**Приложение 3**

**Предложения по внесению изменений в приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении требований по обеспечению значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – Приказ) в части формирования проектной и эксплуатационной документации на значимые объекты критической информационной инфраструктуры (КИИ), определения мер по обеспечению безопасности значимых объектов КИИ в зависимости от вида значимого объекта КИИ и применения риск-ориентированного подхода в реализации процедур выполнения задач по обеспечению безопасности значимых объектов КИИ.**

1. **Пункт 10 Приказа изложить в следующей редакции:**

«Задание требований к обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, устанавливающим требования к обеспечению безопасности значимых объектов, в соответствии **видом и** категорией значимости значимого объекта, определенной в порядке, установленном [Правилами](http://ivo.garant.ru/document/redirect/71876120/1000) категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными [постановлением](http://ivo.garant.ru/document/redirect/71876120/0) Правительства Российской Федерации от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

Требования к обеспечению безопасности включаются в техническое задание на создание значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, **и (или) в состав иной документации на создаваемый объект, порядок и форма ведения которых предусмотрена организационно-распорядительными документами субъекта критической информационной инфраструктуры,** которые должны содержать:

а) цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;

б) категорию значимости значимого объекта **(предварительно установленную категорию значимости)**;

**в) вид значимого объекта;**

**г)** перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;

**д)** перечень типов объектов защиты значимого объекта;

**е)** требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта;

**ж)** стадии (этапы работ) создания подсистемы безопасности значимого объекта **и (или) порядок реализации организационных и технических мер, применяемых для обеспечения безопасности значимого объекта**;

**з)** требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;

**и)** требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями;

**к)** требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта.

В случае если значимый объект создается в рамках объекта капитального строительства, требования к обеспечению безопасности значимого объекта задаются застройщиком и оформляются в виде приложения к заданию на проектирование (реконструкцию) объекта капитального строительства.

При определении требований к обеспечению безопасности значимого объекта учитываются положения организационно-распорядительных документов по обеспечению безопасности значимых объектов, разрабатываемых субъектами критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с [пунктом 4 части 3 статьи 6](http://ivo.garant.ru/document/redirect/71730198/1330) Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - организационно-распорядительные документы по безопасности значимых объектов).».

1. **Пункт 11 Приказа изложить в следующей редакции:**

«Разработка организационных и технических мер по обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по созданию (модернизации) значимого объекта и (или) обеспечению его безопасности, в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта и должна включать:

а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);

б) проектирование подсистемы безопасности значимого объекта **и (или) формирование порядка реализации организационных и технических требований по обеспечению безопасности значимого объекта критической информационной инфраструктуры;**

в) разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности) **и (или) уточнение содержания имеющейся эксплуатационной документации.**

Разрабатываемые организационные и технические меры по обеспечению безопасности значимого объекта не должны оказывать негативного влияния на создание и функционирование значимого объекта.».

1. **Пункт 11.2 Приказа изложить в следующей редакции:**

«Проектирование подсистемы безопасности значимого объекта должно осуществляться в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта с учетом модели угроз безопасности информации, **вида** и категории значимости значимого объекта. **Состав, формы и порядок формирования проектной документации и (или) документации, в которой должно быть отражено содержание пп. «а» - «з» настоящего пункта, должны быть определены в организационно-распорядительных документах субъекта критической информационной инфраструктуры.**

При проектировании подсистемы безопасности значимого объекта:

а) определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;

б) определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);

в) определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта;

г) определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;

д) осуществляется выбор средств защиты информации и (или) их разработка с учетом **вида и** категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;

е) разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации. **Содержание архитектуры подсистемы безопасности может быть отображено в другой документации, разрабатываемой на объект критической информационной инфраструктуры.**

ж) определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;

В случае если в ходе проектирования подсистемы безопасности значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения.

