерпанием ресурсов ИС при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание). При этом легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д.

Возможные последствия:

Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в

установлении соединения. Отказ в предоставлении сервиса.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

Явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИС при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации.

Возможные последствия:

Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов и т.п.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

Явный отказ в обслуживании, вызванный использованием ошибок в программном обеспечении (ПО).

Передача злоумышленником пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер, что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Возможные последствия:

Нарушение работоспособности сетевых устройств.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

### 1.4.7 Угрозы хищения, модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств

***Действия вредоносных программ***

Программно-математическое воздействие – это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На АРМ и серверах системы-112 установлены средства антивирусной защиты.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Установка ПО, несвязанного с исполнением служебных обязанностей***

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИС или ее элементов.

На объектах информатизации, которые подключены к системе-112 введено разграничение прав пользователей на установку ПО и осуществляется контроль. Пользователи проинструктированы о порядке установки ПО.

На АРМ установлено средство защиты информации от несанкционированного доступа Secret Net.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Y=(10+2)/20=0,6 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

### 1.4.8 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС

***Утрата ключей и атрибутов доступа***

Угроза осуществляется за счет действия человеческого фактора пользователей ИС. Они нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Частота (вероятность) реализации угрозы – высокая (Y2=10).

Y=(10+10)/20=1 реализуемость угрозы – очень высокая.

Опасность угрозы – высокая.

***Непреднамеренная модификация (уничтожение) информации сотрудниками***

Угроза осуществляется за счет действия человеческого фактора пользователей ИС, которые нарушают положения принятых правил работы в ИС или не осведомлены о них.

Проектными решениями по созданию системы-112 предусмотрено резервное копирование обрабатываемой информации.

Частота (вероятность) реализации угрозы – средняя (Y2=5).

Y=(10+5)/20=0,75 реализуемость угрозы – высокая.

Опасность угрозы – низкая.

***Непреднамеренное отключение средств защиты***

Угроза осуществляется за счет действия человеческого фактора пользователей ИС, которые нарушают положения принятых правил работы с ИС и средствами защиты или не осведомлены о них.

Частота (вероятность) реализации угрозы – средняя (Y2=5).

Y=(10+5)/20=0,75 реализуемость угрозы – высокая.

Опасность угрозы – средняя.

***Выход из строя аппаратно-программных средств***

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

Проектными решениями по созданию системы-112 предусмотрено резервное копирование обрабатываемой информации.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Сбой системы электроснабжения***

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации. На объектах информатизации, которые подключены к системе-112, используются источники бесперебойного питания. А также проектными решениями по созданию системы-112 предусмотрено резервное копирование обрабатываемой информации.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Стихийное бедствие***

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

На объектах информатизации, которые подключены к системе-112, установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

### 1.4.9 Угрозы преднамеренных действий пользователей

***Доступ к информации, ее модификация и уничтожение лицами, не допущенными к ее обработке***

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИС и средства защиты, а также происходит работа пользователей.

В организациях введен контроль доступа в контролируемую зону, установлена охранная сигнализация, функционирование системы-112 осуществляется в режиме 24х7х365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Y=(10+0)/20=0,5 реализуемость угрозы – средняя.

Опасность угрозы – низкая.

***Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к ее обработке***

Угроза осуществляется за счет действия человеческого фактора пользователей ИС, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

Частота (вероятность) реализации угрозы – высокая (Y2=10).
Y=(10+10)/20=1 реализуемость угрозы – очень высокая.
Опасность угрозы – высокая.

### 1.4.10 Выявление актуальных угроз

Выявление актуальных угроз выполняется на основе правил, приведенных в таблице 8, рекомендованных в «Методике определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн» (ФСТЭК России, 2008 г.).

Таблица 8 – Правила выявления актуальных угроз безопасности информации

| Возможность реализации угрозы | Показатель опасности угрозы | | |
|---|---|---|---|
| | низкая | средняя | высокая |
| Низкая | Неактуальная | Неактуальная | Актуальная |
| Средняя | Неактуальная | Актуальная | Актуальная |
| Высокая | Актуальная | Актуальная | Актуальная |
| Очень высокая | Актуальная | Актуальная | Актуальная |

В таблице 9 приведены перечень и оценки актуальности угроз для системы-112.

Таблица 9 – Перечень и оценки актуальности угроз для системы-112

| Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y1=10)) | | Частота (вероятность) реализации угрозы, Y2 | Возможность реализации угрозы, Y | Опасность угрозы | Актуальность |
|---|---|---|---|---|---|
| Угрозы, реализуемые через технические каналы утечки информации | | | | | |
| 1 | Угроза утечки акустической (речевой) информации | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 2 | Угрозы утечки видовой информации | Низкая (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 3 | Угрозы утечки информации по каналам ПЭМИН | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| Угрозы, реализуемые за счет несанкционированного доступа к информации | | | | | |
| 4 | Угрозы уничтожения, хищения аппаратных средств ИС путем физического доступа к элементам ИС | | | | |
| 4.1 | Кража ПЭВМ | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 4.2 | Кража носителей информации | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 4.3 | Кража, модификация, уничтожение информации | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 4.4 | Вывод из строя узлов ПЭВМ, каналов связи | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 4.5 | Несанкционированный доступ к информации | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |

| Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y1=10)) | | Частота (вероятность) реализации угрозы, Y2 | Возможность реализации угрозы, Y | Опасность угрозы | Актуальность |
|---|---|---|---|---|---|
| | при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | | | | |
| 4.6 | Несанкционированное отключение средств защиты | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 5 | Угрозы непосредственного доступа | | | | |
| 5.1 | Угрозы, реализуемые в ходе загрузки ОС | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 5.2 | Угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем | Низкая (Y2=2) | Средняя (Y=0,6) | Средняя | Актуальная |
| 5.3 | Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ | Низкая (Y2=2) | Средняя (Y=0,6) | Средняя | Актуальная |
| 6 | Угрозы удаленного доступа | | | | |
| 6.1 | Анализ сетевого трафика | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 6.2 | Сканирование сети | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 6.3 | Подмена доверенного объекта сети | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 6.4 | Навязывание ложного маршрута сети | Маловероятная (Y2=0) | Низкая (Y=0,5) | Низкая | Неактуальная |
| 6.5 | Внедрение ложного объекта сети | Маловероятная (Y2=0) | Низкая (Y=0,5) | Низкая | Неактуальная |
| 6.6 | Перехват за пределами КЗ | Маловероятная (Y2=0) | Низкая (Y=0,5) | Низкая | Неактуальная |
| 6.7 | Удаленный запуск приложений | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 6.8 | Внедрение по сети | Низкая | Средняя | Низкая | Неактуальна |

| Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y1=10)) | | Частота (вероятность) реализации угрозы, Y2 | Возможность реализации угрозы, Y | Опасность угрозы | Актуальность |
|---|---|---|---|---|---|
| | вредоносных программ | (Y2=2) | (Y=0,6) | | я |
| 6.9 | Угроза выявления пароля | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 7 | Отказ в обслуживании | | | | |
| 7.1 | Скрытый отказ в обслуживании (частичное исчерпание ресурсов) | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 7.2 | Явный отказ в обслуживании (исчерпание ресурсов) | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 7..3 | Явный отказ в обслуживании (нарушение логической связности) | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 7.4 | Явный отказ в обслуживании (ошибки в ПО) | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий) | | | | | |
| 8 | Действия вредоносных программ (вирусов) | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 9 | Установка ПО, не связанного с исполнением служебных обязанностей | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| 10 | Недекларированные возможности системного ПО и ПО для обработки ПДн | Низкая (Y2=2) | Средняя (Y=0,6) | Низкая | Неактуальная |
| Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС и СрЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера | | | | | |
| 11 | Утрата ключей и атрибутов доступа | Высокая (Y2=10) | Очень высокая (Y=1) | Высокая | Актуальная |
| 12 | Непреднамеренная модификация (уничтожение) информации | Средняя (Y2=5) | Высокая (Y=0,75) | Низкая | Актуальная |

| Наименование угрозы (ИС имеет низкий уровень исходной защищенности (Y1=10)) | | Частота (вероятность) реализации угрозы, Y2 | Возможность реализации угрозы, Y | Опасность угрозы | Актуальность |
|---|---|---|---|---|---|
| | сотрудниками | | | | |
| 13 | Непреднамеренное отключение средств защиты | Средняя (Y2=5) | Высокая (Y=0,75) | Средняя | Актуальная |
| 14 | Выход из строя аппаратно-программных средств | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 15 | Сбой системы электроснабжения | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 16 | Стихийное бедствие | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| Угрозы преднамеренных действий пользователей | | | | | |
| 17 | Доступ к информации, ее модификация и уничтожение лицами, не допущенными к ее обработке | Маловероятная (Y2=0) | Средняя (Y=0,5) | Низкая | Неактуальная |
| 18 | Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к ее обработке | Высокая (Y2=10) | Очень высокая (Y=1) | Высокая | Актуальная |

### 1.4.11 Определение базового набора мер защиты информации для соответствующего класса защищённости и уровня защищенности информационной системы

Определение базового набора мер защиты информации для установленного класса и уровня защищенности информационной системы-112 осуществлено в соответствии с базовыми наборами мер защиты информации в соответствии с Требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17. Базовый набор мер защиты информации приведен в таблице 10.

Таблица 10 - Базовый набор мер защиты информации

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | |
| УПД.6 | Ограничение неуспешных попыток входа в информационную системы (доступа к информационной системе) | + |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | + |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-коммуникационные сети | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | + |
| III. Ограничение программной среды (ОПС) | | |
| ОПС.2 | Управление установкой (инстралляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих устанвоке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | + |
| ОПС.3 | Установка (инсталляция) только | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | разрешенного к использованию программного обеспечения и (или) его компонентов | |
| IV. | Защита машинных носителей информации (ЗНИ) | |
| ЗНИ.1 | Учет машинных носителей персональных данных | + |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | + |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных | + |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | + |
| V. | Регистрация событий безопасности (РСБ) | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | + |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | + |
| РСБ.6 | Генерирование временных меток и | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | (или) синхронизация системного времени в информационной системе | |
| РСБ.7 | Защита информации о событиях безопасности | + |
| VI. Антивирусная защита (АВЗ) | | |
| АВЗ.1 | Реализация антивирусной защиты | + |
| АВЗ.2 | Обновление базы данных признаков вредоностных компьютерных программ (вирусов) | + |
| VII. Обнаружение вторжений (СОВ) | | |
| СОВ.1 | Обнаружение вторжений | + |
| СОВ.2 | Обновление базы решающих правил | + |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | + |
| АНЗ.4 | Контроль состава техничнских средств, программного обеспечения и средств защиты информации | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной среде | + |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | средств защиты информации | |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы | + |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | + |
| X. Обеспечение доступности информации (ОДТ) | | |
| ОДТ.3 | Контроль безотказного функционирования техничесикх средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | + |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | + |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | + |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации | + |
| XI. Защита среды виртуализации (ЗСВ) | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами вирутализации | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | том числе внутри вирутальных машин | |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | + |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | + |
| ЗСВ.6 | Управление перемещением вирутальных машин (контейнеров) и обрабатываемых на них данных | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | + |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | + |
| ЗСВ.10 | Разбиение вирутальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) шруппой пользователей | + |
| | XII. Защита технических средств (ЗТС) | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | + |
| ЗТС.3 | Контроль и управление физическим доступом к | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы | + |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | + |
| ЗИС.7 | Контроль санкционированного и исключение несанкционированного | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода | |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи | + |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации | + |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю | + |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя | + |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | изменению в процессе обработки информации | |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | + |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | + |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы | + |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями | + |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения | + |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе | + |

### 1.4.12 Адаптация базового набора мер защиты информации для соответствующего класса защищённости и уровня защищенности информационной системы

Неактуальными мерами из базового набора мер признаны следующие меры: ИАФ.2 в части идентификации и аутентификации мобильных и портативных устройств, ИАФ.6, УПД.14, УПД.15, все меры защиты среды виртуализации (ЗСВ), ЗИС.5, ЗИС.7, ЗИС.8, ЗИС.9, ЗИС.20, ЗИС.30. Адаптированный базовый набор мер защиты информации приведен в таблице 11.

