Проект

«Об утверждении Методики определения угроз безопасности в информационных системах персональных данных, Типового перечня угроз безопасности персональных данных при обработке персональных данных в информационных системах персональных данных и Форму перечня видов угроз»

В соответствии со статьей 8 Закона Кыргызской Республики «О нормативных правовых актах Кыргызской Республики», во исполнение пункта 2 постановления Правительства Кыргызской Республики от 21 ноября 2017 года № 760, а также руководствуясь абзацами Положением о Государственном комитете информационных технологий и связи Кыргызской Республики, утвержденного постановлением Правительства Кыргызской Республики от 15 июля 2016 года № 402, **приказываю**:

1. Утвердить Методику определения угроз безопасности в информационных системах персональных данных, согласно приложению 1.
2. Утвердить Типовой перечень угроз безопасности персональных данных при обработке персональных данных в информационных системах персональных данных, согласно приложению 2.
3. Утвердить Форму перечня видов угроз, согласно приложению 3.
4. Настоящий приказ вступает в силу со дня официального опубликования.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Председатель
Н.Э.Абасканов

СПРАВКА-ОБОСНОВАНИЕ

к проекту приказа ГКИТС КР «Об утверждении Методики определения угроз безопасности в информационных системах персональных данных, Типового перечня угроз безопасности персональных данных при обработке персональных данных в информационных системах персональных данных и Форму перечня видов угроз»

Настоящие проекты документов разработаны во исполнение пункта 2 постановления Правительства Кыргызской Республики от 21 ноября 2017 года № 760 и в целях установления механизмов по определению угроз безопасности в информационных системах персональных данных и защиты персональных данных при их обработке в информационных системах, обрабатывающих персональные данные в зависимости от требуемого уровня защищенности.

В соответствии с частью первой статьи 17 Закона Кыргызской Республики «Об информации персонального характера» держатель (обладатель) массива персональных данных обязан обеспечивать режим конфиденциальности персональных данных и определить

обработчика для обработки персональных данных, предоставляющего гарантии в отношении мер технической безопасности и организационных мер, регулирующих обработку персональных данных, за исключением случаев, когда держатель (обладатель) самостоятельно возлагает на себя функции и обязанности обработчика, а также обеспечивать сохранность и достоверность персональных данных, а также установленный в нормативном порядке режим доступа к ним. При этом в соответствии со статьей 21 обозначенного Закона держатель (обладатель) массива персональных данных и обработчик принимают необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. При обработке персональных данных держатель (обладатель) массива персональных данных и обработчик обязаны:

- исключить доступ посторонних лиц к оборудованию, используемому для обработки персональных данных (контроль за доступом);

- препятствовать самовольному чтению, копированию, изменению или выносу носителей данных (контроль за пользованием носителями данных);

- препятствовать самовольной записи персональных данных и изменению или уничтожению записанных персональных данных (контроль за записью) и обеспечивать возможность установления задним числом когда, кем и какие персональные данные были изменены;

- обеспечить безопасность систем обработки данных, предназначенных для переноса персональных данных независимо от средств передачи данных (контроль за средствами передачи данных);

- обеспечить, чтобы каждый пользователь системы обработки данных имел доступ только к тем персональным данным, к обработке которых он имеет допуск (контроль за допуском);

- обеспечить возможность установления задним числом когда, кем и какие персональные данные вводились в систему обработки данных (контроль за вводом);

- не допускать несанкционированного чтения, копирования, изменения и уничтожения персональных данных при передаче и транспортировке персональных данных (транспортный контроль);

- обеспечить конфиденциальность информации, полученной при обработке персональных данных;

- обеспечить выполнение установленных Правительством Кыргызской Республики требований к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

Вместе с тем Правительство Кыргызской Республики устанавливает уровни защищенности персональных данных при их обработке в информационных системах, требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

При этом в соответствии со статьей 29 обозначенного Закона Правительством Кыргызской Республики определяется уполномоченный государственный орган Кыргызской Республики, который ведет учет и регистрацию массивов персональных данных и их держателей (обладателей).

Вместе с тем согласно части первой статьи 29-1 вышеназванного Закона, на уполномоченный

государственный орган возлагается обеспечение контроля, за соответствием обработки персональных данных требованиям данного Закона, защитой прав субъектов персональных данных.

Так, в соответствии с проектом постановления Правительства Кыргызской Республики «Об уполномоченном государственном органе по защите персональных данных» будут внесены соответствующие изменения в Положение о Государственном комитете информационных технологий и связи Кыргызской Республики, предусматривающие определение Комитета уполномоченным государственным органом в сфере защиты персональных данных.

В связи с чем в целях принятия нормативных правовых актов, направленных на урегулирование вопросов, связанных с защитой персональных данных, настоящим проектом приказа ГКИТС КР предлагается утвердить Методику определения угроз безопасности в информационных системах персональных данных, Типовой перечень угроз безопасности персональных данных при обработке персональных данных в информационных системах персональных данных, форму перечня угроз, которые позволят выполнять Требования по обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных утвержденные постановлением Правительства Кыргызской Республики от 21 ноября 2017 годя № 760.

Настоящая Методика предназначена для использования при проведении анализа существующих и возможных угроз безопасности обработки персональных данных в информационных системах персональных данных в целях выполнения требований по защите персональных данных в информационных системах с учетом конкретных условий эксплуатации информационных систем персональных данных и оценки рисков, в которой раскрываются:

- типы источников угроз безопасности информации (антропогенные угрозы, техногенные угрозы и угрозы от стихийных бедствий и иных природных явлений);

- комплексный характер угроз, требующий учета различных факторов, таких как возможностей вероятных нарушителей, учитывающих их потенциал, оснащенность и мотивацию; потенциальных уязвимостей информационной системы; вероятных способов реализации угроз безопасности информации; определения объектов информационной системы, на которые направлена угроза безопасности информации;

- последствия от реализации угроз;

- актуальность существующих угроз безопасности персональных данных.

- модель нарушителя, определяющая вид нарушителя, тип нарушителя, мотивацию нарушителя и потенциал нарушителя;

- оценка вероятности (возможности) реализации угрозы безопасности как низкой, средней или высокой вероятности реализации угрозы безопасности информации определяемых экспертным путем в зависимости от структурно-функциональных характеристик информационной системы и условий эксплуатации информационной системы персональных данных;

- оценка степени возможного ущерба от реализации угрозы безопасности от видов ущерба (экономический; политический; репутационный; ущерб в области обороны, безопасности и правопорядка; субъекту персональных данных; технологический).

- определение актуальности угрозы безопасности информации в зависимости от степени возможного ущерба и вероятности реализации угрозы;

- состав мер по обеспечению безопасности персональных данных включающую:

а)идентификация и аутентификация субъектов доступа и объектов доступа:

б) управление доступом субъектов доступа к объектам доступа;

в) ограничение программной среды;

г) защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

д) регистрация событий безопасности;

е) антивирусная защита;

ж) обнаружение (предотвращение) вторжений;

з) контроль (анализ) защищенности персональных данных;

к) обеспечение целостности информационной системы и персональных данных;

л) обеспечение доступности персональных данных;

м) защита среды виртуализации;

н) защита технических средств;

о) защита информационной системы, ее средств, систем связи и передачи данных;

п) выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

р) управление конфигурацией информационной системы и системы защиты персональных данных.

Данная Методика определяет порядок действий при определении требуемых мер защиты персональных данных, начиная от выбора базового набора мер защиты, его адаптации с учетом структурно-функциональных характеристик и особенностей функционирования информационных систем персональных данных, дальнейшего уточнение адаптированного набора мер защиты и при необходимости его дополнения.

Методика включает в себя приложения:

- Рекомендации по экспертной оценке определения угроз безопасности информации, раскрывающие вопросы по созданию экспертной группы и проведению экспертной оценки угроз безопасности информации (приложение 1);

- Структура модели угроз безопасности информации определяеющую состав и содержание разделов модели угроз (приложение 2);

- Определение потенциала нарушителя по реализации угрозы безопасности информации в информационной системе, которая позволяет через численную оценку потенциала нарушителя по пяти основным параметрам, характеризующим нарушителя (затрачиваемому времени, компетентности, осведомленности, возможности доступа, оснащенности) оценить его потенциал качественно в градации низкий-средний-высокий (приложение 3);

- Состав мер по обеспечению безопасности обработки персональных данных для уровней защищенности персональных данных, которая является сводной таблицей необходимых мер безопасности в зависимости от уровня защищенности информационных систем персональных данных (приложение 4);

- Содержание мер защиты персональных данных, которые содержат подробное описание мер защиты персональных данных, указанных в приложении 4, с требованиями к реализации и требованиями к усилению каждой из этих мер (приложение 5).

Принятие настоящего проекта приказа ГКИСТ КР не повлечет за собой социальных, экономических, правовых, правозащитных, гендерных, экологических, коррупционных или иных последствий.

Проведенный анализ показал, что представленный проект приказа не противоречит нормам действующего законодательства, а также вступившим в установленном порядке в силу международных договорам, участницей которых является Кыргызская Республика.

Председатель

Государственного комитета

информационных технологий

и связи Кыргызской республики **Н.Э. Абасканов**

Приложение 1

к Приказу ГКИТиС КР

от _____№_____

МЕТОДИКА

определения угроз безопасности в информационных системах персональных данных

1. **Общие положения**

1. Настоящая Методика устанавливает механизмы определения угроз безопасности в информационных системах персональных данных и защиты персональных данных при их обработке в информационных системах, обрабатывающих персональные данные в зависимости от требуемого уровня защищенности персональных данных.
2. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
3. Защита персональных данных включает в себя организационные и (или) технические меры, определяемые с учетом актуальных угроз безопасности персональных данных, а также используемых информационных технологий.
4. В настоящей методике используются следующие термины:

- **персональные данные** - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для

его биологической, экономической, культурной, гражданской или социальной идентичности.

- **информационная система персональных данных** (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **уровень защищенности персональных данных** – один из четырех условных градаций по степени безопасности ИСПД, установленных требованиями к обеспечению безопасности и защите персональных данных;
- **держатель (обладатель)** массива персональных данных - органы государственной власти, органы местного самоуправления и юридические лица, на которые возложены полномочия определять цели, категории персональных данных и контролировать сбор, хранение, обработку и использование персональных данных в соответствии с настоящим Законом Кыргызской Республики «Об информации персонального характера»;
- **обработчик -** физическое или юридическое лицо, определяемое держателем (обладателем) персональных данных, которое осуществляет обработку персональных данных на основании заключенного с ним договора;
- **угроза** — совокупность условий и факторов, создающих опасность нарушения безопасности объекту или субъекту защиты. Под угрозами понимаются, потенциально возможные события, действия (воздействия), процессы или явления, которые могут привести к нанесению ущерба чьим-либо интересам;
- **внешние нарушители** – нарушители, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
- **внутренние нарушители** – нарушители, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

2. **Организация безопасности обработки информации в ИСПД**

1. Держатель (обладатель) массива персональных данных и обработчик обязаны принимать необходимые правовые, организационные и технические меры и (или) обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
2. В соответствии с «Требованиями по обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных» по оценке актуальности угроз, возможности нанесения ущерба, объема обрабатываемых персональных данных, категории персональных данных и продолжительности обработки персональных данных предусмотрены четыре уровня защищенности персональных данных ИСПД:

- красный;
- желтый;
- зеленый;
- синий.

3. Определение уровня защищенности персональных данных осуществляется держателем (обладателем) массива персональных данных.
4. Договор между держателем и обработчиком должен включать обязанности обработчика по обеспечению безопасности персональных данных при их обработке в ИСПД.

5. Контроль исполнения требований по обеспечению безопасности персональных данных в ИСПД организуется и проводится обработчиком или привлеченным на договорной основе юридическим лицом, имеющим право на осуществление деятельности по защите информации (далее вместе – оператор). Контроль проводится на регулярной основе в сроки, определяемые оператором.
6. В настоящей методике не рассматриваются вопросы касающихся процессов обеспечения безопасности персональных данных, отнесенных в установленном порядке к государственным секретам.

3. **Определение угроз безопасности информации**

1. Предварительно должны быть определены физические и логические границы ИСПД, для которых принимаются и контролируются меры защиты персональных данных.
2. Для определения угроз безопасности персональных данных необходимо установить существующие или предполагаемые возможности нарушений свойств безопасности персональных данных (конфиденциальности, целостности или доступности) в ИСПД, а также произвести оценку последствий нарушения в виде ущерба держателя, оператора ИСПД или субъектов персональных данных.
3. Оценка угроз безопасности персональных данных проводится экспертным методом. Рекомендации по формированию экспертной группы и проведению экспертной оценки угроз безопасности информации приведены в Приложении 1.
4. При определении угроз безопасности информации оценке подлежат те угрозы, у которых источники имеют возможности и условия для реализации угрозы в рассматриваемой информационной системе с заданными структурно-функциональными характеристиками с учетом особенностей ее функционирования.
5. К основным типам источников угроз безопасности информации относятся:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий и иных природных явлений).

6. Особое внимание следует уделять оценке антропогенных угроз, связанных с несанкционированными действиями физических лиц, как преднамеренного, так и непреднамеренного характера.
7. Преднамеренные угрозы безопасности предполагают целенаправленные действия с целью получения доступа к определенной информации, нарушения функционирования информационной системы или нарушения функционирования обслуживающей инфраструктуры информационной системы.
8. Непреднамеренные угрозы безопасности информации возникают, когда лица, имеющие доступ к информационной системе, производят действия без определенного умысла, в результате которых могут нарушаться условия и сама безопасность информации.
9. Для ИСПД, в которых критичными являются обеспечение целостности и доступности персональных данных, в обязательном порядке подлежат оценке техногенные угрозы. Источниками техногенных угроз являются отказы и сбои технических средств или программного обеспечения, обусловленные их низким качеством или надежностью оборудования или программных продуктов, сетей или услуг связи, систем резервирования или технического обслуживания и т.п.
10. Угрозы безопасности информации (далее УгБИ) носят комплексный характер и требуют проведения оценки следующих факторов, влияющих на угрозу:

- возможностей вероятных нарушителей (далее ВозН), учитывающих их потенциал, оснащенность и мотивацию;
- потенциальных уязвимостей информационной системы (далее УязИС);
- вероятных способов реализации угроз безопасности информации (далее СпРУг);
- объекты воздействия (далее ОВ) **-** объектов информационной системы, на которые направлена угроза безопасности информации;
- последствий от нарушения конфиденциальности, целостности, доступности информации: (далее $ПН^{к/ц/д}$).

Каждая угроза безопасности информации в информационной системе описывается (идентифицируется) с учетом выявленных факторов влияния и условно записывается следующим образом:

$$\mathbf{УгБИ_j = [(ВозН) + (УязИС) + (СпРУг) + (ОВ) + (ПН^{к/ц/д})]}$$

11. Описанная угроза безопасности информации подлежит нейтрализации (блокированию), если она является актуальной (далее $УгБИ^{A}_{j}$). Угроза принимается актуальной для информационной системы, если существует вероятность (возможность P_j) реализации идентифицированной угрозы нарушителем с соответствующим потенциалом и её реализация приведет к неприемлемым негативным последствиям (ущербу X_j):

$$\mathbf{УгБИ^{A}_j = [(P_j); (X_j)]}$$

12. Актуальные угрозы безопасности информации включаются в модель угроз безопасности информации. Модель угроз безопасности ИСПД представляет собой формализованное описание угроз безопасности персональных данных конкретной ИСПД в конкретных условиях её функционирования. Модель угроз безопасности информации разрабатывается владельцем информационного ресурса с привлечением специалистов по информационной безопасности. Структура модели угроз безопасности информации приведена в Приложении 2.
13. При определении угроз безопасности информации следует учитывать структурные и функциональные характеристики информационной системы, применяемые технологии и особенности (условия) функционирования информационной системы.
14. Эффективность мер защиты персональных данных зависит от качества проведенных работ по выявлению угроз безопасности информации в конкретных условиях функционирования объекта защиты и составления адекватной модели угроз ИСПД.

4. **Модель нарушителя**

1. Оценка возможностей вероятных нарушителей безопасности информации должно основываться на предположении о типах и видах нарушителей, которые могут реализовать угрозы безопасности информации в ИСПД с заданной структурой и функциональными характеристиками. При этом необходимо провести оценку потенциала этих нарушителей и возможных способов реализации угроз безопасности информации.

2. Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью модели угроз безопасности информации и должна отражать:

- типы, виды и потенциал нарушителя, которые могут обеспечить реализацию угрозы безопасности информации;
- цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации;
- возможные способы реализации угроз безопасности информации.

3. Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам информационной системы, а также анализа возможностей нарушителей по доступу к компонентам информационной системы исходя из структуры построения, функциональных характеристик и особенностей функционирования информационной системы.
4. В зависимости от имеющихся прав доступа, нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) к содержащейся в них информации или не иметь такого доступа.
5. Анализ прав доступа проводится, как минимум, в отношении следующих компонентов информационной системы:

- устройств ввода/вывода (отображения) информации;
- беспроводных устройств;
- программных, программно-технических и технических средств обработки информации;
- съемных машинных носителей информации;
- машинных носителей информации, выведенных из эксплуатации;
- активного (коммутационного) и пассивного оборудования каналов связи;
- каналов связи, выходящих за пределы контролируемой территории.

6. Основные виды нарушителей и возможных целей (мотивации) реализации угроз безопасности информации приведены в таблице 1.

Таблица 1

Вид нарушителя		**Тип нарушителя**	**Мотивация нарушителя**
1	Специальные службы иностранных государств	внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций

2	Террористические, экстремистские группировки	внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты (физические лица)	внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия

7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и других видов работ	внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
8	Лица, обеспечивающие функционирование информационных систем или обслуживание инфраструктуры оператора (охранники, уборщики и т.д.)	внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
9	Пользователи информационной системы	внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.
10	Администраторы информационной системы и администраторы безопасности	внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Бывшие работники (пользователи)	внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия.

При оценке возможностей нарушителей необходимо исходить из условий, что для повышения

своих возможностей нарушители 1 вида могут вступать в сговор с нарушителями 3, 4, 6, 7, 8, 9 и 10 видов. Нарушители 2 вида могут вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. Нарушители 3 вида могут вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. В случае принятия таких предположений цели (мотивация) и возможности нарушителей подлежат объединению.

7. Возможности реализации угрозы безопасности информации определяются потенциалом нарушителя по каждому виду нарушителя. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угрозы безопасности в ИСПД.
8. Различают нарушителей обладающих:

- базовым (низким) потенциалом нападения;
- базовым повышенным (средним) потенциалом нападения;
- высоким потенциалом нападения.

Вероятные возможности различных видов нарушителей в зависимости от потенциала приведены в таблице 2.

Таблица 2

№	**Потенциал нарушителей**	**Виды нарушителей**	**Возможности по реализации угроз безопасности информации**
1	Нарушители с **базовым** (низким) потенциалом	Внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонентов информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак и реализацию атак на информационную систему

2	Нарушители с **базовым повышенным** (средним) потенциалом	Террористические и экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных продуктов, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонентов информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонентов общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

3	Нарушители с **высоким** потенциалом	Специальные службы иностранных государств	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

5. **ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ**

1. В соответствии с пунктом 3.11. актуальность угрозы безопасности информации $\mathbf{УгБИ}_j^A$ характеризуется двумя компонентами, первый из которых характеризует вероятность реализации угрозы $\mathbf{P}_j$, а второй – степень возможного ущерба $\mathbf{X}_j$ в случае реализации

угрозы**.**

Вероятность $\mathbf{P_j}$ определятся на основе анализа статистических данных о частоте реализации угроз безопасности информации (возникновении инцидентов безопасности) в ИСПД и (или) однотипных информационных системах.

Ущерб $\mathbf{X_j}$ определяется на основе оценок степени последствий от нарушения конфиденциальности, целостности или доступности информации.

2. При отсутствии статистических данных о реализации угроз безопасности информации (возникновении инцидентов безопасности) в ИСПД и (или) однотипных информационных системах, актуальность угрозы безопасности информации определяется оценкой возможности реализации угрозы (далее Y_j).

$УгБИ_{jA}$ = [(Y_j); (X_j)])], где:

- Y_j определятся на основе оценки уровня безопасности информационной системы и потенциала нарушителя, требуемого для реализации угрозы безопасности;
- Xj также определяется на основе оценок степени последствий от нарушения конфиденциальности, целостности или доступности информации.

3. Актуальность угроз безопасности информации определяется в отношении угроз, для которых экспертным методом определено, что:

- возможности (потенциал) нарушителя достаточны для реализации угрозы безопасности информации;
- в информационной системе могут иметься потенциальные уязвимости, которые могут быть использованы при реализации j-ой угрозы безопасности информации;
- структурно-функциональные характеристики и особенности функционирования информационной системы не исключают возможности применения способов, необходимых для реализации j-ой угрозы безопасности информации (существует сценарий реализации угрозы безопасности);
- реализация угрозы безопасности информации приведет к нарушению конфиденциальности, целостности или доступности информации, в результате которого возможно возникновение неприемлемых негативных последствий (ущерба).