Результаты проектирования подсистемы безопасности значимого объекта отражаются в проектной документации на значимый объект (подсистему безопасности значимого объекта), разрабатываемой в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта **и (или) иных документах, порядок ведения и формы которых определяются организационно-распорядительными документами субъекта критической информационной инфраструктуры.**

В процессе проектирования значимого объекта его категория значимости может быть уточнена.

В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды. Тестирование должно быть направлено на:

обеспечение работоспособности и совместимости выбранных средств защиты информации с программными и аппаратными средствами значимого объекта;

практическую отработку выполнения средствами защиты информации функций безопасности, а также выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в соответствии с [пунктами 27 - 31](file:///Z%3A%5Cshares%5C%D0%9A%D0%BE%D0%BC%D0%B8%D1%82%D0%B5%D1%82%D1%8B%2C%20%D1%80%D0%B3%2C%20%D1%81%D0%BE%D0%B2%D0%B5%D1%82%D1%8B%5C1_%D0%9A%D0%9E%D0%9C%D0%98%D0%A2%D0%95%D0%A2%D0%AB%5C%D0%9A%D0%BE%D0%BC%D0%B8%D1%82%D0%B5%D1%82%20%D0%BF%D0%BE%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8%5C2021%5C%D0%92%D1%81%D1%82%D1%80%D0%B5%D1%87%D0%B8%20%D1%81%20%D0%A4%D0%A1%D0%A2%D0%AD%D0%9A%5C%D0%9F%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5%202.docx#sub_49) настоящих Требований;

исключение влияния подсистемы безопасности на функционирование значимого объекта.

Макетирование подсистемы безопасности значимого объекта и ее тестирование может проводиться с использованием средств и методов моделирования, а также с использованием технологий виртуализации.

При проектировании подсистем безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями, настоящие Требования применяются с учетом [Требований](http://ivo.garant.ru/document/redirect/71689716/1000) к проектированию сетей электросвязи, утвержденных [приказом](http://ivo.garant.ru/document/redirect/71689716/0) Минкомсвязи России от 9 марта 2017 г. № 101 (зарегистрирован Минюстом России 31 мая 2017 г., регистрационный № 46915), а также иных нормативных правовых актов федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи.».

1. **Пункт 11.3 Приказа изложить в следующей редакции:**

Разработка рабочей (эксплуатационной) документации на значимый объект осуществляется в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта на основе проектной документации.

Рабочая (эксплуатационная) документация на значимый объект должна содержать:

описание архитектуры подсистемы безопасности значимого объекта;

порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;

правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

**Описание архитектуры подсистемы безопасности, порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации, правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации) могут содержаться в других документах, порядок и форма разработки и ведения которых должны определяться организационно-распорядительными документами субъекта критической информационной инфраструктуры.**

Состав и формы рабочей (эксплуатационной) документации определяются в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта **и (или) содержанием иных документов, разрабатываемых на стадии создания (модернизации) значимых объектов критической информационной инфраструктуры.**

1. **Пункт 11.3 Приказа изложить в следующей редакции:**

«Анализ уязвимостей значимого объекта проводится в целях выявления недостатков (слабостей) в подсистеме безопасности значимого объекта и оценки возможности их использования для реализации угроз безопасности информации. При этом анализу подлежат уязвимости кода, конфигурации и архитектуры значимого объекта.

Анализ уязвимостей проводится для всех программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта **в соответствии с разработанным и утвержденным субъектом критической информационной инфраструктуры процессом управления уязвимостями, содержащим как минимум следующие этапы:**

1. **мониторинг уязвимостей, оценка применимости;**
2. **оценка критичности уязвимостей;**
3. **определение методов и приоритетов устранения уязвимостей;**
4. **определение сроков устранения уязвимостей;**
5. **контроль устранения уязвимостей.**

При проведении анализа уязвимостей применяются следующие способы их выявления:

а) анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности значимого объекта;

б) анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта;

в) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством анализа состава установленного программного обеспечения и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации;

г) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности;

д) тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

Применение способов и средств выявления уязвимостей осуществляется субъектом критической информационной инфраструктуры с учетом особенностей функционирования значимого объекта.