Таблица 11 - Адаптированный базовый набор мер защиты информации

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + |
| ИАФ.2 | Идентификация и аутентификация стационарных устройств | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | |
| УПД.6 | Ограничение неуспешных попыток входа в информационную системы (доступа к информационной системе) | + |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | + |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | + |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-коммуникационные сети | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | + |
| III. Ограничение программной среды (ОПС) | | |
| ОПС.2 | Управление установкой (инстралляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | + |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | + |
| IV. Защита машинных носителей информации (ЗНИ) | | |
| ЗНИ.1 | Учет машинных носителей персональных данных | + |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных | + |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | + |
| V. Регистрация событий безопасности (РСБ) | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | + |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | + |
| РСБ.7 | Защита информации о событиях безопасности | + |
| VI. Антивирусная защита (АВЗ) | | |
| АВЗ.1 | Реализация антивирусной защиты | + |
| АВЗ.2 | Обновление базы данных | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | признаков вредоностных компьютерных программ (вирусов) | |
| VII. Обнаружение вторжений (СОВ) | | |
| СОВ.1 | Обнаружение вторжений | + |
| СОВ.2 | Обновление базы решающих правил | + |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | + |
| АНЗ.4 | Контроль состава техничнских средств, программного обеспечения и средств защиты информации | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной среде | + |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | + |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| X. | Обеспечение доступности информации (ОДТ) | |
| ОДТ.3 | Контроль безотказного функционирования техничесикх средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | + |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | + |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | + |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации | + |
| XI. | Защита технических средств (ЗТС) | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | + |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации и средствам обеспечения функционирования информационной системы, в | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | помещения и сооружения, в которых они установлены | |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + |
| XII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы | + |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю | + |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя | + |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации | + |
| ЗИС.17 | Разбиение информационной | + |

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Для класса защищенности К2 |
|---|---|---|
| | системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы | + |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями | + |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения | + |

### 1.4.13 Уточнение адаптированного базового набора мер защиты информации для соответствующего класса защищённости и уровня защищенности информационной системы

Анализ угроз безопасности информации, обрабатываемой в систем-112 показал, что основными причинами возникновения актуальных угроз являются следующие факторы:

преднамеренные или случайные действия пользователей и обслуживающего персонала;

недоработки организационных мер по противодействию угрозам безопасности.

С учетом этого произведено уточнение адаптированного базового набора мер защиты информации. Результат представлен в таблице 12.

Таблица 12 - Уточненный адаптированный базовый набор мер защиты информации

| Условное обозначение и номер меры | Меры защиты информации в информационных системах |
|---|---|
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.2 | Идентификация и аутентификация стационарных устройств |
| ИАФ.3 | Управление идентификаторами, в том числе |

| | |
|---|---|
| | создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную системы (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-коммуникационные сети |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| III. Ограничение программной среды (ОПС) | |
| ОПС.2 | Управление установкой (инстралляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, |

| | |
|---|---|
| | контроль за установкой компонентов программного обеспечения |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |
| IV. Защита машинных носителей информации (ЗНИ) | |
| ЗНИ.1 | Учет машинных носителей персональных данных |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания |
| V. Регистрация событий безопасности (РСБ) | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в |

| | |
|---|---|
| | информационной системе |
| VI. Антивирусная защита (АВЗ) | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоностных компьютерных программ (вирусов) |
| VII. Обнаружение вторжений (СОВ) | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава техничнских средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной среде |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| X. Обеспечение доступности информации (ОДТ) | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного |

| | |
|---|---|
| | обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования техничесикх средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| XI. Защита технических средств (ЗТС) | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| XII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по |

| | |
|---|---|
| | обработке информации и иных функций информационной системы |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |

### 1.4.14 Дополнение уточненного адаптированного базового набора мер защиты информации. Определение необходимого класса СКЗИ для защиты циркулирующих в системе персональных данных

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

– если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

– если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

В системе-112 несанкционированный доступ к персональным данным со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

Для системы-112 актуальны угрозы 3-его типа при этом необходимо обеспечить 2-й уровень защищенности.

Таким образом, использование СКЗИ для обеспечения безопасности персональных данных в системе-112 является актуальным.

Выбор соответствующего класса СКЗИ для системы-112 определяется в соответствии с требованиями, указанными в Приказе ФСБ России от 10.07.2014 № 378. В соответствии с данным Приказом для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе необходимо применять СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3 типа.

Для определения соответствующего класса СКЗИ для системы-112 необходимо проанализировать возможные способы создания, подготовки и проведения атак на систему, а также возможные действия нарушителей.

***Определение актуальных угроз и класса СКЗИ***

*Объекты защиты и актуальные характеристики безопасности объектов защиты угрозы*

Помимо персональных данных к объектам защиты относятся:

СКЗИ;

– среда функционирования СКЗИ (далее – СФ);

– информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

– документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;

– носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

– используемые информационной системой каналы (линии) связи, включая кабельные системы;

– помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

СКЗИ и СФ размещаются на всех объектах системы-112. В ЦОВ (РЦОВ) и ЕДДС МО системы-112 оборудование СКЗИ размещается специально приспособленном помещении серверной.

К информации, относящейся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ, а также документации на СКЗИ и на технические и программные компоненты СФ, имеет доступ только администратор информационной безопасности системы-112, расположенный в ЦОВ (РЦОВ).