6. **Оценка вероятности (возможности) реализации угрозы безопасности**

1. Под вероятностью реализации угрозы безопасности информации понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация j-ой угрозы безопасности информации в ИСПД. Вводятся три градации:

- **низкая вероятность**, при которой отсутствуют объективные предпосылки к реализации угрозы безопасности информации. Статистика по фактам реализации данной угрозы и мотивации к её реализации не превышает одного раза в пять лет;
- **средняя вероятность** – существуют предпосылки к реализации угрозы безопасности информации, зафиксированы случаи реализации угрозы безопасности информации или имеется иная информация, указывающая на возможность реализации угрозы безопасности информации, существуют признаки наличия у нарушителя мотивации для реализации такой угрозы. Возможная частота реализации угрозы не превышает одного раза в год;
- **высокая вероятность** – существуют объективные предпосылки к реализации угрозы

безопасности информации. Существует достоверная статистика реализации угрозы безопасности информации (возникновения инцидентов безопасности), имеется иная информация, указывающая на высокую возможность реализации угрозы безопасности информации, у нарушителя имеются мотивы для реализации угрозы. Возможная частота реализации угрозы – чаще чем один раз в год.

2. В случае отсутствия данных для оценки вероятности реализации угрозы или наличия сомнений в объективности экспертных оценок вероятности реализации угроз при определении градаций, актуальность j-ой угрозы безопасности информации определяется на основе оценки возможности ее реализации **(Y_j).** Возможность реализации j-ой угрозы безопасности информации **(Y_j)** оценивается исходя из уровня безопасности информационной системы **(Y1)** и потенциала нарушителя **(Y2)**, необходимого для реализации этой угрозы безопасности информации в ИСПД:

$$(Y_j) = [(Y1); (Y2)]$$

При определении угроз безопасности информации на этапе создания информационной системы в случае, когда меры защиты информации не реализованы или не проведена оценка их достаточности и эффективности, оценка возможности реализации j-ой угрозы безопасности информации **$(Y_j)^p$** проводится относительно уровня проектной защищенности информационной системы **($Y_{1п}$)**:

$$(Y_j)^p = [(Y_{1п}); (Y2)]$$

Под уровнем проектной безопасности **($Y_{1п}$)** понимается исходная безопасность информационной системы, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования. **($Y_{1п}$)** определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице 3.

Таблица 3

№ п/п	**Структурно-функциональные характеристики информационной системы, условия ее эксплуатации**	**Уровень проектной безопасности информационной системы ($Y_{1п}$)**		
		Высокий	**С**редний	**Н**изкий
1	По структуре информационной системы:			
	автономное автоматизированное рабочее место	+		
	локальная информационная система		+	
	распределенная информационная система			+

2	По используемым информационным технологиям:			
	системы на основе виртуализации			+
	системы, реализующие «облачные вычисления»			+
	системы с мобильными устройствами			+
	системы с технологиями беспроводного доступа			+
	грид-системы			+
	суперкомпьютерные системы		+	
3	По архитектуре информационной системы:			
	системы на основе «тонкого клиента»	+		
	системы на основе одно ранговой сети;		+	
	файл-серверные системы			+
	центры обработки данных			+
	системы с удаленным доступом пользователей			+
	использование разных типов операционных систем (гетерогенность среды)		+	
	использование прикладных программ, независимых от операционных систем		+	
	использование выделенных каналов связи		+	
4	По наличию (отсутствию) взаимосвязей с иными информационными системами:			
	взаимодействующая с системами			+
	не взаимодействующая с системами		+	
5	По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования:			
	подключенная			+
	подключенная через выделенную инфраструктуру		+	
	не подключенная	+		
6	По размещению технических средств:			
	в пределах одной контролируемой зоны	+		
	в пределах нескольких контролируемых зон		+	
	вне контролируемой зоны			+
7	По режимам обработки информации в информационной системе:			
	многопользовательский			+
	однопользовательский	+		
8	По режимам разграничения прав доступа:			
	без разграничения			+
	с разграничением		+	

9	По режимам разделения функций управления информационной системой:			
	без разделения			+
	выделение рабочих мест для администрирования в отдельный домен		+	
	использование различных сетевых адресов		+	
	использование выделенных каналов для администрирования		+	
10	По подходам к сегментированию информационной системы:			
	без сегментирования			+
	с сегментированием		+	

3. В ходе создания информационной системы, уровень ее проектной безопасности $\mathbf{Y_{1п}}$ определяется следующим образом:

а) информационная система имеет высокий уровень проектной безопасности, если не менее 80% характеристик информационной системы соответствуют уровню «высокий», а остальные - среднему уровню безопасности;

б) информационная система имеет средний уровень проектной безопасности, если не выполняются условия по пункту а) и не менее 90% характеристик информационной системы соответствуют уровню не ниже «среднего» (берется отношение суммы положительных решений по столбцу «средний» к общему количеству решений), а остальные - низкому уровню безопасности;

в) информационная система имеет низкий уровень проектной безопасности, если не выполняются условия по пунктам а) и б).

4. В ходе эксплуатации информационной системы уровень ее безопасности (Y1) определяется следующим образом:

а) в информационной системе обеспечивается **высокий** уровень безопасности, если в ходе эксплуатации информационной системы не появились дополнительные угрозы безопасности информации или в отношении появившихся дополнительных угроз безопасности информации оперативно могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

б) в информационной системе обеспечивается **средний** уровень безопасности, если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

в) в информационной системе обеспечивается **низкий** уровень безопасности, если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них не могут быть приняты меры защиты информации, нейтрализующие эти угрозы.

5. Значение потенциала нарушителя (Y2) для j-ой угрозы безопасности информации определяется на основе общедоступных банков данных угроз безопасности информации или типовых моделях угроз безопасности информации для информационных систем различных классов и типов. В случае отсутствия информации о потенциале нарушителя для реализации j-ой угрозы безопасности значение потенциала (Y2) определяется в соответствии с Приложением 3.

6. Возможность реализации j-ой угрозы безопасности информации $(Y_j)^{н/с/в}$ в зависимости от уровня безопасности информационной системы (Y1) или ($Y_{1п}$) и потенциала нарушителя (Y2) оценивается как **высокая** $(Y_j)^{в}$**, средняя** $(Y_j)^{с}$ или **низкая** $(Y_j)^{н}$ в соответствии с таблицей 4.

Таблица 4

Вероятность (возможность) реализации угрозы безопасности информации(Y_j)

Потенциал нарушителя (Y2)	**Уровень безопасности (Y1);($Y_{1п}$)**		
	Высокий	**Средний**	**Низкий**
Низкий (базовый)	низкая	средняя	высокая
Средний (базовый повышенный)	средняя	высокая	высокая
Высокий	высокая	высокая	высокая

7. **Оценка степени возможного ущерба от реализации угрозы безопасности**

1. Для оценки степени возможного ущерба от реализации угрозы безопасности информации определяются:

- возможный результат реализации угрозы безопасности информации в информационной системе;
- вид ущерба, к которому может привести реализация угрозы безопасности информации;
- степень последствий от реализации угрозы безопасности информации для каждого вида ущерба.

2. Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности в соответствии с Таблицей 5.

Таблица 5

Свойство безопасности информации	**Результат реализации угрозы безопасности информации**	
	не оказывает воздействия	**оказывает воздействие**

Конфиденциальность	В результате реализации угрозы безопасности информации отсутствует возможность неправомерного доступа, копирования, предоставления или распространения информации	В результате реализации угрозы безопасности информации возможны неправомерный доступ, копирование, предоставление или распространение информации
Целостность	В результате реализации угрозы безопасности информации отсутствует возможность уничтожения или модифицирования информации	В результате реализации угрозы безопасности информации возможно уничтожение или модифицирование информации
Доступность	В результате реализации угрозы безопасности информации отсутствует возможность блокирования информации	В результате реализации угрозы безопасности информации возможно блокирование информации

3. При определении степени возможного ущерба необходимо исходить из того, что в зависимости от целей и задач, решаемых информационной системой, видов обрабатываемой информации, воздействие на конфиденциальность, целостность или доступность каждого вида информации, содержащейся в ИСПД, может привести к различным видам ущерба. При этом для разных обладателей информации и операторов будут характерны разные виды ущерба.

Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации, приведены в Таблице 6.

Указанные в Таблице 6 виды ущерба могут дополняться другими видами в зависимости от целей и задач, решаемых информационной системой, а также вида обрабатываемой в ней информации

Таблица 6

Вид ущерба	**Возможные негативнее последствия от нарушения конфиденциальности, целостности, доступности информации**
Экономический (финансовый)	Снижение, как минимум, одного экономического показателя. Потеря (кража) финансовых средств. Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Дополнительные или незапланированные затраты на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Дополнительные или незапланированные затраты на восстановление деятельности. Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Потеря договоров, соглашений. Другие прямые или косвенные финансовые потери.

Социальный	Создание предпосылок для нанесения вреда здоровью граждан. Возможность нарушения функционирования для объектов обеспечения жизнедеятельности граждан. Организация пикетов, забастовок, митингов и других акций. Увольнения. Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. Появление негативных публикаций в общедоступных источниках. Невозможность (прерывание) предоставления социальных услуг. Другие последствия, приводящие к нарастанию социальной напряженности в обществе
Политический	Создание предпосылок к обострению отношений в международных отношениях. Срыв двусторонних (многосторонних) контактов с зарубежными партнерами. Неспособность выполнения международных (двусторонних) договорных обязательств. Невозможность заключения международных (двусторонних) договоров, соглашений. Создание предпосылок к внутриполитическому кризису. Нарушение выборного процесса. Другие последствия во внутриполитической и внешнеполитической деятельности
Репутационный	Нарушение законодательных и подзаконных актов. Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Неспособность выполнения договорных обязательств. Другие последствия, приводящие к нарушению репутации
Ущерб в области обороны, безопасности и правопорядка	Создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка. Нарушение общественного правопорядка. Неблагоприятное влияние на обеспечение общественного правопорядка. Возможность потери или снижения уровня контроля общественного правопорядка. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Другие последствия, приводящие к ущербу в области обороны, безопасности и правопорядка.
Ущерб субъекту персональных данных	Создание угрозы личной безопасности. Финансовые или иные материальные потери физического лица. Вторжение в частную жизнь. Создание угрозы здоровью. Моральный вред. Утрата репутации. Другие последствия, приводящие к нарушению прав субъекта персональных данных.

Технологический	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сегмента информационной системы. Другие последствия, приводящие к нарушению технологии обработки информации.

4. Степень негативных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации определяется для каждого вида ущерба, зависит от целей и задач, решаемых ИСПД, и может иметь разные значения для разных держателей и операторов. В качестве шкалы измерения степени негативных последствий принимаются значения: **«критический», «значительный»**, **«неначительный» и «отсутствует»**.

Степень возможного ущерба определяется экспертным методом в соответствии с Таблицей 7.

Таблица 7

Степень ущерба	**Характеристика степени ущерба**
Критический	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор не могут выполнять возложенные на них функции
Значительный	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор не могут выполнять хотя бы одну из возложенных на них функций
Незначительный	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств
Отсутствует (не может быть причинен)	Нарушение одного из свойств безопасности информации (конфиденциальности, целостности, доступности) не приводит к убыткам. Информационная система и (или) оператор могут выполнять возложенные на них функции с незначительным понижением эффективности.

8. **Определение актуальности угрозы безопасности информации**

1. Решение об актуальности угрозы безопасности информации **УгБИ**$_j^A$ для ИСПД с

заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с Таблицей 8, где: буква **Н** обозначает неактуальность угроз, и соответственно буква **А** обозначает актуальность угрозы.

Таблица 8

Вероятность (возможность) реализации угрозы (Y_i)	**Степень возможного ущерба**			
	Отсутствует	**Незначи-тельный**	**Значитель-ный**	**Критический**
Низкая	Н	Н	Н	А
Средняя	Н	Н	А	А
Высокая	А	А	А	А

9. **Состав мер по обеспечению безопасности персональных данных**

1. В состав мер по обеспечению безопасности персональных данных, реализуемых системой защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

а) идентификация и аутентификация субъектов доступа и объектов доступа;

б) управление доступом субъектов доступа к объектам доступа;

в) ограничение программной среды;

г) защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

д) регистрация событий безопасности;

е) антивирусная защита;

ж) обнаружение (предотвращение) вторжений;

з) контроль (анализ) защищенности персональных данных;

к) обеспечение целостности информационной системы и персональных данных;

л) обеспечение доступности персональных данных;

м) защита среды виртуализации;

н) защита технических средств;

о) защита информационной системы, ее средств, систем связи и передачи данных;

п) выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

р) управление конфигурацией информационной системы и системы защиты персональных данных.

2. Содержание указанных в пункте 9.1 мер по обеспечению безопасности персональных данных приведены в Приложении 5.

10. **Порядок действий по выбору мер защиты**

1. Выбор мер защиты информации для каждого объекта защиты производится в следующей последовательности:

а) определение базового набора мер защиты информации для установленного уровня защищенности ИСПД;

б) адаптация базового набора мер защиты информации к существующим структурным и функциональным характеристикам информационной системы;

в) уточнение адаптированного базового набора мер защиты информации с учетом недостающих мер защиты информации для нейтрализации угроз безопасности информации, включенных в модель угроз безопасности объекта;

г) дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

2. Определение базового набора мер защиты персональных данных
    1. Базовый набор мер защиты для ИСПД приведен в Приложении 4.
    2. Первоначально выбирается один из четырех базовых наборов мер защиты информации, соответствующих установленному уровню защищенности ИСПД. Меры, обозначенные в таблице знаком «+», включаются в базовый набор мер защиты информации. Меры защиты информации, не обозначенные знаком «+», могут быть применены при последующих действиях выбора мер защиты (по адаптации, уточнению, дополнению мер защиты или разработке компенсирующих мер защиты информации).
    3. Выбранный базовый набор мер защиты информации в дальнейшем подлежит обязательной адаптации (привязке) с учетом структурно-функциональных характеристик и особенностей функционирования ИСПД.

3. Адаптация базового набора мер защиты информации
    1. С целью максимальной привязки выбранных мер защиты к существующей структуре с учетом особенностей эксплуатации ИСПД необходимо внести требуемые изменения в первоначально выбранный базовый набор мер защиты информации.
    2. При адаптации, как правило, исключаются меры, не используемые в данной информационной системе или обусловленные её структурно-функциональными различиями. Например, в случае если в ИСПД не применяется технология виртуализации, из базовых мер исключаются меры среды виртуализации, или если мобильные устройства не применяются, то исключаются меры по защите мобильных средств.

4. Уточнение адаптированного набора мер защиты информации
    1. Исходными данными для уточнения адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их такие характеристики как потенциал, оснащенность и мотивация нарушителя, включенные в модель угроз безопасности.
    2. При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации сопоставляется мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая нейтрализацию этой угрозы безопасности или снижающая вероятность ее реализации, исходя из условий функционирования информационной системы.
    3. В случае если адаптированный базовый набор мер защиты информации не обеспечивает нейтрализацию всех угроз безопасности информации, в него дополнительно включаются другие меры защиты информации. Содержание дополнительных мер определяется с учетом уровня защищенности ИСПД и потенциала нарушителя.

5. Дополнение уточненного адаптированного набора мер защиты информации
    1. Дополнение уточненного адаптированного базового набора мер защиты информации может потребоваться при необходимости учета требований других нормативных документов по защите информации.

6. Применение компенсирующих мер защиты информации
    1. Сформированный набор мер защиты информации может содержать меры защиты, которые по каким-либо причинам в данный момент в конкретной информационной системе нереализуемы (высокая стоимость, неприемлемо большие сроки реализации, отсутствие компетенции для эксплуатации и пр.). В таких случаях необходимо заменить соответствующие меры защиты информации на компенсирующие меры защиты информации. Выбор компенсирующих мер защиты информации должен быть аргументирован и подтвержден документально.

11. **Содержание мер защиты персональных данных**

1. Подробное описание базовых мер по обеспечению безопасности персональных данных, в ИСПД с изложением требований по реализации меры, а также требований по их усилению при необходимости, приведены в Приложении 5.
2. Обозначенные в таблице Приложения 4 меры знаком «+» обязательны для включения в базовый набор мер защиты информации. Меры, не обозначенные знаком «+», могут быть включены при последующих действиях при адаптации, уточнении, дополнения мер защиты или при разработке компенсирующих мер защиты информации.

Обозначения, приведенные ниже знака «+» в виде цифр и букв обозначают пункт и подпункт усиления меры, указанные в разделе «требования по усилению» данной меры (Приложение 5).

Приложение 1

Рекомендации по экспертной оценке определения угроз безопасности информации

1. **Общие положения**

1. Формирование экспертной группы способствует снижению субъективных факторов при оценке угроз безопасности информации. Занижение (ослабление) экспертами прогнозов может повлечь наступление непрогнозируемого (неожиданного) ущерба в результате реализации угрозы безопасности информации. Завышение экспертами прогнозов может повлечь за собой неоправданные расходы на нейтрализацию угроз, являющихся неактуальными.
2. Независимо от результата формирования экспертной группы при оценке угроз безопасности информации существуют субъективные факторы, связанные с психологией принятия решений человеком, что также может приводить как к занижению, так и к завышению экспертами прогнозов при определении угроз безопасности информации.
3. Любое решение, принимаемое экспертами при определении угроз безопасности информации, должно исходить из правил, при которых нарушитель находится в наилучших условиях для реализации угрозы безопасности (принцип «гарантированности»).

2. **Формирование экспертной группы**

1. В состав экспертной группы для определения угроз безопасности информации рекомендуется включать экспертов:

- от подразделений держателя ИСПДН;
- от подразделений оператора информационной системы;
- от подразделения по защите информации;
- от лиц, предоставляющих услуги по обработке информации;
- от разработчика информационной системы;
- от операторов внешних (взаимодействующих) информационных систем (по согласованию).

2. В качестве экспертов необходимо привлекать специалистов, деятельность которых связана с обработкой информации в ИСПД или имеющих опыт работы в области применения информационных технологий или в области защиты информации.
3. В качестве экспертов рекомендуется привлекать лиц с высшим образованием или прошедших переподготовку (повышение квалификации) по информационной безопасности, или имеющих стаж практической работы в своей сфере деятельности не менее двух лет.
4. Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не допускается формирование экспертной группы из членов, находящихся в прямом подчинении.
5. Состав экспертной группы зависит от поставленных целей и задач, но не должен быть меньше трех экспертов.

3. **Проведение экспертной оценки**

1. При проведении экспертной оценки принимаются меры, направленные на снижение уровня субъективности и неопределенности при определении каждой из угроз безопасности информации.
2. Экспертную оценку рекомендуется проводить в отношении, как минимум, следующих параметров:

- цели реализации угроз безопасности информации (мотивация нарушителей);
- типы и виды нарушителей;
- уязвимости, которые могут быть использованы для реализации угроз безопасности информации;
- способы реализации угроз безопасности информации;
- степень воздействия угрозы безопасности информации на каждое из свойств безопасности информации;
- последствия от реализации угроз безопасности информации;
- вероятность реализации угроз безопасности информации;
- уровень безопасности информационной системы;
- потенциал нарушителя, требуемый для реализации угрозы безопасности информации (в случае отсутствия потенциала в банке данных угроз безопасности информации).

3. Оценка параметров проводится опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы).
4. Вопросы анкеты должны быть четко сформулированы и однозначно трактуемы, предполагающие однозначные ответы.
5. Опрос экспертов включает следующие этапы:

- каждый эксперт проводит оценку параметра, результаты которой заносятся в таблицу опроса (рекомендуется проводить не менее двух раундов оценки);
- определяется среднее значение оцениваемого параметра в каждом раунде;
- определяется итоговое среднее значение оцениваемого параметра.

Таблица опроса

ЭКСПЕРТЫ	**Оценка параметра (1 раунд)**	**Оценка параметра (2 раунд)**
1	Значение оценки	Значение оценки
2	Значение оценки	Значение оценки
3	Значение оценки	Значение оценки
……	Значение оценки	Значение оценки
	Среднее значение 1	**Среднее значение 2**
Итоговое среднее значение оцениваемого параметра		

Приложение 2

Структура модели угроз безопасности информации

1. Общие положения

Раздел содержит:

- назначение и область действия документа;
- полное наименование ИСПД;
- используемые для разработки модели угроз безопасности информации нормативные и методические документы, стандарты;
- информация об источниках, на основе которых определяются угрозы безопасности (документация, исходные тексты программ, опросы персонала, журналы регистрации средств защиты, отчеты об аудите и другие источники).