Допускается проведение анализа уязвимостей на макете (в тестовой зоне) значимого объекта или макетах отдельных сегментов значимого объекта.

Анализ уязвимостей значимого объекта проводится до ввода его в эксплуатацию на этапах, определяемых субъектом критической информационной инфраструктуры.

В случае выявления уязвимостей значимого объекта, которые могут быть использованы для реализации (способствовать возникновению) угроз безопасности информации, **проводится оценка степени критичности уязвимостей,** принимаются меры, направленные на их устранение или исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей **и определяются сроки выполнения этих мероприятий.**

**В качестве мер, направленных на устранение выявленных уязвимостей или исключающих возможность их использования (эксплуатации) нарушителем, могут использоваться меры:**

1. **обновление программных и программно-аппаратных средств, в том числе средств защиты информации;**
2. **настройка конфигураций программных и программно-аппаратных средств, в том числе средств защиты информации;**
3. **удаление уязвимых программных средств, в том числе средств защиты информации;**
4. **компенсирующие мероприятия, при невозможности незамедлительного устранения уязвимости, исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей.**

**Допускается использование методик, разработанных и утвержденных субъектом критической информационной инфраструктуры, (в том числе отраслевых) для оценки степени критичности уязвимостей на основе риск-ориентированного подхода.**

По результатам анализа уязвимостей должно быть подтверждено, что в значимом объекте, **все выявленные** уязвимост**и**, как минимум содержащиеся в банке данных угроз безопасности информации ФСТЭК России, указанном в [пункте 11.1](#sub_12) настоящих Требований, **устраняются в соответствии с разработанным и утвержденным субъектом критической информационной инфраструктуры процессом управления уязвимостями** или выявленные уязвимости не приводят к возникновению угроз безопасности информации в отношении значимого объекта.».

1. **Пункт 22 Приказа изложить в следующей редакции:**

В значимых объектах в зависимости от их **вида и** категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры:

идентификация и аутентификация (ИАФ);

управление доступом (УПД);

ограничение программной среды (ОПС);

защита машинных носителей информации (ЗНИ);

аудит безопасности (АУД);

антивирусная защита (АВЗ);

предотвращение вторжений (компьютерных атак) (СОВ);

обеспечение целостности (ОЦЛ);

обеспечение доступности (ОДТ);

защита технических средств и систем (ЗТС);

защита информационной (автоматизированной) системы и ее компонентов (ЗИС);

планирование мероприятий по обеспечению безопасности (ПЛН);

управление конфигурацией (УКФ);

управление обновлениями программного обеспечения (ОПО);

реагирование на инциденты информационной безопасности (ИНЦ);

обеспечение действий в нештатных ситуациях (ДНС);

информирование и обучение персонала (ИПО).

Состав мер по обеспечению безопасности значимых объектов в зависимости **от вида** **и** категории значимости приведен в приложении к настоящим Требованиям.

При реализации мер по обеспечению безопасности значимых объектов применяются методические документы, разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1. **Пункт 23 Приказа изложить в следующей редакции:**

Выбор мер по обеспечению безопасности значимых объектов для их реализации включает:

а) определение базового набора мер по обеспечению безопасности значимого объекта;

б) адаптацию базового набора мер по обеспечению безопасности значимого объекта;

в) дополнение адаптированного набора мер по обеспечению безопасности значимого объекта мерами, установленными иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и защиты информации.

Базовый набор мер по обеспечению безопасности значимого объекта определяется на основе **вида и** установленной категории значимости значимого объекта в соответствии с приложением к настоящим Требованиям.

Базовый набор мер по обеспечению безопасности значимого объекта подлежит адаптации в соответствии с угрозами безопасности информации, применяемыми информационными технологиями и особенностями функционирования значимого объекта. При этом из базового набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в значимом объекте, или характеристиками, не свойственными значимому объекту. При адаптации базового набора мер по обеспечению безопасности значимого объекта для каждой угрозы безопасности информации, включенной в модель угроз, сопоставляется мера или группа мер, обеспечивающие блокирование одной или нескольких угроз безопасности или снижающие возможность ее реализации исходя из условий функционирования значимого объекта. В случае если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации, в него дополнительно включаются меры, приведенные в приложении к настоящим Требованиям.