В системе-112 используются каналы (линии) связи, арендуемые у оператора связи (выбирается

на конкурсной основе).

Серверные аппаратные средства ЦОВ/РЦОВ размещаются в специально оборудованном серверном помещении ЦОВ/РЦОВ, АРМ пользователей размещаются в помещениях дежурно-диспетчерских служб экстренного реагирования, а также в ЦОВ, РЦОВ и ЕДДС. Доступ к помещениям обеспечивается в соответствии с контрольно-пропускным режимом.

*Классификация и характеристики нарушителей, а также их возможности по реализации атак*

Все физические лица, имеющие доступ к ресурсам системы-112, могут быть классифицированы как:

– лица, не имеющие права доступа в контролируемую зону, в которой размещены технические средства системы-112;

– лица, имеющие право постоянного или разового доступа в контролируемую зону, в которой размещены технические средства системы-112.

Все лица, не имеющие права доступа в контролируемую зону, в которой размещены технические средства системы-112 относятся к категориям:

– лиц не стремящихся к непосредственному доступу к средствам системы-112, размещенным в контролируемой зоне;

– лиц, которые могут осуществить попытку доступа в контролируемую зону.

Все лица, имеющие право постоянного или разового доступа в контролируемую зону, в которой размещены технические средства системы-112 могут быть отнесены к следующим категориям:

– пользователи системы-112;

– лица, не являющиеся пользователями системы-112.

К отдельной категории пользователей системы-112 относятся привилегированные пользователи информационной системы (члены группы администраторов). К администраторам системы-112 (технический персонал, осуществляющий настройку и конфигурирование оборудования и средств защиты информации системы-112) относятся сотрудники системы-112, которые осуществляют:

– эксплуатацию и обслуживание программно-технических средств системы-112, в т.ч. обслуживание технических и программных средств СКЗИ и СФ, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями;

– эксплуатацию и обслуживание средств защиты информации, используемых в системе-112;

– администрирование системы-112 в целом и определение уровней полномочий пользователей.

Лица, не являющиеся пользователями системы-112, подразделяются на:

– сотрудников организации-эксплуатанта системы-112, имеющих санкционированный доступ в помещения, в которых размещаются технические средства системы-112, в служебных целях и не относящихся к группе администраторов (работники по уборке помещений, сотрудники пожарной охраны);

– обслуживающий персонал организации-эксплуатанта системы-112 (охрана, работники инженерно-технических служб и т. д.).

Сотрудники системы-112 и сторонние организации, осуществляющие сопровождение и ремонт технических средств, обладают необходимым уровнем квалификации и имеют полномочия доступа к техническим средствам системы-112. Пользователи и обслуживающий персонал организации-эксплуатанта системы-112 не имеют необходимых прав доступа и необходимой квалификации для изменения технологических процессов работы криптосредств и СФК, а также организации атак.

Таким образом, вероятным нарушителем для криптосредств и СФК может считаться внешний нарушитель и администраторы системы-112.

Степень информированности внешнего нарушителя, по существу, зависит от реализуемых в системе-112 технических и организационных мер.

Предполагается, что вероятные внешние нарушители обладают достаточной информацией, необходимой для подготовки и проведения атак, за исключением той информации, доступ к которой исключен для нарушителя разрабатываемой системой защиты информации.

Внутренний нарушитель (администратор системы-112) имеет возможность доступа к фрагментам информации, содержащей общедоступную информацию и технологическую информацию, в том числе служебную информация СКЗИ системы-112. Также имеет возможность изменять конфигурацию технических средств системы-112, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам системы-112. Внутренний нарушитель имеет широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам (в том числе - возможность осуществления прямого физического доступа к техническим средствам системы) и хорошего знания технологии обработки информации и защитных мер. Действия этой категории нарушителей напрямую связаны с нарушением установленных правил и инструкций.

***Обобщенные возможности источников атак***

На основании исходных данных о системе-112, объектах защиты и источниках атак определены обобщенные возможности источников атак, представленные в таблице 13.

Таблица 13 – Данные об обобщенных возможностях источников атак

| № | Обобщенные возможности источников атак | Да/нет |
|---|---|---|
| 1 | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны | Да |
| 2 | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования | Да |
| 3 | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования | Да |
| 4 | Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ) | Нет |
| 5 | Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения) | Нет |
| 6 | Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ) | Нет |

***Актуальные угрозы и выбор класса СКЗИ***

Реализация угроз безопасности ПДн, обрабатываемых в системе-112, определяется

возможностями источников атак, описанных выше. Таким образом, актуальность использования возможностей источников атак определяет наличие соответствующих актуальных угроз. В таблице 14 представлен анализ уточненных возможностей нарушителей и направления атак (соответствующие актуальные угрозы) и приведено обоснование неактуальности некоторых угроз на основании особенностей функционирования системы-112.

Таблица 14 – Уточненные актуальные угрозы

| № | Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальность использования (применения) для построения и реализации атак | Обоснование отсутствия |
|---|---|---|---|
| 1.1 | проведение атаки при нахождении в пределах контролируемой зоны | актуально | |
| 1.2 | проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ; Помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ | актуально | |
| 1.3 | получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ. | актуально | |
| 1.4 | использование штатных | актуально | |

| | | | |
|---|---|---|---|
| | средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий. | | |
| 2.1 | физический доступ к СВТ, на которых реализованы СКЗИ и СФ | актуально | |
| 2.2 | возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | актуально | |
| 3.1 | создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО | не актуально | В качестве общесистемного программного обеспечения используются программные средства приобретаемые централизовано у доверенного вендора, с соблюдением авторских прав и лицензионности. Доработку УСПО-112 (БД ПДн) осуществляет доверенная организация. Соглашение о конфиденциальности, заключаемое с сотрудниками, реализующими данные функции, и реализованная система защиты информации позволяют судить о маловероятности наличия НДВ в системном и прикладном ПО системы-112 и возможности такой атаки. |
| 3.2 | проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в | не актуально | Исходя из того, что в системе-112 не осуществляется обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять |

| | | | |
|---|---|---|---|
| | информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | | интерес для реализации такой возможности, ввиду высокой стоимости и сложности подготовки такой вид атаки не рассматривается. |
| 3.3 | проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ | не актуально | В научно-исследовательских центрах могут проводить работы по созданию способов и средств атак специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств; располагают наряду с доступными в свободной продаже документацией на криптосредство и СФ исходными текстами прикладного программного обеспечения. Однако, исходя из того, что в системе-112 не осуществляется обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации такой возможности, ввиду высокой стоимости и сложности подготовки такой вид атаки не рассматривается. |
| 4.1 | создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО | не актуально | В качестве общесистемного программного обеспечения используются программные средства приобретаемые централизовано у доверенного вендора, с соблюдением авторских прав и лицензионности. Доработку УСПО-112 (БД ПДн) осуществляет доверенная организация. Соглашение о конфиденциальности, заключаемое с сотрудниками, реализующими данные функции, и реализованная система защиты информации позволяют судить о |

| | | | |
|---|---|---|---|
| | | | маловероятности наличия НДВ в системном и прикладном ПО системы-112 и возможности такой атаки. |
| 4.2 | возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ | не актуально | Исходя из того, что в системе-112 не осуществляется обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации такой возможности, ввиду высокой стоимости и сложности подготовки такой вид атаки не рассматривается. |
| 4.3 | возможность располагать всеми аппаратными компонентами СКЗИ и СФ | не актуально | Исходя из того, что в системе-112 не осуществляется обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации такой возможности, ввиду высокой стоимости и сложности подготовки такой вид атаки не рассматривается. |

В результате анализа актуальных атак, представленных в таблице 11, для системы-112 предусматривается использование СКЗИ класса КС3.

## 2 Определение видов и типов средств защиты информации, обеспечивающих реализацию технических мер защиты информации

Итоговый перечень мер защиты информации и средства их реализации приведены в таблице 15.

Таблица 15 - Итоговый перечень мер защиты информации и средства их реализации приведены

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Требования и средства реализации |
|---|---|---|
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.<br>При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся |

| | | |
|---|---|---|
| | | работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.<br>Реализуется встроенными механизмами операционной системы и средством защиты от НСД Secret Net, программно-аппаратный комплекс "Соболь", ViPNet Administrator. |
| ИАФ.2 | Идентификация и аутентификация стационарных устройств | Идентификация устройств в информационн ой системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.<br>Аутентификация устройств в информацион ной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.<br>Встроенные механизмы операционной системы, средства УСПО, ViPNet Coordinator, ViPNet Administrator. |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:<br>определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;<br>формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;<br>присвоение идентификатора пользователю и (или) устройству;<br>предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;<br>блокирование идентификатора пользователя после установленного оператором времени неиспользования.<br>Реализация средствами УСПО, ViPNet Administrator и организационными мерами оператора. |
| ИАФ.4 | Управление средствами | определение должностного лица (администратора) оператора, ответственного за |

| | | |
|---|---|---|
| | аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;<br>изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;<br>выдача средств аутентификации пользователям;<br>генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);<br>установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):<br>а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;<br>б) задание минимального количества измененных символов при создании новых паролей;<br>в) задание максимального времени действия пароля;<br>г) задание минимального времени действия пароля;<br>д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;<br>блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;<br>назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);<br>обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;<br>защита аутентификационной информации от неправомерных доступа к ней и модифицирования.<br>Реализуется встроенными механизмами операционной системы и средством защиты от НСД Secret Net. |
| ИАФ.5 | Защита обратной связи при вводе | Защита обратной связи "система - субъект доступа" в процессе аутентификации |

| | | |
|---|---|---|
| | аутентификационной информации | обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками "*", "●" или иными знаками.<br>Реализуется встроенными механизмами операционной системы и средствами защиты от НСД. |
| II. | Управление доступом субъектов доступа к объектам доступа (УПД) | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:<br>определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);<br>объединение учетных записей в группы (при необходимости);<br>верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;<br>заведение, активация, блокирование и уничтожение учетных записей пользователей;<br>пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;<br>порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;<br>оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;<br>уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;<br>предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными |

| | | |
|---|---|---|
| | | системами.<br>Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).<br>Реализуется встроенными механизмами операционной системы, средствами защиты от НСД и средствами УСПО. |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | Реализуется ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности). Реализация осуществляется средствами УСПО. |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) | должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:<br>фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором;<br>разрешение передачи информации в информационной системе только по маршруту, установленному оператором;<br>изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;<br>запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.<br>Реализуется с использованием средств УСПО и ViPNet Coordinator. |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | Оператором должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий |

| | | |
|---|---|---|
| | | (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).<br>Реализуется организационными мерами. |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.<br>Реализуется организационными мерами оператора. |
| УПД.6 | Ограничение неуспешных попыток входа в информационную системы (доступа к информационной системе) | В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).<br>Реализуется встроенными механизмами операционной системы, средствами защиты от НСД и средствами УСПО. |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).<br>Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.<br>Реализуется встроенными механизмами операционной системы, средствами защиты от НСД и средствами УСПО. |

| | | |
|---|---|---|
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (вебсайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).<br>Реализуется встроенными механизмами операционной системы и средствами защиты от НСД. |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-коммуникационные сети | Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:<br>установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;<br>ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2;<br>предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);<br>мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;<br>контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).<br>Реализуется ПАК ViPNet Coordinator, ПО ViPNet Administrator 3.x (КС3). |
| УПД.16 | Управление взаимодействием с информационными | Управление взаимодействием с внешними информационными системами должно включать:<br>предоставление доступа к информационной |