2. Описание информационной системы и особенностей ее функционирования

Раздел содержит:

- общую характеристику информационной системы;
- описание структурно-функциональных характеристик информационной системы;
- описание взаимосвязей между сегментами информационной системы;
- описание взаимосвязей с другими информационными системами и информационно-телекоммуникационными сетями;
- описание технологии обработки информации;
- отличительные особенности функционирования (отсутствие неучтенных беспроводных каналов доступа, выделение адресов, другие особенности).

3. Возможности нарушителей (модель нарушителя)

Раздел содержит:

- описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в информационной системе;
- возможные способы реализации угроз безопасности информации;
- приводятся предположения, касающиеся нарушителей (например, отсутствие у нарушителя возможности доступа, оборудования, сделанного на заказ и применяемого при реализации угрозы, наличие сговора между внешними и внутренними нарушителями или др.);
- в раздел включаются любые ограничения, касающиеся определения нарушителей (исключение администраторов из числа потенциальных нарушителей и прочие

предположения).

4. **Актуальные угрозы безопасности информации**

Раздел содержит:

- описание актуальных угроз безопасности, включающее наименование угрозы безопасности информации;
- возможности нарушителя по реализации угрозы;
- используемые уязвимости информационной системы;
- описание способов реализации угрозы;
- объекты воздействия;
- возможные результат и последствия от реализации угрозы безопасности информации.

Приложение 3

Определение потенциала нарушителя по реализации угрозы безопасности информации в информационной системе

1. Настоящая оценка потенциала нарушителя направлена на снижение уровня субъективности и неопределенности при оценке потенциала нарушителя.
2. Исходными данными для определения потенциала нарушителя являются:

- данные об аппаратном, общесистемном и прикладном программном обеспечении, применяемых информационных технологиях, особенностях функционирования информационной системы;
- данные об уязвимостях в аппаратном, общесистемном и прикладном программном обеспечении, опубликованные в различных базах данных уязвимостей, полученные в результате исследований (тестировании) или полученные от уполномоченных органов исполнительной власти или организаций.

3. При оценке потенциала нарушителя необходимо исходить из того, что для успешного достижения целей реализации угроз безопасности информации, нарушителю необходимо

осуществить подготовку к реализации угрозы и непосредственную ее реализацию. При этом одним из необходимых условий на этапе подготовки к реализации угрозы безопасности информации является выявление уязвимостей информационной системы, а на этапе реализации угрозы безопасности информации – использование уязвимостей информационной системы.

4. Для определения потенциала нарушителя необходимо оценить возможности нарушителя в идентификации уязвимостей и их использования.
5. Делается обоснованное предположение о наличии уязвимостей, которые потенциально содержатся в информационной системе и могут быть использованы для реализации угрозы безопасности информации.
6. В качестве исходных данных для определения потенциальных уязвимостей используются сведения о составе информационной системы, особенностям ее функционирования, а также данные об уязвимостях в программном обеспечении, опубликованные в общедоступных источниках, полученные в результате исследований, полученные от других организаций.
7. Для каждой потенциальной уязвимости проводится оценка возможностей ее идентификации и использования в информационной системе нарушителем, обладающим определенными возможностями для каждого из возможных сценариев реализации угрозы.
8. Оценка возможностей нарушителя по идентификации и использованию уязвимости в информационной системе проводится по результатам определения следующих показателей:

- время, затрачиваемое нарушителем на идентификацию и использование уязвимости (затрачиваемое время);
- компетентность нарушителя;
- осведомленность нарушителя об информационной системе;
- оснащенность нарушителя;
- возможности нарушителя по доступу к информационной системе.

Во многих случаях указанные показатели являются зависимыми и могут в различной степени заменять друг друга. В частности, показатели компетентности или оснащенности могут заменяться показателем затрачиваемого времени.

9. Показатель «затрачиваемое время» - это время затрачиваемое нарушителем для идентификации и использования уязвимости для реализации угрозы безопасности информации, который характеризуется как: «за минуты», «за часы», «за дни» или «за месяцы».

Значение «за минуты» присваивается, если для реализации угрозы нарушитель затратит менее получаса на идентификацию и использование уязвимости.

Значение «за часы» присваивается, если для реализации угрозы нарушитель затратит менее чем один день на идентификацию и использование уязвимости.

Значение «за дни» присваивается, если для реализации угрозы нарушитель затратит менее чем один месяц на идентификацию и использование уязвимости.

Значение «за месяцы» присваивается, если для реализации угрозы нарушитель затратит, как минимум, месяц на идентификацию и использование уязвимости.

10. Показатель «компетентность нарушителя» характеризует, каким уровнем знаний и подготовкой в области информационных технологий и защиты информации должен обладать нарушитель, чтобы идентифицировать и использовать уязвимости для реализации угрозы безопасности информации.

Показатель «компетентность нарушителя» определяется как: «специалист», «профессионал» или

«непрофессионал»**.**

Значение **«профессионал»** присваивается, если нарушитель имеет хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе, а также обладает специальными знаниями о методах и средствах выявления новых уязвимостей и способах реализации угроз безопасности информации для информационных систем данного типа.

Значение **«специалист»** присваивается, если нарушитель имеет осведомленность о мерах защиты информации, применяемых в информационной системе данного типа.

Значение **«непрофессионал»** присваивается, если нарушитель имеет слабую осведомленность (по сравнению со специалистами или профессионалами) о мерах защиты информации, применяемых в информационных системах данного типа, и не обладает специальными знаниями по реализации угроз безопасности информации.

11. Показатель «осведомленность нарушителя» характеризует, какие сведения об информационной системе и условиях ее эксплуатации доступны нарушителю, чтобы идентифицировать и использовать уязвимости для реализации угрозы безопасности информации.

Показатель «осведомленность нарушителя» может принимать значения «отсутствие знаний», «ограниченные знания» или «знание чувствительной информации».

Значение **«отсутствие знаний»** присваивается, если в результате принятия мер по защите информации нарушителю не может стать известно о структурно-функциональных характеристиках информационной системы, системе защиты информации информационной системы, а также об иной информации по разработке (проектированию) и эксплуатации информационной системы, включая сведения из конструкторской, проектной и эксплуатационной документации. При этом может быть доступна информация о целях и задачах, решаемых информационной системой. Данный показатель также присваивается, если сведения об информационной системе отнесены к информации ограниченного доступа и не могут быть доступны широкому кругу лиц.

Значение **«ограниченные знания»** присваивается, если нарушителю наряду с информацией о целях и задачах, решаемых информационной системой, может стать известна только эксплуатационная документация на информационную систему (в частности руководство пользователя и (или) правила эксплуатации информационной системы).

Значение **«знание чувствительной информации»** присваивается, если нарушителю может стать известны конструкторская (проектная) и эксплуатационная документация на информационную систему, информация о структурно-функциональных характеристиках информационной системы, системе защиты информационной системы.

12. Показатель «возможности нарушителя по доступу к информационной системе» характеризует, как долго по времени нарушитель должен иметь возможность доступа к информационной системе для идентификации и использования уязвимостей для реализации угроз безопасности информации.

Показатель «возможности нарушителя по доступу к информационной системе» может принимать значения **«за минуты», «за часы», «за дни» или «за месяцы»,** аналогично как в пункте 9. Показатель «возможности нарушителя по доступу к информационной системе» взаимосвязан с показателем «затраченное время».

13. Показатель «оснащенность нарушителя» характеризует, какие программные и (или) программно-технические средства требуются нарушителю для идентификации и

использования уязвимостей для реализации угроз безопасности информации.

Показатель «оснащенность нарушителя» характеризуется значениями:

- «стандартное оборудование»;
- «специализированное оборудование»;
- «оборудование, сделанное на заказ».

Значение **«стандартное оборудование»** присваивается, если для идентификации или использования уязвимостей при реализации угрозы требуются программные (программно-технические) средства легкодоступные для нарушителя. К таким средствам, в первую очередь, относятся программные средства непосредственно информационной системы (отладчик в операционной системе, средства разработки и иные); программные средства, которые могут быть легко получены или имеются простые сценарии реализации угроз.

Значение **«специализированное оборудование»** присваивается, если для идентификации или использования уязвимостей при реализации угрозы требуются программные (программно-технические) средства, которые отсутствуют в свободном доступе, но могут быть приобретены нарушителем без значительных усилий. К таким средствам, в первую очередь, относятся программные (программно-технические) средства, которые имеются в продаже (анализаторы кода, анализаторы протоколов и иные) или требуется разработка более сложных программ и сценариев реализации угрозы. Оборудование может быть закуплено, либо могут быть использованы компьютеры, объединенные через сети (бот-сети).

Значение **«оборудование, сделанное на заказ»** присваивается, если для идентификации или использования уязвимостей при реализации угрозы требуются программные (программно-технические) средства, которые недоступны широкому кругу лиц, и требуется их специальная разработка с привлечением исследовательских организаций, или доступ к этим средствам регулируется законодательством. К такому оборудованию также относятся средства, сведения о которых относятся к информации ограниченного доступа.

14. Для вычисления потенциала нарушителя определяются числовые значения указанных показателей в соответствии с таблицей П3.1.

Таблица П3.1.

Показатель возможностей нарушителя		**Значения при идентификации уязвимости**	**Значения при использовании уязвимости**
Затрачиваемое время	< 0,5 час	0	0
	< 1 день	2	3
	< 1 месяц	3	5
	> 1 месяц	5	8

Компетентность нарушителя	не профессионал	0	0
	специалист	2	3
	профессионал	5	4
Осведомленность нарушителя	отсутствие знаний	0	0
	ограниченные знания	2	2
	знание чувствительной информации	5	4
Возможность доступа к информационной системе	<0,5 час или не обнаруживаемый доступ	0	0
	<1 день	2	4
	<1 месяц	3	6
	> 1 месяц	4	9
	невозможно		
Оснащенность нарушителя	отсутствует	0	0
	стандартное оборудование	1	2
	специализированное оборудование	3	4
	оборудование, сделанное на заказ	5	6

15. Для конкретной потенциальной уязвимости может возникнуть необходимость определять показатели несколько раз для различных способов реализации угроз безопасности информации (попеременно использовать разные значения показателей компетентности в сочетании со значениями времени и оборудования). При этом следует выбирать наибольшее значение, полученное при каждом расчете показателей.
16. Полученные на основе таблицы П3.1 значения характеристик потенциала нарушителя суммируются. Полученная сумма значений характеристик сравнивается с диапазонами значений, приведенных в таблице П3.2, в соответствии с которой определяется потенциал нарушителя.

Таблица П3.2

Диапазон значений	**Потенциал нарушителя**
<10	Потенциал недостаточен для реализации угрозы безопасности
10-17	Базовый (низкий)
18-24	Базовый повышенный (средний)
>24	Высокий

Приложение 4

СОСТАВ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Мера	**Содержание меры**	**Уровни защищенности**			
		Синий	**зеленый**	**желтый**	**красный**
1. **Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)**					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+ 1а, 2а, 3	+ 1а, 2а, 3, 4
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+ 1а, 2а	+ 1а, 2а	+ 1б, 2б
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	+ 1а	+ 1б	+ 1в	+ 1г
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
2. **Управление доступом субъектов доступа к объектам доступа (УПД)**					

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+ 1, 2	+ 1, 2, 3а	+ 1, 2, 3б
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+ 1, 2, 3	+ 1, 2, 3	+ 1, 2, 3, 4
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+ 1
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+ 1
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+ 1
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				

УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				+ 1а, 3
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+ 1а, 2	+ 1б, 2
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+ 2, 3	+ 2, 3, 5	+ 1, 2, 3, 5
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+ 1	+ 1, 3	+ 1, 3, 4, 5
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+ 1, 2	+ 1, 2
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+ 1а	+ 1а, 1б	+ 1а, 1б	+ 1а, 1б
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+ 1	+ 2
3. **Ограничение программной среды (ОПС)**					

ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				+ 1, 2, 3
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+ 1
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
4. **Защита машинных носителей персональных данных (ЗНИ)**					
ЗНИ.1	Учет машинных носителей персональных данных			+ 1 а	+ 1а, 1б
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				

ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных			+	+ 1
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей 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		+ 1,5б	+ 1, 5в	+ 1, 2, 3, 5г
5. **Регистрация событий безопасности (РСБ)**					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+ 1,3, 4а	+ 1, 2, 3, 4б
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+ 1а	+ 1а
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+ 1	+ 1
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			+	+ 1, 2
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+ 1
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				

РСБ.7	Защита информации о событиях безопасности	+	+	+ 1	+ 1
6. **Антивирусная защита (АВЗ)**					
АВЗ.1	Реализация антивирусной защиты	+	+	+ 1, 2	+ 1, 2
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+ 1	+ 1
7. **Обнаружение вторжений (СОВ)**					
СОВ.1	Обнаружение вторжений			+ 2	+ 2
СОВ.2	Обновление базы решающих правил			+	+ 1, 2, 3
8. **Контроль (анализ) защищенности персональных данных (АНЗ)**					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+ 1,4	+ 1, 2,4	+ 1, 2,4,7
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		+	+ 1	+ 1
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+ 1	+ 1, 2
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+ 1	+ 1

9. **Обеспечение целостности информационной системы и персональных данных (ОЦЛ)**					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+ 1, 3	+ 1, 3
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций		+	+	+ 1
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
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 персональных данных и предупреждение пользователей об ошибочных действиях				
10. **Обеспечение доступности персональных данных (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 технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+ 1
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+ 1, 2	+ 1, 3
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+ 1
11. **Защита среды виртуализации (ЗСВ)**					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+ 1	+ 1
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+ 1, 2	+ 1, 2	+ 1, 2

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.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+ 1	+ 1, 2
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+ 3	+ 1, 3
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+ 1, 2, 3
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+ 1	+ 1
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+ 2
12. **Защита технических средств (ЗТС)**					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				

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, средствам защиты 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)				
13. **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 персональных данных, функций по обработке персональных данных и иных функций информационной системы				+ 3
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				

ЗИС.3	Обеспечение защиты персональных данных 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.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	+	+	+ 1	+ 1, 2
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного 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.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+ 1
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				

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 персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
14. **Выявление инцидентов и реагирование на них (ИНЦ)**					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+

15. **Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)**					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

Приложение 5

Содержание мер защиты персональных данных

1. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА (ИАФ)

ИАФ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА

Требования к реализации ИАФ.1

В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.

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.

К внутренним пользователям относятся должностные лица оператора (пользователи, администраторы), использующие программные и технические средства информационной системы в соответствии с должностными регламентами (инструкциями), утвержденными оператором, которым в информационной системе присвоены учетные записи, а также иные лица, которым в информационной системе присвоены учетные записи в соответствии с регламентом работ.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации - определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах по защите информации.

Требования к усилению ИАФ.1:

1) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования;

2) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования;

3) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);

4) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей);

5) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами привилегированных учетных записей (администраторов), где один из факторов обеспечивается аппаратным устройством аутентификации, отделенным от информационной системы, к которой осуществляется доступ;

6) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ;

7) в информационной системе должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;

8) в информационной системе для аутентификации пользователей должно обеспечиваться применение криптографических методов защиты информации, отвечающих требованиям законодательства Кыргызской Республики.

ИАФ.2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ УСТРОЙСТВ, В ТОМ ЧИСЛЕ СТАЦИОНАРНЫХ, МОБИЛЬНЫХ И ПОРТАТИВНЫХ.

Требования к реализации ИАФ.2

В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

Идентификация устройств в информационной системе обеспечивается по логическим именам,

логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Кыргызской Республики криптографических методов защиты информации.

Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ИАФ.2:

1) в информационной системе должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними:

а) взаимная аутентификация устройства и средства вычислительной техники (или другого взаимодействующего устройства);

б) аутентификация по уникальным встроенным средствам аутентификации.

ИАФ.3 УПРАВЛЕНИЕ ИДЕНТИФИКАТОРАМИ, В ТОМ ЧИСЛЕ СОЗДАНИЕ, ПРИСВОЕНИЕ, УНИЧТОЖЕНИЕ ИДЕНТИФИКАТОРОВ.

Требования к реализации ИАФ.3

Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:

- определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;
- блокирование идентификатора пользователя после установленного оператором времени неиспользования.

Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах оператора по защите информации.

Требование к усилению ИАФ.3:

1) оператором должно быть исключено повторное использование идентификатора пользователя в течение:

а) не менее одного года;

б) не менее трех лет;

в) в течение всего периода эксплуатации информационной системы;

2) оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования:

а) не более 90 дней;

б) не более 45 дней;

3) оператором должно быть обеспечено использование различной аутентификационной информации (различных средств аутентификации) пользователя для входа в информационную систему и доступа к прикладному (специальному) программному обеспечению;

4) оператором должно быть исключено использование идентификатора пользователя информационной системы при создании учетной записи пользователя публичной электронной почты или иных публичных сервисов;

5) оператором должно быть обеспечено управление идентификаторами внешних пользователей, учетные записи которых используются для доступа к общедоступным ресурсам информационной системы.

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.

Требования к реализации ИАФ.4

Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

- определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):

а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требование к усилению ИАФ.4:

1) в случае использования в информационной системе механизмов аутентификации на основе

пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

а) длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней;

б) длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;

в) длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней;

г) длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут, смена паролей не более чем через 60 дней;

2) в информационной системе должно быть обеспечено использование автоматизированных средств для формирования аутентификационной информации (генераторов паролей) с требуемыми характеристиками стойкости (силы) механизма аутентификации и для оценки характеристик этих механизмов;

3) в информационной системе должно быть обеспечено использование серверов и (или) программного обеспечения аутентификации для единой аутентификации в компонентах информационной системы и компонентах программного обеспечения, предусматривающего собственную аутентификацию;

4) оператор должен обеспечить получение (запросить) у поставщика технических средств и программного обеспечения информационной системы аутентификационную информацию, заданную производителем этих технических средств и программного обеспечения и не указанную в эксплуатационной документации;

5) оператором должны быть определены меры по исключению возможности использования пользователями их идентификаторов и паролей в других информационных системах.

ИАФ.5 ЗАЩИТА ОБРАТНОЙ СВЯЗИ ПРИ ВВОДЕ АУТЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

Требования к реализации ИАФ.5

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи "система - субъект доступа" в процессе аутентификации 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.

Требования к усилению ИАФ.5

Требования не установлены.

ИАФ.6 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, НЕ ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА (ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ)

Требования к реализации ИАФ.6

В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все пользователи информационной системы, не указанные в ИАФ.1 в качестве внутренних пользователей.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ИАФ.6

Требования не установлены.

2. **УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА (УПД)**

УПД.1 УПРАВЛЕНИЕ (ЗАВЕДЕНИЕ, АКТИВАЦИЯ, БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ) УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ, В ТОМ ЧИСЛЕ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ

Требования к реализации УПД.1

Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);
- объединение учетных записей в группы (при необходимости);
- верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с

периодичностью, определяемой оператором;

- порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

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).

Правила и процедуры управления учетными записями пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.1:

1) оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей;

2) в информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;

3) в информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования:

а) более 90 дней;

б) более 45 дней;

4) в информационной системе должно осуществляться автоматическое блокирование учетных записей пользователей:

а) при превышении установленного оператором числа неуспешных попыток аутентификации пользователя;

б) при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации;

5) в информационной системе должен осуществляться автоматический контроль заведения, активации, блокирования и уничтожения учетных записей пользователей и оповещение администраторов о результатах автоматического контроля.

УПД.2 РЕАЛИЗАЦИЯ НЕОБХОДИМЫХ МЕТОДОВ УПРАВЛЕНИЯ ДОСТУПОМ (ДИСКРЕЦИОННЫЙ, МАНДАТНЫЙ, РОЛЕВОЙ ИЛИ ИНОЙ МЕТОД), ТИПОВ (ЧТЕНИЕ, ЗАПИСЬ, ВЫПОЛНЕНИЕ ИЛИ ИНОЙ ТИП) И ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА

Требования к реализации УПД.2

В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

- дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа - списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
- 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);
- мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

Правила разграничения доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.2:

1) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему;

2) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам;

3) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением;

4) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым прикладным и специальным программным

обеспечением.

УПД.3 УПРАВЛЕНИЕ (ФИЛЬТРАЦИЯ, МАРШРУТИЗАЦИЯ, КОНТРОЛЬ СОЕДИНЕНИЙ, ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА И ИНЫЕ СПОСОБЫ УПРАВЛЕНИЯ) ИНФОРМАЦИОННЫМИ ПОТОКАМИ МЕЖДУ УСТРОЙСТВАМИ, СЕГМЕНТАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, А ТАКЖЕ МЕЖДУ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Требования к реализации УПД.3

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором;
- разрешение передачи информации в информационной системе только по маршруту, установленному оператором;
- изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.

Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

Правила и процедуры управления информационными потоками регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.3:

1) в информационной системе должно обеспечиваться управление информационными потоками на основе атрибутов (меток) безопасности, связанных с передаваемой информацией, источниками и получателями информации;

2) в информационной системе должно обеспечиваться динамическое управление информационными потоками, запрещающее и (или) разрешающее передачу информации на основе анализа изменения текущего состояния информационной системы или условий ее функционирования;

3) в информационной системе должен исключаться обход правил управления информационными потоками за счет преобразования передаваемой информации;

4) в информационной системе должен исключаться обход правил управления информационными потоками за счет встраивания одних данных в другие данные информационного потока;

5) в информационной системе должен обеспечиваться контроль соединений между техническими средствами (устройствами), используемыми для организации информационных потоков;

6) в информационной системе при передаче информации между сегментами информационной системы и (или) информационными системами разных классов защищенности должна обеспечиваться однонаправленная передача информации с использованием аппаратных средств;

7) в информационной системе должно обеспечиваться управление информационными потоками на основе структуры передаваемых данных (текст, таблицы, видео, аудиоинформация);

8) в информационной системе должно обеспечиваться управление информационными потоками на основе используемых сетевых протоколов;

9) в информационной системе должно обеспечиваться управление информационными потоками на основе типов (расширений) файлов и (или) имен файлов;

10) в информационной системе должна обеспечиваться возможность запрета, разрешения и изменения маршрута передачи информации только администраторами;

11) в информационной системе должно обеспечиваться разделение информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации;

12) в информационной системе должна обеспечиваться возможность автоматического блокирования передачи информации при выявлении в передаваемой информации вредоносных компьютерных программ;

13) в информационной системе должно осуществляться управление информационными потоками при передаче информации между информационными системами;

14) в информационной системе должна обеспечиваться возможность фильтрации информационных потоков на уровне прикладного программного обеспечения (приложений);

15) в информационной системе должна осуществляться накопление статистических данных, проверка и фильтрация сетевых пакетов по их содержимому (технология DPI);

16) наделение трафика конкретными параметрами (в частности включение уведомлений пользователей, исключение или замена элементов трафика) в зависимости от получателя информации.

УПД.4 РАЗДЕЛЕНИЕ ПОЛНОМОЧИЙ (РОЛЕЙ) ПОЛЬЗОВАТЕЛЕЙ, АДМИНИСТРАТОРОВ И ЛИЦ, ОБЕСПЕЧИВАЮЩИХ ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации УПД.4

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).

Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с УПД.2.

Требования к усилению УПД.4:

1) оператором должно быть обеспечено выполнение каждой роли по обработке информации, администрированию информационной системы, ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы отдельным должностным лицом;

2) оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по обработке информации и полномочиями (ролью) по администрированию информационной системы и (или) ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы;

3) оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по контролю (мониторингу) за обеспечением уровня защищенности информации и полномочиями (ролью) по администрированию информационной системы и (или) ее системы защиты информации и обеспечению функционирования информационной системы;

4) оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по администрированию системы защиты информации информационной системы и полномочиями (ролью) по обеспечению функционирования информационной системы;

5) оператором должен быть определен администратор, имеющий права по передаче полномочий по администрированию информационной системы и системы защиты информации другим лицам и осуществляющий контроль за использованием переданных полномочий (супервизор).

УПД.5 НАЗНАЧЕНИЕ МИНИМАЛЬНО НЕОБХОДИМЫХ ПРАВ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯМ, АДМИНИСТРАТОРАМ И ЛИЦАМ, ОБЕСПЕЧИВАЮЩИМ ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации УПД.5:

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.

Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий.

Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с УПД.2.

Требования к усилению УПД.5:

1) оператором должно быть обеспечено предоставление прав и привилегий по доступу к функциям безопасности (параметрам настройки) средств защиты информации исключительно администратору, наделенному полномочиями по администрированию системы защиты информации (администратору безопасности);

2) запрет предоставления расширенных прав и привилегий внешним пользователям (пользователям, не являющимся внутренними пользователями).

УПД.6 ОГРАНИЧЕНИЕ НЕУСПЕШНЫХ ПОПЫТОК ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ (ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ)

Требования к реализации УПД.6

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).

Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4.

Требования к усилению УПД.6:

1) в информационной системе обеспечивается автоматическое 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) за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль);

2) в информационной системе обеспечивается автоматическое удаление информации с мобильного технического средства, входящего в состав информационной системы, при превышении допустимого числа неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени, осуществляемых с мобильного устройства;

3) в информационной системе обеспечивается противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания (в том числе с использованием технологии CAPTCHA).

УПД.7 ПРЕДУПРЕЖДЕНИЕ ПОЛЬЗОВАТЕЛЯ ПРИ ЕГО ВХОДЕ В ИНФОРМАЦИОННУЮ СИСТЕМУ О ТОМ, ЧТО В ИНФОРМАЦИОННОЙ СИСТЕМЕ РЕАЛИЗОВАНЫ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ, И О НЕОБХОДИМОСТИ СОБЛЮДЕНИЯ ИМ УСТАНОВЛЕННЫХ ОПЕРАТОРОМ ПРАВИЛ ОБРАБОТКИ ИНФОРМАЦИИ

Требования к реализации УПД.7

В информационной системе должно быть обеспечено предупреждение пользователя в виде сообщения ("окна") при его входе в информационную систему (до процесса аутентификации) о том, что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные оператором правила и ограничения на работу с информацией.

Вход в информационную систему и предоставление пользователю возможности работы в информационной системе осуществляются только после подтверждения пользователем

ознакомления с предупреждением.

Требования к усилению УПД.7:

Требования не установлены.

УПД.8 ОПОВЕЩЕНИЕ ПОЛЬЗОВАТЕЛЯ ПОСЛЕ УСПЕШНОГО ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ О ЕГО ПРЕДЫДУЩЕМ ВХОДЕ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Требования к реализации УПД.8

В информационной системе должно быть обеспечено после успешного входа пользователя в информационную систему (завершения процесса аутентификации) оповещение этого пользователя о дате и времени предыдущего входа в информационную систему от имени этого пользователя.

Требования к усилению УПД.8:

1) в информационной системе обеспечивается оповещение пользователя после успешного входа в информационную систему о количестве неуспешных попыток входа в информационную систему (доступа к информационной системе), зафиксированных с момента последнего успешного входа в информационную систему;

2) в информационной системе обеспечивается оповещение пользователя после успешного входа в информационную систему о количестве успешных и (или) неуспешных попыток входа в информационную систему (доступа к информационной системе), зафиксированных за период времени не менее 7 дней;

3) в информационной системе обеспечивается оповещение пользователя после успешного входа в информационную систему об изменении сведений, относящихся к учетной записи пользователя (в том числе изменении прав доступа), произведенных за период времени не менее чем с момента предыдущего успешного входа в информационную систему.

УПД.9 ОГРАНИЧЕНИЕ ЧИСЛА ПАРАЛЛЕЛЬНЫХ СЕАНСОВ ДОСТУПА ДЛЯ КАЖДОЙ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации УПД.9

В информационной системе должно обеспечиваться ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы.

В информационной системе должна быть предусмотрена возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий), основываясь на идентификаторах пользователей и (или) принадлежности к определенной роли.

Значение числа параллельных сеансов доступа может быть задано для информационной системы в целом, для отдельных сегментов информационной системы, для групп пользователей, отдельных пользователей или их комбинаций.

Ограничения числа параллельных сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.9:

1) в информационной системе для привилегированных учетных записей (администраторов) количество параллельных (одновременных) сеансов (сессий) от их имени с разных устройств

(средств вычислительной техники) не должно превышать следующих значений:

а) не более 2;

б) не более 1;

2) в информационной системе в случае попытки входа под учетной записью пользователя или администратора, для которых достигнуто максимальное значение допустимых параллельных сеансов, при успешной аутентификации пользователя или администратора должно выдаваться сообщение о превышении числа параллельных сеансов доступа, месте (местах) их предыдущего входа (предыдущих входов) с активными сессиями и предложением отключения этой сессии (этих сессий);

3) в информационной системе должны быть предусмотрены программно-технические средства, позволяющие контролировать и отображать администратору число активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей;

4) в информационной системе должны быть предусмотрены программно-технические средства, позволяющие оповещать администратора о попытках превышения числа установленных допустимых активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователя.

УПД.10 БЛОКИРОВАНИЕ СЕАНСА ДОСТУПА В ИНФОРМАЦИОННУЮ СИСТЕМУ ПОСЛЕ УСТАНОВЛЕННОГО ВРЕМЕНИ БЕЗДЕЙСТВИЯ (НЕАКТИВНОСТИ) ПОЛЬЗОВАТЕЛЯ ИЛИ ПО ЕГО ЗАПРОСУ

Требования к реализации УПД.10

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

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).

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации в соответствии с ИАФ.1.

Правила и процедуры блокирования сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.10:

1) в информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя:

а) до 15 минут;

б) до 5 минут;

2) в информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование "хранителя экрана", гашение экрана или иные способы);

3) в информационной системе обеспечивается завершение сеанса пользователя (выхода из системы) после превышения установленного оператором времени бездействия (неактивности) пользователя.

УПД.11 РАЗРЕШЕНИЕ (ЗАПРЕТ) ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ, РАЗРЕШЕННЫХ ДО ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Требования к реализации УПД.11

Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (веб-сайтам, 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).

Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.11

Требования не установлены.

УПД.12 ПОДДЕРЖКА И СОХРАНЕНИЕ АТРИБУТОВ БЕЗОПАСНОСТИ (МЕТОК БЕЗОПАСНОСТИ), СВЯЗАННЫХ С ИНФОРМАЦИЕЙ В ПРОЦЕССЕ ЕЕ ХРАНЕНИЯ И ОБРАБОТКИ

Требования к реализации УПД.12

В информационной системе должны обеспечиваться поддержка (обновление, назначение, изменение) и сохранение атрибутов безопасности (меток безопасности), установленных оператором, связанных с информацией в процессе ее хранения и обработки.

Атрибуты безопасности (метки безопасности) представляют собой свойства (характеристики) объектов и (или) субъектов доступа, которые используются для контроля доступа субъектов к объектам доступа и управления информационными потоками.

Правила и процедуры поддержки и сохранения атрибутов безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.12:

1) в информационной системе обеспечивается динамическое изменение атрибутов безопасности в соответствии с организационно-распорядительными документами по защите информации оператора в зависимости от процесса обработки информации (формирование, объединение, разделение информационных ресурсов);

2) в информационной системе допускается изменение атрибутов безопасности только авторизованными пользователям или процессами;

3) в информационной системе обеспечивается автоматизированный контроль связи атрибутов безопасности с информацией;

4) в информационной системе обеспечивается возможность отображения пользователям в удобочитаемом виде атрибутов безопасности (меток безопасности) для каждого из объектов доступа (отображение атрибутов безопасности на экране монитора и (или) при выводе информации на печать на принтере).

УПД.13 РЕАЛИЗАЦИЯ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА ЧЕРЕЗ ВНЕШНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Требования к реализации УПД.13

Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

- установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;
- 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;
- предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;
- контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.13:

1) в информационной системе для мониторинга и контроля удаленного доступа должны применяться автоматизированные средства (дополнительные программные или программно-технические средства);

2) в информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы;

3) в информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации;

4) в информационной системе при удаленном доступе обеспечивается применение в соответствии

с законодательством Кыргызской Республики криптографических методов защиты информации;

5) в информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой;

6) в информационной системе должен обеспечиваться запрет удаленного доступа с использованием сетевых технологий и протоколов, определенных оператором по результатам анализа защищенности в соответствии с АНЗ.1 как небезопасных.

УПД.14 РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА

Требования к реализации УПД.14

Оператором должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

Регламентация и контроль использования технологий беспроводного доступа должны включать:

- ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с УПД.2;
- предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;
- контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.14:

1) в информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с ИАФ.2;

2) в информационной системе обеспечивается мониторинг точек беспроводного подключения устройств к информационной системе на предмет выявления несанкционированного беспроводного подключения устройств;

3) в информационной системе исключается возможность изменения пользователем точек беспроводного доступа информационной системы;

4) оператором одолжен быть предусмотрен запрет беспроводного доступа к информационной системе из-за пределов контролируемой зоны;

5) в информационной системе должен быть запрещен беспроводный доступ от имени

привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации;

6) в информационной системе исключается возможность изменения пользователем устройств и настроек беспроводного доступа;

7) оператором обеспечивается определение местонахождения несанкционированного беспроводного устройства;

8) оператором обеспечивается блокирование функционирования несанкционированного беспроводного устройства.

УПД.15 РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Требования к реализации УПД.15

Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

Регламентация и контроль использования мобильных технических средств должны включать:

- установление видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы;
- использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30;
- ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2;
- мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;
- запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.15:

1) оператором обеспечивается запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

2) оператором обеспечивается запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);

3)оператором обеспечивается (в соответствии с процедурами, зафиксированными в организационно-распорядительных документах) очистка машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами контролируемой зоны;

4) оператором обеспечивается предоставление доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

5) в информационной системе обеспечивается запрет использования мобильных технических средств, на которые в информационной системе может быть осуществлена запись информации (перезаписываемых съемных машинных носителей информации).

УПД.16 УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ)

Требования к реализации УПД.16

Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы.

Управление взаимодействием с внешними информационными системами должно включать:

- предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с УПД.2;
- определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение системных учетных записей, используемых в рамках данного взаимодействия;
- определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;
- определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

Правила и процедуры управления взаимодействием с внешними информационными системами регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.16:

1) оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу

информации с использованием внешней информационной системы при выполнении следующих условий:

а) при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

б) при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

УПД.17 ОБЕСПЕЧЕНИЕ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Требования к реализации УПД.17

В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

Доверенная загрузка должна обеспечивать:

- блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
- контроль доступа пользователей к процессу загрузки операционной системы;
- контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

В информационной системе применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.17:

1) в информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения;

2) в информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения, реализованные на основе программно-аппаратного модуля;

3) в информационной системе должна осуществляться доверенная загрузка программного обеспечения телекоммуникационного оборудования.

3. **ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ (ОПС)**

ОПС.1 УПРАВЛЕНИЕ ЗАПУСКОМ (ОБРАЩЕНИЯМИ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, В ТОМ ЧИСЛЕ ОПРЕДЕЛЕНИЕ ЗАПУСКАЕМЫХ КОМПОНЕНТОВ, НАСТРОЙКА ПАРАМЕТРОВ ЗАПУСКА КОМПОНЕНТОВ, КОНТРОЛЬ ЗА ЗАПУСКОМ КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Требования к реализации ОПС.1:

Оператором должны быть реализованы следующие функции по управлению запуском (обращениями) компонентов программного обеспечения:

- определение перечня (списка) компонентов программного обеспечения (файлов, объектов баз данных, хранимых процедур и иных компонентов), запускаемых автоматически при загрузке операционной системы средства вычислительной техники;
- разрешение запуска компонентов программного обеспечения, включенных в перечень (список) программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;
- ограничение запуска компонентов программного обеспечения от имени администраторов безопасности (например, разрешение такого запуска только для программного обеспечения средств защиты информации: сенсоры систем обнаружения вторжений, агенты систем мониторинга событий информационной безопасности, средства антивирусной защиты);
- настройка параметров запуска компонентов программного обеспечения от имени учетной записи администратора безопасности таким образом, чтобы текущий пользователь средства вычислительной техники не мог получить через данные компоненты доступ к объектам доступа, на доступ к которым у него нет прав в соответствии с УПД.2;
- контроль за запуском компонентов программного обеспечения, обеспечивающий выявление компонентов программного обеспечения, не включенных в перечень (список) компонентов, запускаемых автоматически при загрузке операционной системы средства вычислительной техники.

Правила и процедуры управления запуском программного обеспечения (в том числе списки программного обеспечения, ограничения запуска, параметры запуска компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОПС.1:

1) в информационной системе обеспечивается разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности;

2) в информационной системе обеспечивается использование средств автоматизированного контроля перечня (списка) компонентов программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;

3) в информационной системе обеспечивается использование автоматизированных механизмов управления запуском (обращениями) компонентов программного обеспечения;

4) в информационной системе обеспечивается управление удаленным запуском компонентов программного обеспечения (например, запрет запуска компонентов программного обеспечения на одном средстве вычислительной техники командой с другого средства вычислительной техники);

5) в информационной системе обеспечивается управление временем запуска и завершения работы компонентов программного обеспечения (например, ограничение запуска только в течение рабочего дня);

6) в информационной системе обеспечивается контроль целостности (состояния) запускаемых компонентов программного обеспечения (файлов (в том числе конфигурационных), объектов баз данных, подключаемых библиотек и др.) в соответствии с ОЦЛ.1;

7) в информационной системе обеспечивается контроль обновления запускаемых компонентов программного обеспечения;

8) в информационной системе обеспечивается регистрация событий, связанных с контролем

состояния и обновлением запускаемых компонентов программного обеспечения;

9) в информационной системе обеспечивается запрет (блокирование) запуска определенных оператором компонентов программного обеспечения, не прошедших аутентификацию в соответствии с ИАФ.7.

ОПС.2 УПРАВЛЕНИЕ УСТАНОВКОЙ (ИНСТАЛЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, В ТОМ ЧИСЛЕ ОПРЕДЕЛЕНИЕ КОМПОНЕНТОВ, ПОДЛЕЖАЩИХ УСТАНОВКЕ, НАСТРОЙКА ПАРАМЕТРОВ УСТАНОВКИ КОМПОНЕНТОВ, КОНТРОЛЬ ЗА УСТАНОВКОЙ КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Требования к реализации ОПС.2

Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

- определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;
- 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 установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);
- выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или невключение в домен);
- контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);
- 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.

Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.

Требования к усилению ОПС.2:

1) в информационной системе должно обеспечиваться использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации;

2) в информационной системе должны быть реализованы автоматизированные механизмы реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации, предусматривающие блокирование доступа к средству вычислительной техники и (или) информации, автоматическое восстановление параметров настройки или другие действия, препятствующие несанкционированному доступу к информации, который может быть получен вследствие несанкционированного изменения параметров настройки;

3) в информационной системе должно обеспечиваться использование средств автоматизации для инсталляции и централизованного управления процессами инсталляции, в том числе с применением пакетов соответствующих дистрибутивов программного обеспечения.

ОПС.3 УСТАНОВКА (ИНСТАЛЛЯЦИЯ) ТОЛЬКО РАЗРЕШЕННОГО К ИСПОЛЬЗОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И (ИЛИ) ЕГО КОМПОНЕНТОВ

Требования к реализации ОПС.3

Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе 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).

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5.

Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.

Требования к усилению ОПС.3:

Требования не установлены.

ОПС.4 УПРАВЛЕНИЕ ВРЕМЕННЫМИ ФАЙЛАМИ, В ТОМ ЧИСЛЕ ЗАПРЕТ, РАЗРЕШЕНИЕ, ПЕРЕНАПРАВЛЕНИЕ ЗАПИСИ, УДАЛЕНИЕ ВРЕМЕННЫХ ФАЙЛОВ

Требования к реализации ОПС.4

В информационной системе должно осуществляться управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

Управление временными файлами должно обеспечивать перехват записи временной информации в файлы на системном (загрузочном) разделе машинного носителя информации средства вычислительной техники и ее перенаправление в оперативную память и (или) в другой раздел машинного носителя информации с последующей очисткой (стиранием).

Оператором должен быть определен и зафиксирован в организационно-распорядительной документации по защите информации (задокументирован) порядок очистки (стирания) временных файлов.

Требования к усилению ОПС.4:

1) в информационной системе должны осуществляться:

а) контроль доступа к временным файлам;

б) удаление временных файлов по завершении сеанса работы с ними.

4. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ (ЗНИ)

ЗНИ.1 УЧЕТ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Требования к реализации ЗНИ.1

Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

Учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации.

Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

Требования к усилению ЗНИ.1:

1) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая:

а) информацию о возможности использования машинного носителя информации вне информационной системы;

б) информацию о возможности использования машинного носителя информации за пределами

контролируемой зоны (конкретных помещений);

в) атрибуты безопасности, указывающие на возможность использования этих машинных носителей информации для обработки (хранения) соответствующих видов информации;

2) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая не отторгаемую цифровую метку носителя информации для обеспечения возможности распознавания (идентификации) носителя в системах управления доступом;

3) оператором обеспечиваться маркировка машинных носителей информации (технических средств), дополнительно включающая использование механизмов распознавания (идентификации) носителя информации по его уникальным физическим характеристикам.

ЗНИ.2 УПРАВЛЕНИЕ ДОСТУПОМ К МАШИННЫМ НОСИТЕЛЯМ ИНФОРМАЦИИ

Требования к реализации ЗНИ.2

Оператором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе:

- определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:
- съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);
- предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций);

Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.2:

1) применение автоматизированной системы контроля физического доступа в помещения, в которых осуществляется хранение машинных носителей информации;

2) опечатывание корпуса средства вычислительной техники, в котором стационарно установлен машинный носитель информации;

3) в информационной системе должно обеспечиваться применение программных (программно-технических) автоматизированных средств управления физическим доступом к машинным носителям информации;

4) контроль физического доступа лиц к машинным носителям информации в соответствии с атрибутами безопасности, установленными для этих носителей.