Дополнение адаптированного набора мер по обеспечению безопасности значимого объекта осуществляется с целью выполнения требований, установленных иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры и защиты информации. Дополнение адаптированного набора мер проводится в случае, если в отношении значимого объекта в соответствии с законодательством Российской Федерации также установлены требования о защите информации, содержащейся в государственных информационных системах, требования к защите персональных данных при их обработке в информационных системах персональных данных, требования к криптографической защите информации или иные требования в области защиты информации и обеспечения безопасности критической информационной инфраструктуры.

1. **Приложение к Приказу изложить в следующей редакции:**

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

| Обозначение и номер меры | Меры обеспечения безопасности значимого объекта | **Вид** | Категория значимости |
| --- | --- | --- | --- |
| **ЗОКИИ** |
| **ИС/АС** | **ИТКС** | 3 | 2 | 1 |
| I. Идентификация и аутентификация (ИАФ) |
| ИАФ.0 | Регламентация правил и процедур идентификации и аутентификации |  | **+** | + | + | + |
| ИАФ.1 | Идентификация и аутентификация пользователей и инициируемых ими процессов | **+** |  | + | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств | **+** |  | + | + | + |
| ИАФ.3 | Управление идентификаторами | **+** |  | + | + | + |
| ИАФ.4 | Управление средствами аутентификации | **+** |  | + | + | + |
| ИАФ.5 | Идентификация и аутентификация внешних пользователей | **+** | **+** | + | + | + |
| ИАФ.6 | Двусторонняя аутентификация |  | **+** |   |   |   |
| ИАФ.7 | Защита аутентификационной информации при передаче | **+** |  | + | + | + |
| II. Управление доступом (УПД) |
| УПД.0 | Регламентация правил и процедур управления доступом | **+** | **+** | + | + | + |
| УПД.1 | Управление учетными записями пользователей | **+** | **+** | + | + | + |
| УПД.2 | Реализация модели управления доступом | **+** | **+** | + | + | + |
| УПД.3 | Доверенная загрузка | **+** |  |  | + | + |
| УПД.4 | Разделение полномочий (ролей) пользователей | **+** | **+** | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий | **+** |  | + | + | + |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему | **+** |  | + | + | + |
| УПД.7 | Предупреждение пользователя при его доступе к информационным ресурсам | **+** |  |   |   |   |
| УПД.8 | Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе | **+** |  |   |   |   |
| УПД.9 | Ограничение числа параллельных сеансов доступа | **+** |  |   |   | + |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности | **+** |  | + | + | + |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации | **+** |  | + | + | + |
| УПД.12 | Управление атрибутами безопасности | **+** |  |   |   |   |
| УПД.13 | Реализация защищенного удаленного доступа | **+** | **+** | + | + | + |
| УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем | **+** |  | + | + | + |
| III. Ограничение программной среды (ОПС) |
| ОПС.0 | Регламентация правил и процедур ограничения программной среды | **+** |   |   | + | + |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения | **+** |   |  |   | + |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения | **+** |   |   | + | + |
| ОПС.3 | Управление временными файлами | **+** |   |   |   |   |
| IV. Защита машинных носителей информации (ЗНИ) |
| ЗНИ.0 | Регламентация правил и процедур защиты машинных носителей информации | **+** |   | + | + | + |
| ЗНИ.1 | Учет машинных носителей информации | **+** |  | + | + | + |
| ЗНИ.2 | Управление физическим доступом к машинным носителям информации | **+** |  | + | + | + |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | **+** |  |   |   |   |