| | | |
|---|---|---|
| | системами сторонних организаций (внешние информационные системы) | системе только авторизованным (уполномоченным) пользователям в соответствии с УПД.2;<br>определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;<br>определение системных учетных записей, используемых в рамках данного взаимодействия;<br>определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;<br>определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.<br>Средства УСПО, ViPNet Coordinator, средства защиты от НСД. |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | Доверенная загрузка должна обеспечивать:<br>блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;<br>контроль доступа пользователей к процессу загрузки операционной системы;<br>контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.<br>ПО ViPNet Administrator 3.x (КС3), средства защиты от НСД |
| III. Ограничение программной среды (ОПС) | | |
| ОПС.2 | Управление установкой (инстралляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов | должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:<br>определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;<br>настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске |

| | | |
|---|---|---|
| | программного обеспечения | установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);<br>выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен);<br>контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);<br>определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.<br>Реализация средствами УСПО и средствами защиты от НСД. |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке ("белый список"), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке ("черный список"). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются).<br>Реализуется механизмами операционной системы, средствами защиты от НСД и организационными мерами. |
| | IV. Защита машинных носителей информации (ЗНИ) | |
| ЗНИ.1 | Учет машинных носителей персональных данных | Учету подлежат:<br>съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);<br>портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, |

| | | |
|---|---|---|
| | | цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);<br>машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).<br>Реализуется организационными мерами. |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | должен быть определен перечень должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:<br>съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);<br>портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);<br>машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);<br>предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций);<br>Реализуется организационными мерами. |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | При контроле перемещения машинных носителей информации должны осуществляться:<br>определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;<br>предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функции);<br>учет перемещаемых машинных носителей информации в соответствии с ЗНИ.1;<br>периодическая проверка наличия машинных носителей информации.<br>Реализуется организационными мерами. |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах должно предусматривать: |

| | | |
|---|---|---|
| | хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах | определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);<br>физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);<br>защита машинных носителей информации до уничтожения (стирания) с них данных и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации.<br>Реализуется организационными мерами. |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных | Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать:<br>определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе;<br>определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода);<br>принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода);<br>контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).<br>Средства защиты от НСД и организационные меры. |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации | Контроль ввода (вывода) информации на машинные носители информации должен предусматривать:<br>определение оператором типов носителей информации, ввод (вывод) информации на которые подлежит контролю;<br>определение оператором категорий пользователей, которым предоставлены полномочия по вводу (выводу) информации на машинные носители в соответствии с УПД.2;<br>запрет действий по вводу (выводу) информации для пользователей, не имеющих |

| | | |
|---|---|---|
| | | полномочий на ввод (вывод) информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации;<br>регистрация действий пользователей и событий по вводу (выводу) информации на машинные носители информации в соответствии с РСБ.3.<br>Организационные меры, средства УСПО, средства защиты от НСД. |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.<br>Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.<br>Реализуется через организационные меры. |
| V. Регистрация событий безопасности (РСБ) | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.<br>Реализуется организационными мерами и ViPNet IDS, ViPNet Administrator. |
| РСБ.2 | Определение состава и содержания информации о событиях | Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность |

| | | |
|---|---|---|
| | безопасности, подлежащих регистрации | идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.<br>Реализуется организационными мерами и ViPNet IDS, ViPNet Administrator. |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:<br>возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с РСБ.1;<br>генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2;<br>хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1.<br>Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1.<br>Реализуется организационными мерами, средствами ОС, ViPNet, ViPNet Administrator. |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | Реагирование на сбои при регистрации событий безопасности должно предусматривать:<br>предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;<br>реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о |

| | | |
|---|---|---|
| | | событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.<br>Реализуется организационными мерами, средствами ОС, ViPNet Administrator, ПАК Соболь |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.<br>Реализуется организационными мерами, средствами ОС, ViPNet Administrator, средствами защиты от НСД. |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.<br>Средствами операционной системы |
| РСБ.7 | Защита информации о событиях безопасности | Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.<br>Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.<br>Средства операционной системы, организационные меры, средства защиты от НСД. |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе | Сведения о действиях отдельных пользователей в информационной системе должны предоставляться уполномоченным должностным лицам для просмотра и анализа с целью расследования причин возникновения инцидентов в информационной системе в соответствии с законодательством Российской Федерации.<br>Реализуется средствами операционной системы, организационными мерами, средствами защиты от НСД, ViPNet Administrator |

| VI. Антивирусная защита (АВЗ) | | |
|---|---|---|
| АВЗ.1 | Реализация антивирусной защиты | Реализация антивирусной защиты должна предусматривать:<br>применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);<br>установку, конфигурирование и управление средствами антивирусной защиты;<br>предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;<br>проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);<br>проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;<br>оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);<br>определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).<br>Реализуется организационными мерами, а также применением программного обеспечения Dr.Web®, сертифицированного ФСТЭК. |
| АВЗ.2 | Обновление базы | Обновление базы данных признаков |

| | | |
|---|---|---|
| | данных признаков вредоностных компьютерных программ (вирусов) | вредоносных компьютерных программ (вирусов) должно предусматривать:<br>получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);<br>получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);<br>контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).<br>Реализуется организационными мерами, а также применением программного обеспечения Dr.Web®, сертифицированного ФСТЭК. |
| VII. Обнаружение вторжений (СОВ) | | |
| СОВ.1 | Обнаружение вторжений | Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.<br>Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором.<br>Реализуется с использованием ViPNet. |
| СОВ.2 | Обновление базы решающих правил | Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:<br>получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;<br>получение из доверенных источников и установку обновлений базы решающих правил;<br>контроль целостности обновлений базы решающих правил.<br>Реализуется с использованием ViPNet. |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное | При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:<br>выявление (поиск) уязвимостей, связанных с ошибками кода в программном |

| | | |
|---|---|---|
| | устранение вновь выявленных уязвимостей | (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;<br>разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;<br>анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;<br>устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;<br>информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.<br>Реализуется организационными мерами |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.<br>Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах.<br>Реализуется организационными мерами, а также применением программного обеспечения Dr.Web®, сертифицированного ФСТЭК, средствами операционной системы, ViPNet |