ЗНИ.3 КОНТРОЛЬ ПЕРЕМЕЩЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

Требования к реализации ЗНИ.3

Оператором должен обеспечиваться контроль перемещения используемых в информационной системе машинных носителей информации за пределы контролируемой зоны. При контроле перемещения машинных носителей информации должны осуществляться:

- определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;
- предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функций);
- учет перемещаемых машинных носителей информации в соответствии с ЗНИ.1;
- периодическая проверка наличия машинных носителей информации.

Правила и процедуры контроля перемещения машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.3:

1) оператором информационной системы определяются задачи (виды деятельности, функции), для решения которых необходимо перемещение машинных носителей информации за пределы контролируемой зоны;

2) применение в соответствии с законодательством Кыргызской Республики криптографических методов защиты информации, хранимой на носителе, при перемещении машинных носителей информации за пределы контролируемой зоны;

3) оператором определяется должностное лицо, ответственное за перемещение машинных носителей информации;

4) оператором информационной системы осуществляется периодическая проверка машинных носителей информации после их возврата в 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

Требования к реализации ЗНИ.4:

Оператором должно обеспечиваться исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах должно предусматривать:

- определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);
- физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище

машинных носителей информации);
- 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.

Правила и процедуры управления, направленные на исключение несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах, регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.4:

1) оператором должны применяться средства контроля съемных машинных носителей информации;

2) оператором должны применяться в соответствии с законодательством Кыргызской Республики криптографические методы защиты информации, хранящейся на машинных носителях;

3) оператором должен быть определен перечень машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации).

ЗНИ.5 КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ИНТЕРФЕЙСОВ ВВОДА (ВЫВОДА)

Требования к реализации ЗНИ.5

В информационной системе должен осуществляться контроль использования интерфейсов ввода (вывода).

Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать:

- определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе;
- определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода);
- принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода);
- контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода(вывода), могут применяться:

- опечатывание интерфейсов ввода (вывода);
- использование механических запирающих устройств;
- удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);
- применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

Правила и процедуры контроля использования интерфейсов ввода (вывода) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.5:

1) в информационной системе должна быть обеспечена регистрация использования интерфейсов ввода (вывода) в соответствии с РСБ.3;

2) оператором обеспечивается конструктивное (физическое) исключение из средства вычислительной техники запрещенных к использованию интерфейсов ввода (вывода);

3) оператором информационной системы обеспечивается программное отключение запрещенных к использованию интерфейсов ввода (вывода).

ЗНИ.6 КОНТРОЛЬ ВВОДА (ВЫВОДА) ИНФОРМАЦИИ НА МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Требования к реализации ЗНИ.6

В информационной системе должен осуществляться контроль ввода (вывода) информации на машинные носители информации.

Контроль ввода (вывода) информации на машинные носители информации должен предусматривать:

- определение оператором типов носителей информации, ввод (вывод) информации на которые подлежит контролю;
- определение оператором категорий пользователей, которым предоставлены полномочия по вводу (выводу) информации на машинные носители в соответствии с УПД.2;
- 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;
- регистрация действий пользователей и событий по вводу (выводу) информации на машинные носители информации в соответствии с РСБ.3.

Правила и процедуры контроля ввода (вывода) информации на машинные носители информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.6:

1) в информационной системе должна создаваться копия информации, записываемой пользователями на съемные машинные носители информации (теневое копирование);

2) оператором должны применяться средства контроля подключения съемных машинных носителей информации.

ЗНИ.7 КОНТРОЛЬ ПОДКЛЮЧЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Требования к реализации ЗНИ.7:

В информационной системе должен обеспечиваться контроль подключения машинных носителей информации.

Контроль подключения машинных носителей информации должен предусматривать:

- определение оператором типов носителей информации, подключение которых к информационной системе разрешено в соответствии с УПД.2;
- определение оператором категорий пользователей, которым предоставлены полномочия по

подключению носителей к информационной системе в соответствии с УПД.2;
- запрет подключения носителей информации, подключение которых к информационной системе не разрешено;
- регистрация действий пользователей и событий по подключению к информационной системе носителей в соответствии с РСБ.3.

Правила и процедуры контроля подключения машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.7:

1) оператором должен обеспечиваться контроль подключения машинных носителей информации с использованием средств контроля подключения съемных машинных носителей информации, позволяющих устанавливать разрешенные и (или) запрещенные типы и (или) конкретные съемные машинные носители информации для различных категорий пользователей;

2) запрет подключения к информационной системе носителей пользователями, не имеющими полномочий на подключение носителей.

ЗНИ.8 УНИЧТОЖЕНИЕ (СТИРАНИЕ) ИНФОРМАЦИИ НА МАШИННЫХ НОСИТЕЛЯХ ПРИ ИХ ПЕРЕДАЧЕ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ, В СТОРОННИЕ ОРГАНИЗАЦИИ ДЛЯ РЕМОНТА ИЛИ УТИЛИЗАЦИИ, А ТАКЖЕ КОНТРОЛЬ УНИЧТОЖЕНИЯ (СТИРАНИЯ)

Требования к реализации ЗНИ.8

Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

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.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации.

Требования к усилению ЗНИ.8:

1) оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации;

2) оператором должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации;

3) оператором перед подключением к информационной системе должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к информационной системе, при использовании в иных информационных системах, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях, определяемых оператором;

4) оператором должно быть обеспечено уничтожение машинных носителей информации, которые не подлежат очистке (неперезаписываемые машинные носители информации, такие как

оптические диски);

5) оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

а) удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

б) перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

в) очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

г) полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

д) размагничивание машинного носителя информации;

е) физическое уничтожение машинного носителя информации (в том числе сжигание, измельчение, плавление, расщепление, распыление и другое).

5. **РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ (РСБ)**

РСБ.1 ОПРЕДЕЛЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ, И СРОКОВ ИХ ХРАНЕНИЯ

Требования к реализации РСБ.1

Оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки 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.

События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации

(документируется).

В информационной системе как минимум подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2.

Требования к усилению РСБ.1:

1) оператором должен обеспечиваться пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

2) оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с действиями от имени привилегированных учетных записей (администраторов);

3) оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей;

4) оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Кыргызской Республики, при этом:

а) осуществляется хранение только записей о выявленных событиях безопасности;

б) осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности;

в) осуществляется хранение журналов приложений, которые послужили основанием для регистрации события безопасности;

г) осуществляется хранение всех записей системных журналов и событий безопасности;

д) осуществляется хранение всех записей журналов приложений.

РСБ.2 ОПРЕДЕЛЕНИЕ СОСТАВА И СОДЕРЖАНИЯ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ

Требования к реализации РСБ.2

В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность 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.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации, состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.2:

1) в информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающую:

а) полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);

б) запись сетевых потоков (дампов), связанных с событием безопасности;

2) в информационной системе обеспечивается централизованное управление записями

регистрации событий безопасности в рамках сегментов информационной системы, определяемых оператором, и (или) информационной системы в целом;

3) в информационной системе обеспечивается индивидуальная регистрация пользователей групповых учетных записей (локальные и доменные группы пользователей);

4) в информационной системе обеспечивается регистрация информации о месте (в частности сетевой адрес, географическая привязка и (или) другая информация), с которого осуществляется вход субъектов доступа в информационную систему;

5) в информационной системе состав и содержание регистрационных записей при регистрации запуска процессов (приложений) должны включать следующие сведения:

а) параметров запуска процесса (приложения);

б) продолжительность работы;

в) объекты доступа, к которым осуществлялось обращение процесса (приложения);

г) использованные процессом (приложением) устройства;

6) в информационной системе обеспечивается запись следующей информации, связанной с доступом к объектам доступа (в частности к файлам):

а) тип доступа (в том числе чтение, исполнение, запись и (или) иные типы);

б) изменение атрибутов объектов доступа (права доступа, контрольные суммы, размер, содержание, путь, тип и (или) иные атрибуты);

в) продолжительность доступа.

РСБ.3 СБОР, ЗАПИСЬ И ХРАНЕНИЕ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В ТЕЧЕНИЕ УСТАНОВЛЕННОГО ВРЕМЕНИ ХРАНЕНИЯ

Требования к реализации РСБ.3

В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с РСБ.1;
- 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;
- хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1.

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.

Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.3:

1) в информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности;

2) в информационной системе обеспечивается объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по времени для своевременного выявления инцидентов и реагирования на них;

3) в информационной системе обеспечивается объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по событиям безопасности для своевременного выявления инцидентов и реагирования на них в масштабах оператора;

4) в информационной системе обеспечивается хранение записей системных журналов и записей о событиях безопасности в обособленном хранилище, физически отделенном от технических средств, входящих в состав информационной системы.

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

Требования к реализации РСБ.4

В информационной системе должно осуществляться 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:

- предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- 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.

Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.4:

1) в информационной системе обеспечивается выдача предупреждения администратору при

заполнении установленной оператором части (процент или фактическое значение) объема памяти для хранения информации о событиях безопасности;

2) в информационной системе обеспечивается выдача предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации, определенных оператором;

3) в информационной системе обеспечивается запрет обработки информации в случае аппаратных или программных ошибок, сбоев в механизмах сбора информации или достижения предела или переполнения объема (емкости) памяти.

РСБ.5 МОНИТОРИНГ (ПРОСМОТР, АНАЛИЗ) РЕЗУЛЬТАТОВ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ

Требования к реализации РСБ.5

Оператором должен осуществляться 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.

В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.5:

1) в информационной системе должны обеспечиваться интеграция результатов мониторинга (просмотра и анализа) записей регистрации (аудита) из разных источников (журналов, хранилищ информации о событиях безопасности) и их корреляция с целью выявления инцидентов безопасности и реагирования на них;

2) в информационной системе обеспечивается интеграция процессов мониторинга (просмотра, анализа) результатов регистрации событий безопасности с результатами анализа уязвимостей, проводимого в соответствии с АНЗ.1, и результатами обнаружения вторжений, проводимого в соответствии с СОВ.1 с целью усиления возможностей по выявлению признаков инцидентов безопасности;

3) в информационной системе обеспечивается полнотекстовый анализ привилегированных команд;

4) оператором обеспечивается анализ записанных сетевых потоков (дампов).

РСБ.6 ГЕНЕРИРОВАНИЕ ВРЕМЕННЫХ МЕТОК И (ИЛИ) СИНХРОНИЗАЦИЯ СИСТЕМНОГО ВРЕМЕНИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации РСБ.6

В информационной системе должно осуществляться генерирование надежных меток времени и

(или) синхронизация системного времени.

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.

Требования к усилению РСБ.6:

1) оператором информационной системы должен быть определен источник надежных меток времени; в информационной системе должна выполняться синхронизация системного времени с периодичностью, определенной оператором.

РСБ.7 ЗАЩИТА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ

Требования к реализации РСБ.7: В информационной системе должна обеспечиваться 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.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.7:

1) в информационной системе обеспечивается резервное копирование записей регистрации (аудита);

2) в информационной системе обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (не перезаписываемые носители информации);

3) в информационной системе для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Кыргызской Республики криптографические методы;

4) оператор предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу администраторов.

6. **АНТИВИРУСНАЯ ЗАЩИТА (АВЗ)**

АВЗ.1 РЕАЛИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Требования к реализации АВЗ.1

Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, средствах защиты информации по периметру (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);
- установку, конфигурирование и управление средствами антивирусной защиты;
- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;
- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);
- 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;
- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АВЗ.1:

1) в информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности;

2) в информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах);

3) оператором должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов);

4) в информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей;

5) в информационной системе должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты;

6) в информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы;

7) в информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

8) оператором должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники.

АВЗ.2 ОБНОВЛЕНИЕ БАЗЫ ДАННЫХ ПРИЗНАКОВ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (ВИРУСОВ)

Требования к реализации АВЗ.2: Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АВЗ.2:

1) в информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов);

2) в информационной системе должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных программ (вирусов) на всех компонентах информационной системы;

3) в информационной системе должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах;

4) в информационной системе должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов).

7. **ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ (СОВ)**

СОВ.1 ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ

Требования к реализации СОВ.1

Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения 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.

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.

Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам.

Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования информационных систем.

Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению СОВ.1:

1) оператором обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) информационной системы;

2) в информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы;

3) обнаружение и реагирование (уведомление администратора безопасности, блокирование трафика и иные действия по реагированию) на компьютерные атаки в масштабе времени, близком к реальному;

4) защита информации, собранной и сгенерированной системой обнаружения вторжений, от несанкционированного доступа, модификации и удаления;

5) оператором информационной системы обеспечивается применение систем обнаружения вторжений уровня узла на автоматизированных рабочих местах и серверах информационной системы;

6) оператором информационной системы обеспечивается применение систем обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем.

СОВ.2 ОБНОВЛЕНИЕ БАЗЫ РЕШАЮЩИХ ПРАВИЛ

Требования к реализации СОВ.2

Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;
- получение из доверенных источников и установку обновлений базы решающих правил;
- контроль целостности обновлений базы решающих правил.

Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению СОВ.2:

1) в информационной системе должно обеспечиваться централизованное управление обновлением базы решающих правил системы обнаружения вторжений;

2) в информационной системе должна обеспечиваться возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченных должностных лиц (администраторов) для предотвращения определенных оператором компьютерных атак и (или) сокращения нагрузки на информационную систему, а также минимизации ложных срабатываний системы обнаружения вторжений;

3) оператором информационной системы устанавливается порядок редактирования базы решающих правил. В случае редактирования базы решающих правил запись об этом событии с указанием произведенных изменений фиксируется в соответствующем журнале регистрации событий безопасности.

8. **КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ (АН3)**

АН3.1 ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации АН3.1

Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (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;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- 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;
- информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и

эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором.

При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

Правила и процедуры выявления, анализа и устранения уязвимостей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АН3.1:

1) оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

2) оператор должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях;

3) оператором определяется информация об информационной системе, которая может стать известной нарушителям и использована ими для эксплуатации уязвимостей (в том числе уязвимостей "нулевого дня" - уязвимостей, описание которых отсутствует в базах данных разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств), и принимаются меры по снижению (исключению) последствий от эксплуатации нарушителями неустранимых уязвимостей;

4) оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности);

5) оператором применяются автоматизированные средства для сравнения результатов сканирования уязвимостей в разные периоды времени для анализа изменения количества и классов (типов) уязвимостей в информационной системе;

6) оператором применяются автоматизированные средства для обнаружения в информационной системе неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности);

7) оператором проводится анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в информационной системе для нарушения безопасности информации;

8) оператором обеспечивается проведение выявления уязвимостей "нулевого дня", о которых стало известно, но информация о которых не включена в сканеры уязвимостей;

9) оператором обеспечивается проведение выявления новых уязвимостей, информация о которых не опубликована в общедоступных источниках;

10) оператором должно осуществляться выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах;

11) оператором должно использоваться тестирование информационной системы на проникновение.

АНЗ.2 КОНТРОЛЬ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации АНЗ.2

Оператором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

Оператором должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

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.

Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах.

При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с АВЗ.2, баз решающих правил систем обнаружения вторжений в соответствии с СОВ.2, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АНЗ.2:

1) оператором должна осуществляться проверка корректности функционирования обновлений в тестовой среде с обязательным оформлением результатов проверки в соответствующем журнале;

2) оператором обеспечивается регламентация и контроль обновлений программного обеспечения базовой системы ввода-вывода (иного микропрограммного обеспечения).

АНЗ.3 КОНТРОЛЬ РАБОТОСПОСОБНОСТИ, ПАРАМЕТРОВ НАСТРОЙКИ И ПРАВИЛЬНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации АН3.3

Оператором должен проводиться 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:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;
- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
- 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.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АН3.3:

1) в информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации;

2) оператором в случае обнаружения нарушений работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации должен обеспечиваться перевод информационной системы, сегмента или компонента информационной системы в режим ограничения обработки информации и (или) запрет обработки информации в информационной системе, сегменте или компоненте информационной системы до устранения нарушений;

3) оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию параметров настройки программного обеспечения и средств защиты информации и восстановление параметров настройки программного обеспечения и средств защиты информации;

4) в информационной системе должно использоваться программное обеспечение, прошедшее контроль отсутствия не декларированных возможностей и отсутствия влияния на корректность работы средств защиты информации.

АН3.4 КОНТРОЛЬ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации АН3.4

Оператором должен проводиться контроль состава технических средств, программного

обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

- 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;
- 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;
- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АН3.4:

1) в информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации;

2) оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию технических средств, программного обеспечения и средств защиты информации.

АН3.5 КОНТРОЛЬ ПРАВИЛ ГЕНЕРАЦИИ И СМЕНЫ ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ, ЗАВЕДЕНИЯ И УДАЛЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ, РЕАЛИЗАЦИИ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПОМ, ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации АН3.5:

Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;
- контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;
- контроль реализации правил разграничения доступом в соответствии с УПД.2;
- контроль реализации полномочий пользователей в соответствии с УПД.4 и УПД.5;
- 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;
- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АН3.5:

1) в информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;

2) оператором должны использоваться автоматизированные средства, обеспечивающие контроль правил генерации и смены паролей пользователей, учетных записей пользователей, правил разграничения доступом и полномочий пользователей.

9. **ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ИНФОРМАЦИИ (ОЦЛ)**

ОЦЛ.1 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации ОЦЛ.1

В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:

- 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;
- 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;
- контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;
- 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 АН3.1 и АН3.2;
- обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3.

В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ,

оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.1:

1) в информационной системе контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

2) в информационной системе должен обеспечиваться контроль целостности средств защиты информации с использованием криптографических методов в соответствии с законодательством Кыргызской Республики, всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

3) оператором исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды;

4) оператором обеспечивается выделение рабочих мест с установленными средствами разработки и отладки программ в отдельный сегмент (тестовую среду);

5) в информационной системе должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности.

ОЦЛ.2 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В БАЗАХ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ОЦЛ.2

В информационной системе должен осуществляться контроль целостности информации, содержащейся в базах данных информационной системы.

Контроль целостности информации, содержащейся в базах данных информационной системы, должен предусматривать:

- 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;
- контроль целостности с периодичностью, установленной оператором, объектов баз данных, определяемых оператором, по контрольным суммам и (или) с использованием криптографических методов в соответствии с законодательством Кыргызской Республики в процессе загрузки и (или) динамически в процессе работы информационной системы;
- обеспечение физической защиты технических средств информационной системы, на которых установлена база данных, в соответствии с ЗТС.2 и ЗТС.3.

Правила и процедуры контроля целостности информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.2:

1) в информационной системе должны выполняться процедуры контроля целостности информации, содержащейся в базе данных, перед каждым запуском программного обеспечения доступа к базе данных;

2) в информационной системе должен обеспечиваться контроль целостности исполняемых модулей, хранящихся в базах данных (например, хранимые процедуры, триггеры);

3) в информационной системе должна обеспечиваться блокировка запуска системы управления базы данных и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности;

4) контроль целостности структуры базы данных и контроль целостности информации, хранящейся в базе данных, с применением специальных программных автоматизированных средств контроля целостности.

ОЦЛ.3 ОБЕСПЕЧЕНИЕ ВОЗМОЖНОСТИ ВОССТАНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

Требования к реализации ОЦЛ.3

Оператором должна быть предусмотрена возможность 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.

Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

- восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
- восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;
- 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.

Оператором применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

Правила и процедуры восстановления (в том числе планы по действиям персонала, порядок применения компенсирующих мер) отражаются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.3:

1) оператором обеспечивается восстановление отдельных функциональных возможностей информационной системы с применением резервированного программного обеспечения

зеркальной информационной системы (сегмента информационной системы, технического средства, устройства) в соответствии с ОДТ.2 и ОДТ.4.

ОЦЛ.4 ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ НА ПОСТУПЛЕНИЕ В ИНФОРМАЦИОННУЮ СИСТЕМУ НЕЗАПРАШИВАЕМЫХ ЭЛЕКТРОННЫХ СООБЩЕНИЙ (ПИСЕМ, ДОКУМЕНТОВ) И ИНОЙ ИНФОРМАЦИИ, НЕ ОТНОСЯЩИХСЯ К ФУНКЦИОНИРОВАНИЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ (ЗАЩИТА ОТ СПАМА)

Требования к реализации ОЦЛ.4

Оператором должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

- фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;
- фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием "черных" списков (запрещенные отправители) и (или) "белых" списков (разрешенные отправители).

Оператором должно осуществляться обновление базы "черных" ("белых") списков и контроль целостности базы "черных" ("белых") списков.

Правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.4:

1) оператором обеспечивается централизованное управление средствами защиты от спама;

2) в информационной системе должна обеспечиваться фильтрация на основе информации об отправителе электронного сообщения с использованием эвристических методов (например, "серые" списки серверов электронной почты, распознавание автоматически генерируемых имен отправителей и другие);

3) в информационной системе должна обеспечиваться аутентификация отправителей электронных сообщений в соответствии с ИАФ.1, ИАФ.6, ИАФ.7;

4) в информационной системе должна обеспечиваться аутентификация серверов электронной почты (в том числе в соответствии с ИАФ.2, ИАФ.7);

5) в информационной системе должен обеспечиваться контроль поступления в информационную систему информационных сообщений и документов на основе контентного анализа.

ОЦЛ.5 КОНТРОЛЬ СОДЕРЖАНИЯ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ (КОНТЕЙНЕРНЫЙ, ОСНОВАННЫЙ НА СВОЙСТВАХ ОБЪЕКТА ДОСТУПА, И КОНТЕНТНЫЙ, ОСНОВАННЫЙ НА ПОИСКЕ ЗАПРЕЩЕННОЙ К ПЕРЕДАЧЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СИГНАТУР, МАСОК И ИНЫХ МЕТОДОВ), И ИСКЛЮЧЕНИЕ НЕПРАВОМЕРНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ ИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ОЦЛ.5

В информационной системе должен осуществляться контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы.

Контроль содержания информации, передаваемой из информационной системы, должен предусматривать:

- выявление фактов неправомерной передачи защищаемой информации из информационной системы через различные типы сетевых соединений, включая сети связи общего пользования, и реагирование на них;
- выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации и реагирование на них;
- выявление фактов неправомерного вывода на печать документов, содержащих защищаемую информацию, и реагирование на них;
- выявление фактов неправомерного копирования защищаемой информации в прикладное программное обеспечение из буфера обмена и реагирование на них;
- контроль хранения защищаемой информации на серверах и автоматизированных рабочих местах;
- выявление фактов хранения информации на общих сетевых ресурсах (общие папки, системы документооборота, базы данных, почтовые архивы и иные ресурсы).

Контроль содержания информации, передаваемой из информационной системы, осуществляется по цифровым отпечаткам информации, по регулярным выражениям и (или) по атрибутам безопасности (меткам безопасности) файлов, а также с помощью иных методов.

Правила и процедуры контроля содержания передаваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.5:

1) в информационной системе должно осуществляться хранение всей передаваемой из информационной системы информации и (или) информации с недопустимым к передаче из информационной системы содержанием, в течение времени, определяемого оператором;

2) в информационной системе должна осуществляться блокировка передачи из информационной системы информации с недопустимым содержанием.

ОЦЛ.6 ОГРАНИЧЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЕЙ ПО ВВОДУ ИНФОРМАЦИИ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Требования к реализации ОЦЛ.6

В информационной системе должно осуществляться 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.

Ограничения прав пользователей по вводу информации в информационную систему должны фиксироваться в организационно-распорядительных документах по защите информации (документироваться) и реализовываться в соответствии с УПД.4 и УПД.5.

Требования к усилению ОЦЛ.6:

1) в информационной системе обеспечивается исключение возможности ввода пользователями информации в информационную систему, вследствие реализации ограничительных интерфейсов по вводу информации только через специальные формы прикладного программного обеспечения.

ОЦЛ.7 КОНТРОЛЬ ТОЧНОСТИ, ПОЛНОТЫ И ПРАВИЛЬНОСТИ ДАННЫХ, ВВОДИМЫХ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Требования к реализации ОЦЛ.7

В информационной системе должен осуществляться 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.

Вводимые данные должны проверяться на наличие конструкций, которые могут быть интерпретированы программно-техническими средствами информационной системы как исполняемые команды.

Требования к усилению ОЦЛ.7:

Требования не установлены.

ОЦЛ.8 КОНТРОЛЬ ОШИБОЧНЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ПО ВВОДУ И (ИЛИ) ПЕРЕДАЧЕ ИНФОРМАЦИИ И ПРЕДУПРЕЖДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ ОБ ОШИБОЧНЫХ ДЕЙСТВИЯХ

Требования к реализации ОЦЛ.8

В информационной системе должен осуществляться 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:

- определение оператором типов ошибочных действий пользователей, которые потенциально могут привести к нарушению безопасности информации в информационной системе;
- генерирование сообщений для пользователей об их ошибочных действиях и о возможности нарушения безопасности информации в информационной системе для корректировки действий пользователей;

- 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;
- предоставление доступа к сообщениям об ошибочных действиях пользователей только администраторам.

Требования к усилению ОЦЛ.8:

Требования не установлены.

10. **ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ ИНФОРМАЦИИ (ОДТ)**

ОДТ.1 ИСПОЛЬЗОВАНИЕ ОТКАЗОУСТОЙЧИВЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Требования к реализации ОДТ.1

Оператором должно обеспечиваться использование отказоустойчивых технических средств, предусматривающее:

- 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;
- 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;
- применение в информационной системе технических средств с установленными оператором характеристиками (коэффициентом) готовности и надежности, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;
- 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);
- замена технических средств, характеристики (коэффициенты) готовности и надежности которых достигли предельного значения.

Оператором должно быть обеспечено определение требуемых характеристик (коэффициентов) надежности и готовности в соответствии с национальными стандартами.

Требования к усилению ОДТ.1:

1) оператор выводит из эксплуатации техническое средство путем передачи его функций другому (резервному) техническому средству до достижения первым предельных (пороговых) значений характеристик (коэффициентов) готовности и (или) надежности;

2) в информационной системе реализуется автоматическое оповещение (сигнализация) о достижении техническим средством предельных (пороговых) значений характеристик (коэффициентов) готовности и надежности (степень достижения предельных значений определяется оператором);

3) в информационной системе реализуется автоматическое оповещение (сигнализация) о достижении техническим средством предельных (пороговых) значений характеристик загрузки.

ОДТ.2 РЕЗЕРВИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ, СРЕДСТВ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ОДТ.2

Оператором должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы, предусматривающее:

- 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;
- 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;
- 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.

Резервирование технических средств в зависимости от требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации включает ненагруженное ("холодное") и (или) нагруженное ("горячее") резервирование.

При резервировании программного обеспечения осуществляется создание резервных копий общесистемного, специального и прикладного программного обеспечения, а также программного обеспечения средств защиты информации, необходимых для обеспечения требуемых условий непрерывности функционирования информационной системы и доступности информации.

Резервирование каналов передачи информации включает:

- резервирование каналов связи, обеспечивающее снижение вероятности отказа в доступе к информационной системе;
- наличие у основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров) информационной системы планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления.

Резервирование средств обеспечения функционирования информационной системы включает:

- использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы сегмента информационной системы (технического средства, устройства) в случае отключения основного источника питания;
- использование долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения сегментом информационной системы (техническим средством, устройством) установленных функциональных (задач);

- определение перечня энергозависимых технических средств, которым необходимо обеспечить наличие резервных источников питания (кратковременных и долговременных).

Правила и процедуры резервирования регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОДТ.2:

1) в информационной системе должно обеспечиваться резервирование автоматизированных рабочих мест, на которых обрабатывается информация (совокупности технических средств, установленного программного обеспечения, средств защиты информации и параметров настройки), в том числе предусматривающее:

- пространственное (географическое) отделение резервных автоматизированных рабочих мест от основных мест обработки информации, с учетом возможных угроз нарушения доступности информации;
- конфигурацию резервных мест обработки информации, предусматривающую минимально требуемые эксплуатационные возможности рабочего места;
- разработку оператором процедур обеспечения требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации в случае нарушения функционирования (сбоев, аварий) резервных мест обработки информации;
- ограничение времени обработки информации на резервном рабочем месте до времени восстановления функционирования основного рабочего места;

2) в информационной системе должно обеспечиваться предоставление резервных каналов связи от альтернативных поставщиков телекоммуникационных услуг (провайдеров), отличных от поставщиков (провайдеров) основных каналов связи;

3) в информационной системе должно обеспечиваться использование резервных каналов связи, проходящих по трассам, отличным от трасс прохождения основных каналов связи;

4) в информационной системе должно обеспечиваться использование резервных (отделенных от основных) телекоммуникационных сервисов, обеспечивающих доступность информации, до восстановления доступности основных телекоммуникационных сервисов поставщиком телекоммуникационных услуг (провайдером).

ОДТ.3 КОНТРОЛЬ БЕЗОТКАЗНОГО ФУНКЦИОНИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБНАРУЖЕНИЕ И ЛОКАЛИЗАЦИЯ ОТКАЗОВ ФУНКЦИОНИРОВАНИЯ, ПРИНЯТИЕ МЕР ПО ВОССТАНОВЛЕНИЮ ОТКАЗАВШИХ СРЕДСТВ И ИХ ТЕСТИРОВАНИЕ

Требования к реализации ОДТ.3

Оператором должен осуществляться контроль безотказного функционирования технических 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).

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.

Требования к усилению ОДТ.3:

1) в информационной системе должна быть обеспечена сигнализация (уведомление) о неисправностях, сбоях и отказах в функционировании программно-технических средств информационной системы;

2) оператором должна обеспечиваться регистрация сбоев и отказов в функционировании технических средств информационной системы;

3) в информационной системе должны применяться программные средства мониторинга технического состояния информационной системы, осуществляющие мониторинг отказов программных и программно-технических средств в соответствии с перечнем, определенным оператором.

ОДТ.4 ПЕРИОДИЧЕСКОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ ИНФОРМАЦИИ НА РЕЗЕРВНЫЕ МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Требования к реализации ОДТ.4

Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

- резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью;
- разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;
- регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;
- принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОДТ.4:

1) оператором должна осуществляться с установленной им периодичностью проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий (периодичность проверки работоспособности определяется оператором);

2) оператором должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию;

3) оператором должно осуществляться резервное копирование информации на зеркальную информационную систему (сегмент информационной системы, техническое средство, устройство);

4) оператором должна обеспечиваться соответствующая пропускная способность каналов связи,

используемых для передачи резервных копий в процессе их создания или восстановления информации, для достижения требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации;

5) оператором должно осуществляться пространственное (географическое) разнесение мест хранения носителей резервных копий информации и мест расположения оригиналов этой информации.

ОДТ.5 ОБЕСПЕЧЕНИЕ ВОЗМОЖНОСТИ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ С РЕЗЕРВНЫХ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ (РЕЗЕРВНЫХ КОПИЙ) В ТЕЧЕНИЕ УСТАНОВЛЕННОГО ВРЕМЕННОГО ИНТЕРВАЛА

Требования к реализации ОДТ.5

Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:

- определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;
- восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;
- регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОДТ.5:

1) оператором должна обеспечиваться возможность восстановления информации с учетом нагруженного ("горячего") резервирования технических средств в соответствии с ОДТ.2;

2) в информационной системе должно осуществляться предоставление пользователям резервных мест обработки информации в соответствии с ОДТ.2 до восстановления из резервных копий информации и обеспечения ее доступности на основных местах обработки информации.

11. **ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ (ЗСВ)**

ЗСВ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ АДМИНИСТРАТОРОВ УПРАВЛЕНИЯ СРЕДСТВАМИ ВИРТУАЛИЗАЦИИ

Требования к реализации ЗСВ.1

В информационной системе должны обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7.

Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

В качестве компонентов виртуальной инфраструктуры необходимо, как минимум, рассматривать серверное оборудование, аппаратное обеспечение консолей управления, оборудование хранения данных, сетевое оборудование, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальное аппаратное обеспечение, виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенным для выполнения определенных функций в виртуальной инфраструктуре), программное обеспечение управления виртуальной инфраструктурой (в том числе гипервизором, настройками виртуальных машин, миграцией виртуальных машин, балансировкой нагрузки), служебные данные компонентов виртуальной инфраструктуры (настройки и иные служебные данные), средства резервного копирования компонентов среды виртуализации и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

В качестве объектов доступа в виртуальной инфраструктуре необходимо, как минимум, рассматривать программное обеспечение управления виртуальной инфраструктурой, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальные контейнеры (зоны), виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенная для выполнения определенных функций в виртуальной инфраструктуре), средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

- идентификация и аутентификация администраторов управления средствами виртуализации;
- идентификация и аутентификация субъектов доступа при их локальном и удаленном обращении к объектам доступа в виртуальной инфраструктуре;
- блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
- защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;
- защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;
- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1 - ИАФ.7.

Требования к усилению ЗСВ.1:

1) в информационной системе должны обеспечиваться взаимная идентификация и аутентификация

пользователя и сервера виртуализации (виртуальных машин) при удаленном доступе.

ЗСВ.2 УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ ВНУТРИ ВИРТУАЛЬНЫХ МАШИН

Требования к реализации ЗСВ.2

В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13.

При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться:

- контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;
- контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;
- управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;
- контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

Кроме того, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать:

- разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);
- разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом.

Требования к усилению ЗСВ.2:

1) в информационной системе должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры;

2) в информационной системе должен обеспечиваться доступ к конфигурации виртуальных машин только администраторам виртуальной инфраструктуры;

3) администратор виртуальной инфраструктуры определяет ограничения по изменению состава устройств виртуальных машин, объема используемой оперативной памяти, подключаемых виртуальных и физических носителей информации;

4) в информационной системе должен обеспечиваться контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора, в памяти хостовой операционной системы, виртуальных машин и (или) иных объектов доступа.

ЗСВ.3 РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

Требования к реализации ЗСВ.3

В информационной системе должна обеспечиваться регистрация событий безопасности в виртуальной инфраструктуре в соответствии с РСБ.1, РСБ.2, РСБ.3, РСБ.4 и РСБ.5.

При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в РСБ.1, должны подлежать регистрации следующие события:

- запуск (завершение) работы компонентов виртуальной инфраструктуры;
- доступ субъектов доступа к компонентам виртуальной инфраструктуры;
- изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;
- изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период ее аппаратного отключения состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил

разграничения доступа к указанным компонентам виртуальной инфраструктуры.

Требования к усилению ЗСВ.3:

1) в информационной системе должен обеспечиваться централизованный сбор, хранение и анализ информации о зарегистрированных событиях безопасности виртуальной инфраструктуры;

2) в информационной системе при регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) программ и процессов в гипервизоре и хостовой операционной системе;

3) в информационной системе должна обеспечиваться регистрация событий безопасности, связанных с перемещением и размещением виртуальных машин.

ЗСВ.4 УПРАВЛЕНИЕ (ФИЛЬТРАЦИЯ, МАРШРУТИЗАЦИЯ, КОНТРОЛЬ СОЕДИНЕНИЯ, ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА) ПОТОКАМИ ИНФОРМАЦИИ МЕЖДУ КОМПОНЕНТАМИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ, А ТАКЖЕ ПО ПЕРИМЕТРУ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Требования к реализации ЗСВ.4

В информационной системе должно осуществляться управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с УПД.3, ЗИС.3.

При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться:

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;
- обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);
- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объему и иным характеристикам;
- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;
- обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети;
- семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

Требования к усилению ЗСВ.4:

1) в информационной системе, построенной с применением технологии виртуализации, должна быть обеспечена единая точка подключения к виртуальной инфраструктуре (при необходимости резервирования каналов связи, точка подключения должна рассматриваться как комплексное решение, включающее в себя средства взаимодействия с основным и резервными каналами связи);

2) в информационной системе должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой виртуальной машины;

3) в информационной системе должен обеспечиваться запрет прямого (с использованием механизмов, встроенных в средства виртуализации) взаимодействия виртуальных машин между собой; для служебных данных должен обеспечиваться контроль прямого взаимодействия виртуальных машин между собой;

4) в информационной системе в соответствии с законодательством Кыргызской Республики применяются криптографические методы защиты информации конфиденциального характера, передаваемой по виртуальным и физическим каналам связи гипервизора, хостовой операционной системы;

5) в информационной системе при реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться семантический и статистический анализ сетевого трафика;

6) в информационной системе должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов в рамках виртуальной инфраструктуры;

7) в информационной системе должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов между виртуальной инфраструктурой и сетями, являющимися внешними по отношению к виртуальной инфраструктуре.

ЗСВ.5 ДОВЕРЕННАЯ ЗАГРУЗКА СЕРВЕРОВ ВИРТУАЛИЗАЦИИ, ВИРТУАЛЬНОЙ МАШИНЫ (КОНТЕЙНЕРА), СЕРВЕРОВ УПРАВЛЕНИЯ ВИРТУАЛИЗАЦИЕЙ

Требования к реализации ЗСВ.5

В информационной системе должна обеспечиваться доверенная загрузка серверов виртуализации, виртуальных машин (контейнеров) и серверов управления виртуализацией в соответствии с УПД.17.

Доверенная загрузка должна обеспечивать блокирование попыток несанкционированной загрузки гипервизора, хостовой и гостевых операционных систем.

Доверенная загрузка гипервизоров обеспечивается с использованием средств доверенной загрузки функционирующих на серверах виртуализации.

Доверенная загрузка виртуальных машин (контейнеров) обеспечивается с использованием многокомпонентных средств доверенной загрузки, отдельные компоненты которых функционируют в гипервизорах.

Требования к усилению ЗСВ.5:

1) должна обеспечиваться доверенная загрузка автоматизированных рабочих мест администраторов управления средствами виртуализации.

ЗСВ.6 УПРАВЛЕНИЕ ПЕРЕМЕЩЕНИЕМ ВИРТУАЛЬНЫХ МАШИН (КОНТЕЙНЕРОВ) И ОБРАБАТЫВАЕМЫХ НА НИХ ДАННЫХ

Требования к реализации ЗСВ.6

Оператором должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных должны обеспечиваться:

- регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);
- управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);
- управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;
- управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

Управление перемещением виртуальных машин (контейнеров) должно предусматривать:

- полный запрет перемещения виртуальных машин (контейнеров);
- ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
- ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

Требования к усилению ЗСВ.6:

1) оператором должно обеспечиваться перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных);

2) оператором должна осуществляться обработка отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных;

3) в информационной системе должны использоваться механизмы централизованного управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

4) в информационной системе должна быть обеспечена непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения;

5) в информационной системе должна осуществляться очистка освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных.

ЗСВ.7 КОНТРОЛЬ ЦЕЛОСТНОСТИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ И ЕЕ КОНФИГУРАЦИЙ

Требования к реализации ЗСВ.7

В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1.

При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

- контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);
- контроль целостности состава и конфигурации виртуального оборудования;
- контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;
- контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров).

Требования к усилению ЗСВ.7:

1) в информационной системе должен обеспечиваться контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры;

2) в информационной системе должен обеспечиваться контроль целостности микропрограмм и служебных данных элементов аппаратной части виртуальной инфраструктуры (в том числе загрузочных записей машинных носителей информации);

3) в информационной системе должен обеспечиваться контроль состава аппаратной части компонентов виртуальной инфраструктуры;

4) в информационной системе должен обеспечиваться контроль целостности программного обеспечения облачных клиентов.

ЗСВ.8 РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ, РЕЗЕРВИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ, А ТАКЖЕ КАНАЛОВ СВЯЗИ ВНУТРИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Требования к реализации ЗСВ.8

В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с ОДТ.2, ОДТ.4, ОДТ.5.

При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должны обеспечиваться:

- определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;
- резервное копирование виртуальных машин (контейнеров);
- резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;
- резервирование программного обеспечения виртуальной инфраструктуры;
- резервирование каналов связи, используемых в виртуальной инфраструктуре;
- периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

Требования к усилению ЗСВ.8:

1) в информационной системе должно выполняться резервное копирование конфигурации виртуальной инфраструктуры;

2) в информационной системе должно выполняться резервное копирование программного обеспечения серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации;

3) в информационной системе должно выполняться резервирование дистрибутивов средств построения виртуальной инфраструктуры (в том числе средств управления виртуальной инфраструктурой);

4) в информационной системе должно обеспечиваться резервирование технических средств для серверов виртуализации, серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации;

5) в информационной системе должно обеспечиваться резервирование технических средств систем хранения данных и их компонент, используемых в виртуальной инфраструктуре;

6) в информационной системе должно обеспечиваться резервирование технических средств активного (коммутационного) и пассивного оборудования каналов связи, используемых в виртуальной инфраструктуре;

7) в информационной системе должно обеспечиваться применение технологий распределенного хранения информации и восстановления информации после сбоев для обеспечения отказоустойчивости виртуальной инфраструктуры.

ЗСВ.9 РЕАЛИЗАЦИЯ И УПРАВЛЕНИЕ АНТИВИРУСНОЙ ЗАЩИТОЙ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

Требования к реализации ЗСВ.9

В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2.