| ЗНИ.4 | Исключение возможности несанкционированного чтения информации на машинных носителях информации | **+** |  |   |   |   |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации | **+** |  | + | + | + |
| ЗНИ.6 | Контроль ввода (вывода) информации на съемные машинные носители информации | **+** |  |   |   | + |
| ЗНИ.7 | Контроль подключения съемных машинных носителей | **+** |  | + | + | + |
| информации |
| ЗНИ. 8 | Уничтожение (стирание) информации на машинных носителях информации | **+** |  | + | + | + |
| V. Аудит безопасности (АУД) |
| АУД.0 | Регламентация правил и процедур аудита безопасности | **+** | **+** | + | + | + |
| АУД.1 | Инвентаризация информационных ресурсов | **+** | **+** | + | + | + |
| АУД.2 | Анализ уязвимостей и их устранение | **+** | **+** | + | + | + |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени | **+** | **+** | + | + | + |
| АУД.4 | Регистрация событий безопасности | **+** | **+** | + | + | + |
| АУД.5 | Контроль и анализ сетевого трафика |  | **+** |   |   | + |
| АУД.6 | Защита информации о событиях безопасности | **+** | **+** | + | + | + |
| АУД.7 | Мониторинг безопасности | **+** | **+** | + | + | + |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности | **+** | **+** | + | + | + |
| АУД.9 | Анализ действий отдельных пользователей | **+** | **+** |   |   | + |
| АУД.10 | Проведение внутренних аудитов | **+** | **+** | + | + | + |
| АУД.11 | Проведение внешних аудитов | **+** | **+** |   |   |   |
| VI. Антивирусная защита (АВЗ) |
| АВЗ.0 | Регламентация правил и процедур антивирусной защиты | **+** |   | + | + | + |
| АВЗ.1 | Реализация антивирусной защиты | **+** |   | + | + | + |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов | **+** |   | + | + | + |
| АВЗ.3 | Контроль использования архивных, исполняемых и зашифрованных файлов | **+** |   |   |   | + |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | **+** |   | + | + | + |
| АВЗ.5 | Использование средств антивирусной защиты различных производителей | **+** |   |   |   | + |
| VII. Предотвращение вторжений (компьютерных атак) (СОВ) |
| СОВ.0 | Регламентация правил и процедур предотвращения вторжений (компьютерных атак) | **+** | **+** |   | + | + |
| СОВ.1 | Обнаружение и предотвращение компьютерных атак | **+** | **+** |  | + | + |
| СОВ.2 | Обновление базы решающих правил | **+** | **+** |   | + | + |
| VIII. Обеспечение целостности (ОЦЛ) |
| ОЦЛ.0 | Регламентация правил и процедур обеспечения целостности | **+** |  | + | + | + |
| ОЦЛ.1 | Контроль целостности программного обеспечения | **+** | **+** | + | + | + |
| ОЦЛ.2 | Контроль целостности информации | **+** |  |   |   |   |
| ОЦЛ.3 | Ограничения по вводу информации в информационную (автоматизированную) систему | **+** |  |   |   | + |
| ОЦЛ.4 | Контроль данных, вводимых в информационную (автоматизированную) систему | **+** |  |   | + | + |
| ОЦЛ.5 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | **+** |  |   | + | + |
| ОЦЛ.6 | Обезличивание и (или) деидентификация информации | **+** |  |   |   |   |
| IX. Обеспечение доступности (ОДТ) |
| ОДТ.0 | Регламентация правил и процедур обеспечения доступности | **+** | **+** | + | + | + |
| ОДТ.1 | Использование отказоустойчивых технических средств | **+** | **+** |   | + | + |
| ОДТ.2 | Резервирование средств и систем | **+** | **+** |  | + | + |
| ОДТ.3 | Контроль безотказного функционирования средств и систем | **+** | **+** |   | + | + |
| ОДТ.4 | Резервное копирование информации | **+** |  | + | + | + |
| ОДТ.5 | Обеспечение возможности восстановления информации | **+** |  | + | + | + |
| ОДТ.6 | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях | **+** | **+** | + | + | + |
| ОДТ.7 | Кластеризация информационной (автоматизированной) системы | **+** | **+** |   |   |   |