| | | |
|---|---|---|
| | | Administrator |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:<br>контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;<br>проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;<br>контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;<br>восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.<br>Реализуется организационными мерами, средствами УСПО-112, средствами операционной системы, ViPNet. |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:<br>контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;<br>контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;<br>контроль выполнения условий и сроков действия сертификатов соответствия на средства |

| | | |
|---|---|---|
| | | защиты информации и принятие мер, направленных на устранение выявленных недостатков;<br>исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.<br>Реализуется организационными мерами. |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной среде | При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:<br>контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;<br>контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;<br>контроль реализации правил разграничения доступом в соответствии с УПД.2;<br>контроль реализации полномочий пользователей в соответствии с УПД.4 и УПД.5;<br>контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;<br>устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.<br>Реализуется организационными мерами, средствами УСПО-112, средствами операционной системы, ViPNet. |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:<br>контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в |

| | | |
|---|---|---|
| | | процессе работы информационной системы;<br>контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;<br>контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;<br>тестирование с периодичностью установленной оператором функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АНЗ.1 и АНЗ.2;<br>обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3.<br>Организационные меры, средства резервного копирования и восстановления, средства УСПО-112, средства защиты от НСД. |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы | Контроль целостности информации, содержащейся в базах данных информационной системы, должен предусматривать:<br>контроль целостности с периодичностью, установленной оператором, структуры базы данных по наличию имен (идентификаторов) и (или) по контрольным суммам программных компонент базы данных в процессе загрузки и (или) динамически в процессе работы информационной системы;<br>контроль целостности с периодичностью, установленной оператором, объектов баз данных, определяемых оператором, по контрольным суммам и (или) с использованием криптографических методов в соответствии с законодательством Российской Федерации в процессе загрузки и (или) динамически в процессе работы информационной системы;<br>обеспечение физической защиты технических средств информационной системы, на которых установлена база данных, в соответствии с ЗТС.2 и ЗТС.3.<br>Средства УСПО-112. |

| | | |
|---|---|---|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | Для обеспечения возможности восстановления программного обеспечения в информационной системе должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.<br>Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:<br>восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;<br>восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;<br>возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.<br>Реализуется организационными мерами, средствами УСПО-112, средствами защиты от НСД, средствами резервного копирования и восстановления. |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему | Ограничение прав пользователей по вводу информации предусматривает ограничение по вводу в определенные типы объектов доступа (объекты файловой системы, объекты баз данных, объекты прикладного и специального программного обеспечения) информации исходя из задач и полномочий, решаемых пользователем в информационной системе.<br>Реализуется средствами УСО-112 в части ролей пользователей, а также средствами операционной системы. |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему | Контроль точности, полноты и правильности данных, вводимых в информационную систему, обеспечивается путем установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в информационную систему (допустимые наборы символов, размерность, область числовых значений, допустимые значения, количество символов) для |

| | | |
|---|---|---|
| | | подтверждения того, что ввод информации соответствует заданному оператором формату и содержанию.<br>Реализуется средствами УСПО-112, а также средствами операционной системы. |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях должен предусматривать:<br>определение оператором типов ошибочных действий пользователей, которые потенциально могут привести к нарушению безопасности информации в информационной системе;<br>генерирование сообщений для пользователей об их ошибочных действиях и о возможности нарушения безопасности информации в информационной системе для корректировки действий пользователей;<br>регистрация информации об ошибочных действиях пользователей, которые могут привести к нарушению безопасности информации в информационной системе, в журналах регистрации событий безопасности в соответствии с РСБ.3;<br>предоставление доступа к сообщениям об ошибочных действиях пользователей только администраторам.<br>Реализуется средствами УСПО-112, а также средствами операционной системы. |
| X. Обеспечение доступности информации (ОДТ) | | |
| ОДТ.1 | Использование отказоустойчивых технических средств | определение сегментов информационной системы, в которых должны применяться отказоустойчивые технические средства, обладающие свойствами сохранять свою работоспособность после отказа одного или нескольких их составных частей, и перечня таких средств исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;<br>определение предельных (пороговых) значений характеристик (коэффициента) готовности, показывающего, какую долю времени от общего времени работы информационной системы техническое средство (техническое решение) находится в рабочем состоянии, и характеристик надежности (требуемое значение вероятности отказа в единицу времени) исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и |

| | | |
|---|---|---|
| | | доступности информации, установленных оператором;<br>применение в информационной системе технических средств с установленными оператором характеристиками (коэффициентом) готовности и надежности, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;<br>контроль с установленной оператором периодичностью за значениями характеристик (коэффициентов) готовности и надежности технических средств и реагирование на ухудшение значений данных характеристик (инициализация плана восстановления работоспособности и иные методы реагирования);<br>замена технических средств, характеристики (коэффициенты) готовности и надежности которых достигли предельного значения.<br>Реализуется путем использования в системе-112 технических средств, обеспечивающих характеристики, соответствующие расчету надежности, приведенному в проекте на систему-112. |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы | определение сегментов информационной системы, в которых должно осуществляться резервирование технических средств, программного обеспечения, каналов передачи информации и средств обеспечения функционирования, а также перечня резервируемых средств исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;<br>применение резервных (дублирующих) технических средств, программного обеспечения, каналов передачи информации и (или) средств обеспечения функционирования информационной системы, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;<br>ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении требуемых условий непрерывности функционирования информационной системы и доступности информации. |