При реализации соответствующих мер должны обеспечиваться:

- проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;
- проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

Требования к усилению ЗСВ.9:

1) в информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты;

2) в информационной системе должен обеспечиваться контроль функционирования средств антивирусной защиты в виртуальной инфраструктуре, в том числе маршрутизация потоков информации в виртуальной инфраструктуре через средство антивирусной защиты;

3) в информационной системе должна обеспечиваться реализация технологии обновления программного обеспечения и баз данных признаков компьютерных вирусов средств антивирусной защиты, предусматривающая однократную передачу обновлений на сервер виртуальной инфраструктуры для их последующего применения в виртуальных машинах;

4) в информационной системе должна обеспечиваться проверка наличия вредоносных программ

(вирусов) в гипервизоре;

5) в информационной системе должна обеспечиваться проверка наличия вредоносных программ в файлах конфигурации виртуального оборудования;

6) в информационной системе должна обеспечиваться проверка наличия вредоносных программ в файлах-образах виртуализированного программного обеспечения и виртуальных машин.

ЗСВ.10 РАЗБИЕНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ НА СЕГМЕНТЫ (СЕГМЕНТИРОВАНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ) ДЛЯ ОБРАБОТКИ ИНФОРМАЦИИ ОТДЕЛЬНЫМ ПОЛЬЗОВАТЕЛЕМ И (ИЛИ) ГРУППОЙ ПОЛЬЗОВАТЕЛЕЙ

Требования к реализации ЗСВ.10

В информационной системе должно обеспечиваться разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17.

Требования к усилению ЗСВ.10:

1) в информационной системе должно обеспечиваться логическое сегментирование виртуальной инфраструктуры, предусматривающее выделение группы виртуальных машин, хранилищ информации и информационных потоков, предназначенных для решения выделенных (обособленных) задач;

2) в информационной системе должно обеспечиваться выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией (автоматизированного рабочего места администратора управления средствами виртуализации);

3) в информационной системе должно обеспечиваться физическое сегментирование виртуальной инфраструктуры для решения выделенных (обособленных) задач.

12. **ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ (ЗТС)**

ЗТС.1 ЗАЩИТА ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ, ОТ ЕЕ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Требования к реализации ЗТС.1

Оператором должна обеспечиваться защита информации, обрабатываемой техническими средствами, от ее утечки за счет побочных электромагнитных излучений и наводок.

Защита информации от утечки по техническим каналам должна осуществляться в соответствии с утвержденными требованиями по технической защите информации.

Требования к усилению ЗТС.1:

Требования не установлены.

ЗТС.2 ОРГАНИЗАЦИЯ КОНТРОЛИРУЕМОЙ ЗОНЫ, В ПРЕДЕЛАХ КОТОРОЙ ПОСТОЯННО РАЗМЕЩАЮТСЯ СТАЦИОНАРНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА, ОБРАБАТЫВАЮЩИЕ ИНФОРМАЦИЮ, И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, А ТАКЖЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ

Требования к реализации ЗТС.2

Оператором должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

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.

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.

Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

Требования к усилению ЗТС.2:

Требования не установлены.

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, СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ И СРЕДСТВАМ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ПОМЕЩЕНИЯ И СООРУЖЕНИЯ, В КОТОРЫХ ОНИ УСТАНОВЛЕНЫ

Требования к реализации ЗТС.3

Оператором должны обеспечиваться 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, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом должны предусматривать:

- определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Правила и процедуры контроля и управления физическим доступом регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗТС.3:

1) оператором должны применяться автоматизированные системы контроля и управления доступом (СКУД), обеспечивающие контроль и учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

2) оператором должны применяться средства видеонаблюдения, обеспечивающие регистрацию доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

3) оператором обеспечивается интеграция системы контроля и управления доступом (СКУД) со средствами идентификации и аутентификации пользователей в информационной системе в соответствии с ИАФ.1, ИАФ.6 и средствами управления доступом в соответствии с УПД.2, УПД.10.

ЗТС.4 РАЗМЕЩЕНИЕ УСТРОЙСТВ ВЫВОДА (ОТОБРАЖЕНИЯ) ИНФОРМАЦИИ, ИСКЛЮЧАЮЩЕЕ ЕЕ НЕСАНКЦИОНИРОВАННЫЙ ПРОСМОТР

Требования к реализации ЗТС.4:

Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, 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.

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.

Требования к усилению ЗТС.4:

1) оператором обеспечивается установка на окна помещений информационной системы средств, ограничивающих возможность визуального ознакомления с защищаемой информацией извне помещений (жалюзи, плотные шторы и иные средства), если в этих помещениях размещены устройства вывода информации на печать и (или) осуществляется отображение информации на видеоустройства.

ЗТС.5 ЗАЩИТА ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ (ВОЗДЕЙСТВИЙ ОКРУЖАЮЩЕЙ СРЕДЫ, НЕСТАБИЛЬНОСТИ ЭЛЕКТРОСНАБЖЕНИЯ, КОНДИЦИОНИРОВАНИЯ И ИНЫХ ВНЕШНИХ ФАКТОРОВ)

Требования к реализации ЗТС.5

Оператором должна осуществляться защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

Защита от внешних воздействий в соответствии с требованиями законодательства, стандартов и технических регламентов должна предусматривать:

- выполнение норм и правил пожарной безопасности;

- выполнение норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств;
- обеспечение необходимых для эксплуатации технических средств температурно-влажностного режима и условий по степени запыленности воздуха.

Требования к усилению ЗТС.5:

Требования не установлены.

13. **ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ, ЕЕ СРЕДСТВ И 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

Требования к реализации ЗИС.1

В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

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.

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.

Требования к усилению ЗИС.1:

1) в информационной системе должно обеспечиваться исключение отображения функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации в интерфейсе пользователя;

2) в информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов информационной системы;

3) в информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности;

4) оператором должно обеспечиваться исключение возможности управления (администрирования) информационной системой, управления (администрирования) системой защиты информации из-за пределов контролируемой зоны.

ЗИС.2 ПРЕДОТВРАЩЕНИЕ ЗАДЕРЖКИ ИЛИ ПРЕРЫВАНИЯ ВЫПОЛНЕНИЯ ПРОЦЕССОВ С ВЫСОКИМ ПРИОРИТЕТОМ СО СТОРОНЫ ПРОЦЕССОВ С НИЗКИМ ПРИОРИТЕТОМ

Требования к реализации ЗИС.2

В информационной системе должно обеспечиваться предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов (служб, сервисов) с низким приоритетом, предусматривающее:

- определение приоритетов процессов (служб, сервисов) для пользователей и (или) групп пользователей и (или) ролей в информационной системе;
- выполнение процессов (служб, сервисов) в информационной системе с учетом их приоритета (в первую очередь должны выполняться процессы с более высоким приоритетом);
- исключение задержки и (или) вмешательства в выполнение процессов (служб, сервисов) с более высоким приоритетом со стороны процессов (служб, сервисов) с более низким приоритетом.

Требования к усилению ЗИС.2:

1) в информационной системе должно обеспечиваться исключение возможности несанкционированного изменения приоритетов выполнения процессов.

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

Требования к реализации ЗИС.3

Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Кыргызской Республики средств криптографической защиты информации или иными методами.

Требования к усилению ЗИС.3:

1) оператор обеспечивает защиту от модификации и навязывания (ввода ложной информации) видеоинформации (звуковой информации) путем ее маркирования и контроля (в том числе с использованием цифровых водяных знаков) в различных точках тракта ее формирования и распространения;

2) оператор обеспечивает защиту от модификации и навязывания (ввода ложной информации) передаваемой видеоинформации путем выявления и удаления скрытых вставок.

ЗИС.4 ОБЕСПЕЧЕНИЕ ДОВЕРЕННЫХ КАНАЛА, МАРШРУТА МЕЖДУ АДМИНИСТРАТОРОМ, ПОЛЬЗОВАТЕЛЕМ И СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ (ФУНКЦИЯМИ БЕЗОПАСНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ)

Требования к реализации ЗИС.4:

В информационной системе должны обеспечиваться доверенные маршруты передачи данных между администратором (пользователем) и средствами защиты информации (функциями

безопасности средств защиты информации), определяемыми оператором.

Оператором должен быть определен перечень целей (функций) передачи данных, для которых требуется доверенный канал (маршрут).

Доверенный канал между пользователем и средствами защиты информации должен обеспечиваться при удаленном и локальном доступе в информационную систему.

Требования к усилению ЗИС.4:

Требования не установлены.

ЗИС.5 ЗАПРЕТ НЕСАНКЦИОНИРОВАННОЙ УДАЛЕННОЙ АКТИВАЦИИ ВИДЕОКАМЕР, МИКРОФОНОВ И ИНЫХ ПЕРИФЕРИЙНЫХ УСТРОЙСТВ, КОТОРЫЕ МОГУТ АКТИВИРОВАТЬСЯ УДАЛЕННО, И ОПОВЕЩЕНИЕ ПОЛЬЗОВАТЕЛЕЙ ОБ АКТИВАЦИИ ТАКИХ УСТРОЙСТВ

Требования к реализации ЗИС.5

В информационной системе должны осуществляться запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечения, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением.

В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких устройств.

Требования к усилению ЗИС.5:

1) в информационной системе должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны);

2) в информационной системе должна обеспечиваться возможность блокирования входящего и исходящего трафика от пользователей систем, предоставляющих внешние сервисы (например, системы видеоконференцсвязи), в которых конфигурации (настройки) сервисов для конечных пользователей устанавливаются провайдерами или самими пользователями;

3) оператором обеспечивается удаление (отключение) из информационной системы (отдельных сегментов, например, расположенных в защищаемых и выделенных помещениях) периферийных устройств, перечень которых определяется оператором;

4) оператором обеспечивается запись и хранение в течение установленного времени информации, переданной (полученной) периферийными устройствами ввода (вывода) информации при

разрешенной удаленной активации периферийных устройств ввода (вывода) информации.

ЗИС.6 ПЕРЕДАЧА И КОНТРОЛЬ ЦЕЛОСТНОСТИ АТРИБУТОВ БЕЗОПАСНОСТИ (МЕТОК БЕЗОПАСНОСТИ), СВЯЗАННЫХ С ИНФОРМАЦИЕЙ, ПРИ ОБМЕНЕ ИНФОРМАЦИЕЙ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Требования к реализации ЗИС.6

В информационной системе должна осуществляться передача, сопоставление (сравнение) атрибутов безопасности (меток безопасности) с информацией, которой она обменивается с иными (внешними) информационными системами.

Атрибуты безопасности могут сопоставляться с информацией, содержащейся в информационной системе, в явном или скрытом виде.

Меры по передаче и контролю целостности (сопоставлению, сравнению) атрибутов безопасности (меток безопасности) реализуются в соответствии с УПД.12.

Требования к усилению ЗИС.6:

1) в информационной системе должен обеспечиваться контроль целостности атрибутов безопасности (меток безопасности).

ЗИС.7 КОНТРОЛЬ САНКЦИОНИРОВАННОГО И ИСКЛЮЧЕНИЕ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОГО КОДА, В ТОМ ЧИСЛЕ РЕГИСТРАЦИЯ СОБЫТИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ МОБИЛЬНОГО КОДА, ИХ АНАЛИЗ И РЕАГИРОВАНИЕ НА НАРУШЕНИЯ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ МОБИЛЬНОГО КОДА

Требования к реализации ЗИС.7

Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

При контроле использования технологий мобильного кода должно быть обеспечено:

определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе;

определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода;

регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода;

исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки.

Правила и процедуры контроля использования технологий мобильного кода регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.7:

1) в информационной системе должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия, определяемые оператором;

2) в информационной системе должен осуществляться запрет загрузки и выполнения запрещенного мобильного кода;

3) в информационной системе для приложений, определяемых оператором, должен осуществляться запрет автоматического выполнения разрешенного мобильного кода (уведомление пользователя о получении мобильного кода и запрос разрешения на запуск или иные действия, определяемые оператором);

4) в информационной системе должен осуществляться контроль подлинности источника мобильного кода и контроль целостности 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

Требования к реализации ЗИС.8

Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. При контроле использования технологий передачи речи должно быть обеспечено:

- определение перечня технологий (сервисов) передачи речи разрешенных и (или) запрещенных для использования в информационной системе;
- определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи речи в соответствии с установленными ролями;
- реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи речи;
- регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи речи;
- исключение возможности использования запрещенной технологии передачи речи в информационной системе, а также разработки, приобретения и внедрения технологий передачи речи субъектам доступа (пользователям), которым не разрешено ее использование.
- Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP).

Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.8:

Требования не установлены.

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

Требования к реализации ЗИС.9

Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи видеоинформации, их анализ и реагирование на нарушения, связанные с использованием технологий передачи видеоинформации. При контроле использования технологий передачи видеоинформации должно быть обеспечено:

- определение перечня технологий (сервисов) передачи видеоинформации, разрешенных и (или) запрещенных для использования в информационной системе;
- определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи видеоинформации в соответствии с установленными ролями;
- реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи видеоинформации;
- регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи видеоинформации;
- исключение возможности использования запрещенной технологии передачи видеоинформации в информационной системе, а также разработки, приобретения и внедрения технологий передачи видеоинформации субъектов доступа (пользователям), которым не разрешено ее использование.

Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи.

Правила и процедуры контроля передачи видеоинформации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.9:

Требования не установлены.

ЗИС.10 ПОДТВЕРЖДЕНИЕ ПРОИСХОЖДЕНИЯ ИСТОЧНИКА ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ СЕТЕВЫХ АДРЕСОВ ПО СЕТЕВЫМ ИМЕНАМ ИЛИ ОПРЕДЕЛЕНИЯ СЕТЕВЫХ ИМЕН ПО СЕТЕВЫМ АДРЕСАМ

Требования к реализации ЗИС.10

В информационной системе должна обеспечиваться возможность подтверждения происхождения источника и целостности информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам, в том числе с использованием DNS-серверов. При подтверждении происхождения источника должны обеспечиваться:

- аутентификация в соответствии с ИАФ.7 и (или) ИАФ.2 сервера, являющегося источником ответов на запросы (сервер доменных имен или DNS-сервер) по определению сетевых адресов (IP-адресов) по сетевым именам (доменные имена);

- аутентификация в соответствии с ИАФ.7 и (или) ИАФ.2 сервера, являющегося источником ответов на запросы (кэширующийDNS-сервер) по определению сетевых имен (доменных имен) по сетевым адресам (IP-адресам).

Требования к усилению ЗИС.10:

1) в информационной системе должен осуществляться процесс верификации цепочки доверия между основным (корневым) и подчиненными (дочерними) доменами (например, с использованием записей ресурсов в системе доменных имен, сопоставляющих сетевое имя и сетевой адрес средств вычислительной техники и технических средств).

ЗИС.11 ОБЕСПЕЧЕНИЕ ПОДЛИННОСТИ СЕТЕВЫХ СОЕДИНЕНИЙ (СЕАНСОВ ВЗАИМОДЕЙСТВИЯ), В ТОМ ЧИСЛЕ ДЛЯ ЗАЩИТЫ ОТ ПОДМЕНЫ СЕТЕВЫХ УСТРОЙСТВ И СЕРВИСОВ

Требования к реализации ЗИС.11

В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа "человек посередине").

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.

Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3).

Требования к усилению ЗИС.11:

1) в информационной системе должно обеспечиваться признание идентификатора сеанса связи недействительным после окончания сетевого соединения;

2) в информационной системе должна осуществляться регистрация установления и разрыва сетевых соединений (сеансов взаимодействия) в целях выявления возможных инцидентов (событий безопасности);

3) в информационной системе должна осуществляться генерация и присвоение уникальных идентификаторов (одноразовых) для каждого сетевого соединения (сеанса взаимодействия) и контроль их подлинности (восприниматься должны только идентификаторы, сгенерированные информационной системой);

4) в информационной системе должно обеспечиваться обнаружение попыток повторного использования идентификаторов сетевых соединений и реагирование на эти попытки;

5) в информационной системе должна осуществляться защита от подбора идентификаторов, присваиваемых будущим сетевым соединениям (сеансам взаимодействия).

ЗИС.12 ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ ОТРИЦАНИЯ ПОЛЬЗОВАТЕЛЕМ ФАКТА ОТПРАВКИ ИНФОРМАЦИИ ДРУГОМУ ПОЛЬЗОВАТЕЛЮ

Требования к реализации ЗИС.12

Оператором должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю.

Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться:

- определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);
- обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с ЗИС.3;
- регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.

Требования к усилению ЗИС.12:

1) в информационной системе должна обеспечиваться генерация свидетельства отправления информации (например, электронной подписи);

2) в информационной системе должна обеспечиваться связь атрибутов отправителя информации в соответствии с учетом ИАФ.1 и ИАФ.6 с полями отправляемой информации (текстом сообщения);

3) в информационной системе должна быть обеспечена возможность верификации (проверки) свидетельства отправления информации;

4) в информационной системе должна быть обеспечена возможность записи и защищенного хранения в течение установленного оператором времени информации, отправленной пользователем другому пользователю.

ЗИС.13 ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ ОТРИЦАНИЯ ПОЛЬЗОВАТЕЛЕМ ФАКТА ПОЛУЧЕНИЯ ИНФОРМАЦИИ ОТ ДРУГОГО ПОЛЬЗОВАТЕЛЯ

Требования к реализации ЗИС.13

Оператором должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя.

Для исключения возможности отрицания пользователем факта получения информации должны осуществляться:

определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);

обеспечение целостности полученной информации в соответствии с ЗИС.3;

регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.

Требования к усилению ЗИС.13:

1) в информационной системе должна обеспечиваться генерация свидетельства получения информации (запрос подтверждения получения или электронная подпись);

2) в информационной системе должна быть обеспечена связь атрибутов получателя информации в соответствии с ИАФ.1 и ИАФ.6 с полями отправляемой информации (текстом сообщения);

3) в информационной системе должна быть обеспечена возможность верификации (проверки) свидетельства получения информации;

4) в информационной системе должна быть обеспечена возможность записи и защищенного хранения в течение установленного оператором времени информации, полученной пользователем

от другого пользователя.

ЗИС.14 ИСПОЛЬЗОВАНИЕ УСТРОЙСТВ ТЕРМИНАЛЬНОГО ДОСТУПА ДЛЯ ОБРАБОТКИ ИНФОРМАЦИИ

Требования к реализации ЗИС.14

Оператором для обработки информации в информационной системе должны применяться устройства терминального доступа, обладающие минимальными функциональными возможностями по обработке и хранению информации.

Применение устройств терминального доступа должно быть направлено на сосредоточение основных функций по обработке и хранению информации на серверах (в центрах обработки данных), уменьшение состава мер защиты информации, реализуемых на каждой рабочей станции, и перенос их реализации на серверы.

К таким устройствам относятся, в том числе, бездисковые рабочие станции, при использовании которых информация текущей сессии хранится в оперативной памяти или на защищенном съемном машинном носителе информации, устройства, поддерживающие технологию виртуального рабочего стола, и иные устройства.

Требования к усилению ЗИС.14:

Требования не установлены.

ЗИС.15 ЗАЩИТА АРХИВНЫХ ФАЙЛОВ, ПАРАМЕТРОВ НАСТРОЙКИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНЫХ ДАННЫХ, НЕ ПОДЛЕЖАЩИХ ИЗМЕНЕНИЮ В ПРОЦЕССЕ ОБРАБОТКИ ИНФОРМАЦИИ

Требования к реализации ЗИС.15

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, 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.

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.

Требования к усилению ЗИС.15:

1) оператором для обеспечения конфиденциальности и целостности архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, в соответствии с законодательством Кыргызской Республики применяются криптографические (шифровальные) средства защиты информации (данных);

2) использование не перезаписываемых носителей или носителей с защищенной областью памяти для размещения (хранения) параметров настройки средств защиты информации и программного

обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.

ЗИС.16 ВЫЯВЛЕНИЕ, АНАЛИЗ И БЛОКИРОВАНИЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В ОБХОД РЕАЛИЗОВАННЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ ВНУТРИ РАЗРЕШЕННЫХ СЕТЕВЫХ ПРОТОКОЛОВ

Требования к реализации ЗИС.16

Оператором должны выполняться мероприятия по выявлению и анализу скрытых каналов передачи информации для определения параметров передачи информации, которые могут использоваться для скрытого хранения информации и скрытой передачи информации за пределы информационной системы.

Выявление и анализ скрытых каналов передачи информации осуществляется на этапах разработки и реализации системы защиты информации.

Требования к усилению ЗИС.16:

Требования не установлены.

ЗИС.17 РАЗБИЕНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА СЕГМЕНТЫ (СЕГМЕНТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ) И ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРИМЕТРОВ СЕГМЕНТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ЗИС.17

Оператором должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

Сегментирование информационной системы проводится с целью построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах. Принципы сегментирования информационной системы определяются оператором с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента.

Сегментирование информационной системы также может проводиться с целью разделения информационной системы на сегменты, имеющие различные классы защищенности информационной системы.