| ОДТ.8 | Контроль предоставляемых вычислительных ресурсов и каналов связи | **+** | **+** | + | + | + |
| X. Защита технических средств и систем (ЗТС) |
| ЗТС.0 | Регламентация правил и процедур защиты технических средств и систем | **+** | **+** | + | + | + |
| ЗТС.1 | Защита информации от утечки по техническим каналам | **+** | **+** |  |   |   |
| ЗТС.2 | Организация контролируемой зоны | **+** | **+** | + | + | + |
| ЗТС.3 | Управление физическим доступом | **+** | **+** | + | + | + |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | **+** |  | + | + | + |
| ЗТС.5 | Защита от внешних воздействий | **+** | **+** | + | + | + |
| ЗТС.6 | Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации | **+** | **+** |   |   |   |
|  XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) |
| ЗИС.0 | Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов | **+** | **+** | + | + | + |
| ЗИС.1 | Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями | **+** | **+** | + | + | + |
| ЗИС.2 | Защита периметра информационной (автоматизированной) системы | **+** | **+** | + | + | + |
| ЗИС.3 | Эшелонированная защита информационной (автоматизированной) системы | **+** | **+** | + | + | + |
| ЗИС.4 | Сегментирование информационной (автоматизированной) системы | **+** | **+** |   | + | + |
| ЗИС.5 | Организация демилитаризованной зоны |  | **+** | + | + | + |
| ЗИС.6 | Управление сетевыми потоками |   | **+** | + | + | + |
| ЗИС.7 | Использование эмулятора среды функционирования программного обеспечения ("песочница") | + |   |  |   |   |
| ЗИС.8 | Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы | + | + | + | + | + |
| ЗИС.9 | Создание гетерогенной среды | + | + |   |   |   |
| ЗИС.10 | Использование программного обеспечения, функционирующего в средах различных операционных систем | + |   |  |   |   |
| ЗИС.11 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | + |   |   |   |   |
| ЗИС.12 | Изоляция процессов (выполнение программ) в выделенной области памяти | + |   |   |   |   |
| ЗИС.13 | Защита неизменяемых данных | + |   |   | + | + |
| ЗИС.14 | Использование неперезаписываемых машинных носителей информации | + |   |   |   |   |
| ЗИС.15 | Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек | + |   |   |   |   |
| ЗИС.16 | Защита от спама | + |   |   | + | + |
| ЗИС.17 | Защита информации от утечек | + | + |   |   |   |
| ЗИС.18 | Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию |   | + |   |   |   |
| ЗИС.19 | Защита информации при ее передаче по каналам связи |   | + | + | + | + |
| ЗИС.20 | Обеспечение доверенных канала, маршрута |   | + | + | + | + |
| ЗИС.21 | Запрет несанкционированной удаленной активации периферийных устройств | + |   | + | + | + |
| ЗИС.22 | Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами | + |   |   |   |   |
| ЗИС.23 | Контроль использования мобильного кода | + |   |   |   |   |
| ЗИС.24 | Контроль передачи речевой информации | + |   |   |   |   |
| ЗИС.25 | Контроль передачи видеоинформации | + | + |   |   |   |
| ЗИС.26 | Подтверждение происхождения источника информации |   | + |  |   |   |
| ЗИС.27 | Обеспечение подлинности сетевых соединений |   | + |   | + | + |
| ЗИС.28 | Исключение возможности отрицания отправки информации | + | + |   |   |   |
| ЗИС.29 | Исключение возможности отрицания получения информации | + | + |   |   |   |
| ЗИС.30 | Использование устройств терминального доступа | + | + |  |   |   |
| ЗИС.31 | Защита от скрытых каналов передачи информации |   | + |   |   |   |
| ЗИС.32 | Защита беспроводных соединений |   | + | + | + | + |
| ЗИС.33 | Исключение доступа через общие ресурсы | + |   |   |   | + |
| ЗИС.34 | Защита от угроз отказа в обслуживании (DOS, DDOS-атак) |   | + | + | + | + |
| ЗИС.35 | Управление сетевыми соединениями |   | + | + | + | + |