| | | |
|---|---|---|
| | | Реализуется путём резервирования аппаратных средств (серверов, сетевого оборудования), резервированием объектов системы-112 ЦОВ (РЦОВ), использованием основных и резервных каналов связи. |
| ОДТ.3 | Контроль безотказного функционирования техничесикх средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия "ответов", визуального контроля, контроля трафика, контроля "поведения" системы или иными методами).<br>При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с ОЦЛ.3, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах.<br>Реализуется средствами апаратного обеспечения, а также организационными мерами. |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью;<br>разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;<br>регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;<br>принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.<br>Реализуется организационными мерами, а также средствами резервного копирования и восстановления. |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в | Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:<br>определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности |

| | | |
|---|---|---|
| | течение установленного временного интервала | информации;<br>восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;<br>регистрация событий, связанных с восстановлением информации с резервных машинных носителей информации.<br>Реализуется организационными мерами, а также средствами резервного копирования и восстановления. |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов | В информационной системе должно обеспечиваться выделение групп однотипных узлов, объединенных каналами передачи информации и рассматриваемых как единый программно-технический ресурс, информационной системы в целом и (или) отдельных ее сегментов (серверов приложений, файловых серверов, серверов баз данных, средств защиты информации и иных сегментов) для обеспечения доступности информации, сервисов и механизмов защиты информации.<br>Реализуется путем дублирования функциональных объектов ЦОВ (РЦОВ), резервированием каналов связи. |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации | контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);<br>мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей);<br>мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) услуг по передаче информации.<br>Реализуется организационными мерами. |
| XI. Защита технических средств (ЗТС) | | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и | Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств. |

| | | |
|---|---|---|
| | средства защиты информации, а также средства обеспечения функционирования | Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации.<br>Реализуется организационными мерами, в т.ч. посетители в помещения, в которых расположены ТС системы-112, не допускаются без сопровождения лиц, допущенных в КЗ. Все оборудование, необходимое для функционирования Системы-112, находится в пределах КЗ. Приняты организационные меры, при которых неконтролируемое пребывание посторонних лиц в служебных помещениях маловероятно. |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | Контроль и управление физическим доступом должны предусматривать:<br>определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;<br>санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;<br>учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.<br>Реализуется организационными мерами. |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее | В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, |

| | | |
|---|---|---|
| | несанкционированный просмотр | мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.<br>Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.<br>Реализуется организационными мерами. |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) | выполнение норм и правил пожарной безопасности;<br>выполнение норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств;<br>обеспечение необходимых для эксплуатации технических средств температурно-влажностного режима и условий по степени запыленности воздуха.<br>Реализуется организационными мерами и мерами по приспособлению помещений, описанными в техническом проекте на создание системы-112. |
| XII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы | Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.<br>Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) |

| | | |
|---|---|---|
| | | информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.<br>Реализация стредствами операционной системы, средствами VipNet Administrator |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.<br>Реализуется применением ViPNet Coordinator. |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) | Оператором должен быть определен перечень целей (функций) передачи данных, для которых требуется доверенный канал (маршрут).<br>Доверенный канал между пользователем и средствами защиты информации должен обеспечиваться при удаленном и локальном доступе в информационную систему.<br>Реализуется применением ViPNet Coordinator и средствами защиты от НСД. |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с ИАФ.2 и ЗИС.10.<br>Реализуется применением механизмов защищенного удаленного доступа (VPN), применением ViPNet Coordinator |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю | определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);<br>обеспечение целостности информации при ее подготовке к передаче и непосредственной ее |

| | | |
|---|---|---|
| | | передаче по каналам связи в соответствии с ЗИС.3;<br>регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.<br>Реализуется средствами УСПО-112 в рамках использования единой УКИО в системе-112. |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя | Для исключения возможности отрицания пользователем факта получения информации должны осуществляться:<br>определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);<br>обеспечение целостности полученной информации в соответствии с ЗИС.3;<br>регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.<br>Реализуется средствами УСПО-112 в рамках использования единой УКИО в системе-112. |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором в соответствии с настоящим методическим документом, направленных на обеспечение их конфиденциальности и целостности.<br>Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.<br>Реализуется организационными мерами, средствами защиты от НСД и межсетевого экранирования. |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | |
| ЗИС.18 | Обеспечение загрузки и исполнения | выделение в составе операционной системы и прикладного программного обеспечения частей, |

| | | |
|---|---|---|
| | программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения | немодифицируемых в процессе загрузки и выполнения, и размещение их на машинных носителях информации, доступных только для чтения;<br>загрузка и выполнение на средствах вычислительной техники, определяемых оператором, операционной системы с машинных носителей информации, доступных только для чтения;<br>загрузка и выполнение на средствах вычислительной техники прикладного программного обеспечения, определяемого оператором, с машинных носителей информации, доступных только для чтения.<br>Реализуется средствами операционной системы и УСПО-112. |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы | Исключение доступа к информации через общие для пользователей ресурсы должно обеспечивать запрет доступа текущему пользователю (учетной записи) или текущему процессу к системным ресурсам (реестрам, оперативной памяти, внешним запоминающим устройствам) при их повторном использовании, в которых хранится информация другого (предыдущего) пользователя.<br>Реализуется средствами операционной системы и УСПО-112. |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы | Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.2, ОДТ.4 и ОДТ.5.<br>Реализуется применением механизмов защищенного удаленного доступа (VPN) и использованием отказоустойичовго оборудования, резервированием каналов и объектов системы-112. |
| ЗИС.23 | Защита периметра | управление (контроль) входящими в |

| | | |
|---|---|---|
| | (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями | информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);<br>обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).<br>Реализуется применением механизмов защищенного удаленного доступа (VPN), ViPNet Coordinator. |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения | В информационной системе должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.<br>Реализуется средствами межсетевого экранирования. |

**Лист регистрации изменений**

| Изм. | Номер листов (страниц) | | | | Всего листов (страниц) в докум. | № докум. | Входящий № сопроводительного докум. и дата | Подп. | Дата |
|---|---|---|---|---|---|---|---|---|---|
| | измененных | замененных | новых | аннулированных | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Подп. и дата | Инв. № | Взам. инв. | Подп. и дата | Инв. №