При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с УПД.3 и ЗИС.23.

Требования к усилению ЗИС.17:

1) оператором осуществляется выделение сегментов информационной системы для размещения общедоступной (публичной) информации:

а) путем выделения отдельных физических сетевых интерфейсов коммуникационного оборудования и (или) средств защиты периметра;

б) путем физической изоляции сегментов информационной системы для размещения общедоступной (публичной) информации.

ЗИС.18 ОБЕСПЕЧЕНИЕ ЗАГРУЗКИ И ИСПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ДОСТУПНЫХ ТОЛЬКО ДЛЯ ЧТЕНИЯ, И КОНТРОЛЬ ЦЕЛОСТНОСТИ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Требования к реализации ЗИС.18

В информационной системе должно обеспечиваться:

- выделение в составе операционной системы и прикладного программного обеспечения частей, немодифицируемых в процессе загрузки и выполнения, и размещение их на машинных носителях информации, доступных только для чтения;
- загрузка и выполнение на средствах вычислительной техники, определяемых оператором, операционной системы с машинных носителей информации, доступных только для чтения;
- загрузка и выполнение на средствах вычислительной техники прикладного программного обеспечения, определяемого оператором, с машинных носителей информации, доступных только для чтения.

В качестве машинных носителей информации, доступных только для чтения, рассматриваются, в том числе, оптические носители CD-R/DVD-R или иные аппаратные машинные носители информации, возможность перезаписи на которые исключена технологически.

Требования к усилению ЗИС.18:

1) в сегментах (компонентах) информационной системы, определяемых оператором, применяются не перезаписываемые (защищенные от записи) машинные носители информации, устойчивые к сбоям в программном обеспечении информационной системы и отключению питания;

2) оператором должен осуществляться контроль целостности программного обеспечения, записанного на машинные носители информации, доступные только для чтения, в соответствии с ОЦЛ.1.

ЗИС.19 ИЗОЛЯЦИЯ ПРОЦЕССОВ (ВЫПОЛНЕНИЕ ПРОГРАММ) В ВЫДЕЛЕННОЙ ОБЛАСТИ ПАМЯТИ

Требования к реализации ЗИС.19

В информационной системе должна осуществляться изоляция процессов (выполнение программ) в выделенной области памяти.

Изоляция процессов (выполнение программ) в выделенной области памяти должна обеспечивать недоступность областей памяти, используемых процессами (программами) выполняемыми от имени одного пользователя (учетной записи), для процессов (программ), исполняемых от имени другого пользователя (учетной записи).

Изоляция процессов (выполнение программ) в выделенной области памяти реализуется в средствах вычислительной техники, определенных оператором, и как минимум должна включать изоляцию процессов, связанных с выполнением функций безопасности средств защиты информации.

Требования к усилению ЗИС.19:

Требования не установлены.

ЗИС.20 ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ, ПРИМЕНЯЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации ЗИС.20

Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе. Защита беспроводных соединений включает:

ограничение на использование в информационной системе беспроводных соединений (в частности 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) информационной системы, для решения которых такие соединения необходимы;

предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администраторам информационной системы;

обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);

регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

При обеспечении защиты беспроводных соединений в зависимости от их типов должны реализовываться меры по идентификации и аутентификации в соответствии с ИАФ.1, ИАФ.2 и ИАФ.6.

При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с УПД.13 и ЗИС.3.

Правила и процедуры применения беспроводных соединений регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.20:

1) оператором для защиты беспроводных соединений должны применяться средства криптографической защиты информации в соответствии с законодательством Кыргызской Республики;

2) в информационной системе должны применяться программно-технические средства обнаружения, анализа и блокирования несанкционированного использования беспроводных технологий и подключений к информационной системе;

3) оператором должно обеспечиваться блокирование несанкционированных беспроводных подключений к информационной системе;

4) оператором должна быть исключена возможность установления беспроводных соединений из-за пределов контролируемой зоны.

14. **ВЫЯВЛЕНИЕ ИНЦИНДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ (ИНЦ)**

ИНЦ.1 ОПРЕДЕЛЕНИЕ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ВЫЯВЛЕНИЕ ИНЦИНДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ

Требования к реализации ИНЦ.1

Оператором должны быть назначены лица ответственные за организацию работ по отслеживанию инцидентов при обработке персональных данных и реагированию на эти инциденты. Должен производиться анализ инцидентов и принятие мер по устранению и предупреждению инцидентов.

Требования к усилению ИНЦ.1:

Требования не установлены.

ИНЦ.2 ОБНАРУЖЕНИЕ, ИДЕНТИФИКАЦИЯ И РЕГИСТРАЦИЯ ИНЦИДЕНТОВ

Требования к реализации ИНЦ.2:

Меры по выявлению инцидентов должны обеспечивать своевременное обнаружение и проведение идентификации и его регистрацию с указанием даты, времени, места обнаружения и краткой характеристики инцидента.

Требования к усилению ИНЦ.2:

Требования не установлены.

ИНЦ.3 СВОЕВРЕМЕННОЕ ИНФОРМИРОВАНИЕ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ, О ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПОЛЬЗОВАТЕЛЯМИ И АДМИНИСТРАТОРАМИ

Требования к реализации ИНЦ.3

Пользователи и администраторы информационной системы должны незамедлительно информировать о любом случае нарушения порядка обработки персональных данных или возникновения нештатных ситуаций при их обработке ответственных лиц.

Требования к усилению ИНЦ.3:

Требования не установлены.

ИНЦ.4 АНАЛИЗ ИНЦИДЕНТОВ, В ТОМ ЧИСЛЕ ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ И ПРИЧИН ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ, А ТАКЖЕ ОЦЕНКА ИХ ПОСЛЕДСТВИЙ

Требования к реализации ИНЦ.4

Лица ответственные за организацию работ по отслеживанию инцидентов проводят анализ ситуации, условия и причины возникновения инцидента, устанавливает последствия инцидента и производит оценку этих последствий.

Требования к усилению ИНЦ.4:

1. для детализации анализа или оценки последствий и нанесенного ущерба привлекаются специалисты, в том числе из сторонних организаций.

ИНЦ.5 ПРИНЯТИЕ МЕР ПО УСТРАНЕНИЮ ПОСЛЕДСТВИЙ ИНЦИДЕНТОВ

Требования к реализации ИНЦ.5

По результатам проведенного анализа инцидента принимаются конкретные меры по устранению последствий инцидента.

Требования к усилению ИНЦ.5:

Требования не установлены.

ИНЦ.6 ПЛАНИРОВАНИЕ И ПРИНЯТИЕ МЕР ПО ПРЕДОТВРАЩЕНИЮ ПОВТОРНОГО ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ

Требования к реализации ИНЦ.6

По результатам проведенного анализа инцидента ответственными лицами разрабатываются меры по предотвращению или повторению подобных инцидентов.

Требования к усилению ИНЦ.6:

Требования не установлены

15. **УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (УКФ)**

УКФ.1 ОПРЕДЕЛЕНИЕ ЛИЦ, КОТОРЫМ РАЗРЕШЕНЫ ДЕЙСТВИЯ ПО ВНЕСЕНИЮ ИЗМЕНЕНИЙ В КОНФИГУРАЦИЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Требования к реализации УКФ.1

Оператором ИСПД должны быть определены лица наделенные правом внесения соответствующих изменений в конфигурацию ИСПД и системы защиты персональных данных.

Требования к усилению УКФ.1:

Требования не установлены.

УКФ.2 УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ КОНФИГУРАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Требования к реализации УКФ.2

Управление конфигурацией информационной системы возлагается на администраторов системы, а управление системой защиты персональных данных осуществляется администраторами безопасности ИСПД, которые несут ответственность за действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей. Совмещение этих функций одним лицом не допускается.

Требования к усилению УКФ.2:

Требования не установлены.

УКФ.3 АНАЛИЗ ПОТЕНЦИАЛЬНОГО ВОЗДЕЙСТВИЯ ПЛАНИРУЕМЫХ ИЗМЕНЕНИЙ В КОНФИГУРАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И СОГЛАСОВАНИЕ ИЗМЕНЕНИЙ В КОНФИГУРАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ДОЛЖНОСТНЫМ ЛИЦОМ (РАБОТНИКОМ) ОТВЕТСТВЕННЫМ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Требования к реализации УКФ.3

Любые изменения конфигурации информационной системы и системы защиты информации должны быть санкционированными на выполнение этих изменений. Каждое изменение конфигурации информационной системы и системы защиты информации в обязательном порядке оформляется запросом на изменение, который проходит процедуру согласования и одобрения должностными лицами. В зависимости от масштаба изменения решение может приниматься на разных уровнях управления организации. Все изменения должны в обязательном порядке быть зарегистрированы процессом управления конфигурацией.

Требования к усилению УКФ.3:

Требования не установлены.

УКФ.4 ДОКУМЕНТИРОВАНИЕ ИНФОРМАЦИИ (ДАННЫХ) ОБ ИЗМЕНЕНИЯХ В КОНФИГУРАЦИИ

ИНФОРМАЦИОННОЙ СИСТЕМЫ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Требования к реализации УКФ.4

Все изменения конфигурации информационной системы и системы защиты информации должны в обязательном порядке быть зарегистрированы процессом управления конфигурацией.

Требования к усилению УКФ.4:

1. При необходимости должна производиться архивация изменений конфигурации информационной системы и системы защиты информации.

Приложение 2

к Приказу ГКИТиС КР

от _____№_____

ТИПОВОЙ ПЕРЕЧЕНЬ

УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание

Обозначения и сокращения

АРМ – автоматизированное рабочее место

ВИ – видовая информация

ВТСС – вспомогательные технические средства и системы

ИСПД – информационная система персональных данных

НСД – несанкционированный доступ

ПД – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

СЗИ – средство защиты информации

УБПД – угрозы безопасности персональных данных

1. Термины и определения

Для целей настоящего Типового перечня используются следующие термины и понятия:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. **Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или)

сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей обработчика и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения обработчиком или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Обработчик – физическое или юридическое лицо, определяемое держателем (обладателем) персональных данных, которое осуществляет обработку персональных данных на основании заключенного с ним договора.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми

добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения

Настоящий «Типовой перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Типовой перечень) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПД), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Типовой перечень содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПД), связанным:

- с перехватом (съемом) ПД по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПД с целью изменения, копирования, неправомерного распространения ПД или деструктивных воздействий на элементы ИСПД и обрабатываемых в них ПД с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПД.

Настоящий Типовой перечень применяется совместно с банком данных угроз безопасности информации сформированным Государственным комитетом информационных технологий и связи Кыргызской Республики (далее – ГКИТиС КР) (**ict.gov.kg**), а также Методикой определения угроз безопасности в информационных системах персональных данных.

Типовой перечень является методическим документом и предназначен для государственных и муниципальных органов, юридических и (или) физических лиц (далее – обработчиков), организующих и (или) осуществляющих обработку ПД, а также определяющих цели и содержание обработки ПД, заказчиков и разработчиков ИСПД и их подсистем. С применением Типового перечня решаются следующие задачи:

- разработка отраслевых перечней угроз безопасности ПД в конкретных ИСПД с учетом

их назначения, условий и особенностей функционирования;
- анализ защищенности ИСПД от угроз безопасности ПД в ходе организации и выполнения работ по обеспечению безопасности ПД;
- разработка системы защиты ПД, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПД, предусмотренных для соответствующего класса ИСПД;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПД, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

В Типовом перечне дано обобщенное описание ИСПД как объектов защиты, возможных источников угрозы безопасности персональных данных (УБПД), основных классов уязвимостей ИСПД, возможных видов деструктивных воздействий на ПД, а также основных способов их реализации. Угрозы безопасности ПД, обрабатываемых в ИСПД, содержащиеся в настоящем Типовом перечне, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПД в ИСПД. Внесение изменений в Типовой перечень осуществляется ГКИТиС КР.

3. Классификация угроз безопасности персональных данных

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

Совокупность таких условий и факторов формируется с учетом характеристик ИСПД, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПД, обусловливающим возникновение УБПД, можно отнести категорию и объем обрабатываемых в ИСПД персональных данных, актуальности угроз, возможности нанесения ущерба, продолжительности обработки персональных данных, структуру ИСПД, наличие подключений ИСПД к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПД, обрабатываемых в ИСПД, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПД, местонахождение и условия размещения технических средств ИСПД.

Информационные системы ПД представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПД.

Основными элементами ИСПД являются:

1. персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПД;
2. информационные технологии, применяемые при обработке ПД;
3. технические средства, осуществляющие обработку ПД (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее – технические средства ИСПД);

4. программные средства (операционные системы, системы управления базами данных и т.п.);
5. средства защиты информации;
6. вспомогательные технические средства и системы (ВТСС) – технические средства и системы, их коммуникации, не предназначенные для обработки ПД, но размещенные в помещениях (далее – служебные помещения), в которых расположены ИСПД, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПД, и определяются при оценке возможности реализации УБПДн\.

Возможности источников УБПД обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПД, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПД.

Угроза безопасности ПД реализуется в результате образования канала реализации УБПД между источником угрозы и носителем (источником) ПД, что создает условия для нарушения безопасности ПД (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПД (рисунок 1) являются:

1. источник УБПД – субъект, материальный объект или физическое явление, создающие УБПДн;

2. среда (путь) распространения ПД или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПД;

3. носитель ПД – физическое лицо или материальный объект, в том числе физическое поле, в котором ПД находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Рисунок 1. Обобщенная схема канала реализации угроз безопасности ПД

Носители ПД могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПД при осуществлении им функции голосового ввода ПД в ИСПД, либо воспроизводимая акустическими средствами ИСПД (если такие функции предусмотрены технологией обработки ПД), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

- видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации;

- средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПД;

- информация, обрабатываемая (циркулирующая) в ИСПД, в виде электрических, электромагнитных, оптических сигналов;

- информация, обрабатываемая в ИСПД, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПД при их обработке в ИСПД и разработке на их основе отраслевых перечней применительно к конкретному виду ИСПД угрозы классифицируются в соответствии со следующими признаками (рисунок 2):

- по виду защищаемой от УБПД информации, содержащей ПД;

- по видам возможных источников УБПД;

- по типу ИСПД, на которые направлена реализация УБПД;

- по способу реализации УБПД;

- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПД);

- по используемой уязвимости;

- по объекту воздействия.

По видам возможных источников УБПД выделяются следующие классы угроз:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПД, включая пользователей ИСПД, реализующих угрозы непосредственно в ИСПД (внутренний нарушитель);

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПД, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПД, на которые направлена реализация УБПД, выделяются следующие классы угроз:

- угрозы безопасности ПД, обрабатываемых в ИСПД на базе автономного автоматизированного рабочего места (АРМ);

- угрозы безопасности ПД, обрабатываемых в ИСПД на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

- угрозы безопасности ПД, обрабатываемых в ИСПД на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

- угрозы безопасности ПД, обрабатываемых в ИСПД на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

- угрозы безопасности ПД, обрабатываемых в ИСПД на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

- угрозы безопасности ПД, обрабатываемых в ИСПД на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

Рисунок 2. Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных

По способам реализации УБПД выделяются следующие классы угроз:

- угрозы, связанные с НСД к ПД (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПД по техническим каналам утечки информации;

- угрозы специальных воздействий на ИСПД.

По виду несанкционированных действий, осуществляемых с ПД, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПД (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПД или их уничтожение;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПД, в результате которого осуществляется блокирование ПД.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного ПО; угрозы, реализуемые с использованием уязвимости прикладного ПО;

- угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;

- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

- угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПД, обрабатываемых на АРМ;

- угрозы безопасности ПД, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

- угрозы безопасности ПД, передаваемых по сетям связи;

- угрозы прикладным программам, с помощью которых обрабатываются ПД;

-угрозы системному ПО, обеспечивающему функционирование ИСПД.

Реализация одной из УБПД перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПД:

-значительным негативным последствиям для субъектов ПД;

-негативным последствиям для субъектов ПД;

-незначительным негативным последствиям для субъектов ПД.

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

Угрозы, связанные с несанкционированным доступом (НСД) (далее – угрозы НСД в ИСПД), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПД, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПД или самих ПД) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

угроза НСД: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

4. Угрозы утечки информации по техническим каналам

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПД, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения, может быть, как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем ПД является пользователь ИСПД, осуществляющий голосовой ввод ПД в ИСПД, акустическая система ИСПД, воспроизводящая ПД, а также технические средства ИСПД 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 ПД в ИСПД за счет реализации технических каналов утечки информации возможно возникновение следующих УБПД:

- угроз утечки акустической (речевой) информации; - - угроз утечки видовой информации;

- угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПД, при обработке ПД в ИСПД, обусловлено наличием функций голосового ввода ПД в ИСПД или функций воспроизведения ПД акустическими средствами ИСПД.

Перехват акустической (речевой) информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки ПДн, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки ПД, ВТСС и помещения или подключенных к каналам связи.

Угрозы безопасности ПД, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации («закладочных устройств»), определяются в соответствии с нормативным документами Государственного комитета национальной безопасности Кыргызской Республики (далее – ГКНБ КР) в установленном ею порядке.

Перехват акустической (речевой) информации может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях

(зданиях) с неконтролируемым пребыванием посторонних лиц;

- портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

- портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;

- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

2. Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПД с помощью оптических (оптикоэлектронных) 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 ИСПД.

Кроме этого, просмотр (регистрация) ПД возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Угрозы безопасности ПД, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видеозакладок), определяются в соответствии с нормативным документами ГКНБ КР в установленном ею порядке.

Необходимым условием осуществления просмотра (регистрации) ПД является наличие прямой видимости между средством наблюдения и носителем ПД.

Перехват ПД может вестись:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

- портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

- портативной носимой аппаратурой – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

Перехват (просмотр) ПД может осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов ИСПД с использованием оптических (оптикоэлектронных) средств.

3. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Возникновение угрозы ПД по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПД) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПД.

Генерация информации, содержащей ПД и циркулирующей в технических средствах ИСПД в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПД сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПД.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, обрабатывающих ПД (в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПД, в том числе в средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео- и буквенно-цифровой информации).

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПД.

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с

неконтролируемым пребыванием посторонних лиц;

- портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

- портативной носимой аппаратурой – физическими лицами в непосредственной близости от ИСПД;

- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПД.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПД и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений технических средств ИСПД возникают при излучении элементами технических средств ИСПД информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПД, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информативный сигнал.

Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств ИСПД и цепей питания.

Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе аппаратуры ТСПИ и цепей заземления.

Для съема информации с проводных линий могут использоваться:

- средства съема сигналов, содержащих защищаемую информацию, с

цепей технических средств ИСПД и ВТСС, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты

сети, токовые трансформаторы, пробники);

- средства съема наведенных информативных сигналов с цепей электропитания;

- средства съема наведенных информативных сигналов с шин заземления;

- средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций.

Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна.

Появление новых каналов связи – сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных – привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:

- перехвата пейджинговых сообщений и сотовой связи;

- перехвата информации в каналах передачи данных вычислительных сетей.

5. Угрозы несанкционированного доступа к информации в информационной системе

персональных данных

Угрозы НСД в ИСПД с применением программных и программно- аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПД, 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.п.;

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

Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПД с использованием штатного программного обеспечения разделяются 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.

Эти угрозы реализуются относительно ИСПД как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПД, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза НСД в ИСПД: = <источник угрозы>, <уязвимость ИСПД>,

<способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Угрозы создания нештатных режимов работы программных (программно- аппаратных) средств – это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к ИСПД на базе локальных и распределенных информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;

- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);

- форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);

- программного обеспечения обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др.

Описание таких угроз формально может быть представлено следующим образом:

угроза «Отказа в обслуживании»: = <источник угрозы>,

<уязвимость ИСПД>, <способ реализации угрозы>, <объект воздействия (носитель ПД)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т.п.)>.

Угрозы внедрения вредоносных программ (программно- математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что, во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации защиты информации на практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования). В связи с этим угрозы программно-математического воздействия (ПМВ) формально могут быть представлены следующим образом:

угроза ПМВ в ИСПД: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>,

<способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т.п.)>, <описание возможных деструктивных действий>,<дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

Приложение 3

к Приказу ГКИТиС КР

от _____№_____

Форма

Перечень угроз

_____

(наименование держателя (обладателя) массива персональных данных)

определил следующие угрозы безопасности персональных данных, обрабатываемых в

_____

(наименование информационной системы или группы систем)

№ п/п	Наименование или краткое описание угрозы	Рейтинг по критериям, баллов					
		1	2	3	4	5	Произведение

1.							
2.							
…							

Требуемый уровень защищенности персональных данных при их обработке в информационной системе (информационных системах): _____.

Уполномоченное должностное лицо держателя (обладателя) массива персональных данных, подпись, печать, дата подписания.