| ЗИС.36 | Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем | + |   |  |   |   |
| ЗИС.37 | Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев) | + |   |   |   |   |
| ЗИС.38 | Защита информации при использовании мобильных устройств | + | + | + | + | + |
| ЗИС.39 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | + |   | + | + | + |
| XII. Реагирование на компьютерные инциденты (ИНЦ) |
| ИНЦ.0 | Регламентация правил и процедур реагирования на компьютерные инциденты | + | + | + | + | + |
| ИНЦ.1 | Выявление компьютерных инцидентов | + | + | + | + | + |
| ИНЦ.2 | Информирование о компьютерных инцидентах | + | + | + | + | + |
| ИНЦ.3 | Анализ компьютерных инцидентов | + | + | + | + | + |
| ИНЦ.4 | Устранение последствий компьютерных инцидентов | + | + | + | + | + |
| ИНЦ.5 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов | + | + | + | + | + |
| ИНЦ.6 | Хранение и защита информации о компьютерных инцидентах | + | + | + | + | + |
| XIII. Управление конфигурацией (УКФ) |
| УКФ.0 | Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы | + |   | + | + | + |
| УКФ.1 | Идентификация объектов управления конфигурацией | + | + |  |   |   |
| УКФ.2 | Управление изменениями | + | + | + | + | + |
| УКФ.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения | + | + | + | + | + |
| УКФ.4 | Контроль действий по внесению изменений | + | + |   |   |   |
| XIV. Управление обновлениями программного обеспечения (ОПО) |
| ОПО.0 | Регламентация правил и процедур управления обновлениями программного обеспечения | + | + | + | + | + |
| ОПО.1 | Поиск, получение обновлений программного обеспечения от доверенного источника | + | + | + | + | + |
| ОПО.2 | Контроль целостности обновлений программного обеспечения | + | + | + | + | + |
| ОПО.3 | Тестирование обновлений программного обеспечения | + | + | + | + | + |
| ОПО.4 | Установка обновлений программного обеспечения | + | + | + | + | + |
| XV. Планирование мероприятий по обеспечению безопасности (ПЛН) |
| ПЛН.0 | Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации | + | + | + | + | + |
| ПЛН.1 | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации | + | + | + | + | + |
| ПЛН.2 | Контроль выполнения мероприятий по обеспечению защиты информации | + | + | + | + | + |
| XVI. Обеспечение действий в нештатных ситуациях (ДНС) |
| ДНС.0 | Регламентация правил и процедур обеспечения действий в нештатных ситуациях | + | + | + | + | + |
| ДНС.1 | Разработка плана действий в нештатных ситуациях | + | + | + | + | + |
| ДНС.2 | Обучение и отработка действий персонала в нештатных ситуациях | + | + | + | + | + |
| ДНС.3 | Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций | + | + |   | + | + |
| ДНС .4 | Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций | + | + |   | + | + |
| ДНС.5 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций | + | + | + | + | + |
| ДНС.6 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения | + | + | + | + | + |
| XVII. Информирование и обучение персонала (ИПО) |
| ИПО.0 | Регламентация правил и процедур информирования и обучения персонала | + | + | + | + | + |
| ИПО.1 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы | + | + | + | + | + |
| ИПО.2 | Обучение персонала правилам безопасной работы | + | + | + | + | + |
| ИПО.3 | Проведение практических занятий с персоналом по правилам | + | + |   | + | + |
| безопасной работы |
| ИПО.4 | Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы | + | + | + | + | + |

"+" - мера обеспечения безопасности включена в базовый набор мер для соответствующей категории значимого объекта.

Меры обеспечения безопасности, не обозначенные знаком "+", применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер в значимом объекте критической информационной инфраструктуры соответствующей категории значимости.