Муниципальное казенное общеобразовательное учреждение
«Гимназия»

УТВЕРЖДАЮ:
Директор МКОУ «Гимназия»
Борщевцева Г.А.
Приказ № 2 от
«21» января 2015 г.

Положение о Политике МКОУ «Гимназия» в области обработки персональных данных

Содержание

1. Общие положения

Политика обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных разработана в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах.

Требования являются обязательными при защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), содержащейся в государственных информационных системах, создаваемых и эксплуатируемых на территории Российской Федерации, а также в муниципальных информационных системах, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

Требования могут применяться для защиты информации, содержащейся в негосударственных информационных системах, а также для защиты общедоступной информации, содержащейся в государственных информационных системах.

Требования предназначены для обладателей информации, заказчиков, заключивших государственный контракт на создание государственной информационной системы (далее – заказчики), операторов государственных информационных систем (далее – операторы), а также лиц, привлекаемых обладателями информации, заказчиками или операторами в соответствии с законодательством Российской Федерации к проведению работ по защите информации, содержащейся в государственных информационных системах.

При обработке в государственной информационной системе (далее - информационная система) информации, содержащей персональные данные, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, установленных в соответствии с пунктом 2 части 3 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».Защита информации, содержащейся в информационных системах, обеспечивается путем принятия обладателями информации (заказчиками) и операторами (уполномоченными лицами) правовых, организационных и технических мер (далее – меры защиты информации), направленных на:

обеспечение защиты информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования,

предоставления и распространения, а также от иных неправомерных действий в отношении информации;

соблюдение конфиденциальности информации;

реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

Лица, обрабатывающие информацию, содержащуюся в информационной системе (государственный информационный ресурс), по поручению оператора или заказчика этой информационной системы и (или) предоставляющие оператору компьютерные ресурсы и мощности для обработки информации на основании заключенного с этим лицом договора (далее – уполномоченное лицо), принимают меры защиты информации в соответствии с законодательством Российской Федерации. Договор между оператором (заказчиком) информационной системы и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечивать защиту информации, содержащейся в информационной системе, в соответствии с настоящими Требованиями.

Обеспечение защиты информации, содержащейся в информационной системе, достигается выполнением требований к организации защиты информации, содержащейся в информационной системе, и требований к системе защиты информации информационной системы.

Пересмотр политики с целью поддержания в актуальном состоянии проводится при возникновении следующих условий:

- возникновение условий, существенно влияющих на процессы обработки персональных данных и нерегламентированных настоящим документом;
- по результатам контрольных мероприятий и проверок контролирующих органов, выявивших несоответствие требованиям по обеспечению безопасности персональных данных;
- при появлении новых требований к обеспечению безопасности персональных данных со стороны законодательства Российской Федерации и контролирующих органов.

2. Требования к организации защиты информации, содержащейся в информационной системе

В информационной системе объектами защиты являются:

- информация, содержащаяся в информационной системе;
- технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации, иные технические средства, используемые для обработки информации), общесистемное, прикладное, специальное программное обеспечение, реализующие информационные технологии, входящие в периметр защиты информационной системы;
- средства защиты информации.

Периметр защиты информационной системы определяется совокупностью физически и (или) логически выделенных технических средств и программного обеспечения, эксплуатируемых оператором (уполномоченным лицом), в отношении которых применяются меры защиты информации и осуществляется контроль за их применением.

Для обеспечения защиты информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и (или) оператором назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение защиты информации.

Для проведения работ по защите информации в ходе создания и эксплуатации информационных систем заказчиками и (или) операторами в соответствии с законодательством Российской Федерации могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие в соответствии с законодательством Российской Федерации оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

Защита информации, содержащейся в информационной системе, является неотъемлемой частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) создания и эксплуатации информационной системы с помощью системы (подсистемы) защиты информации, включающей организационные и технические меры защиты информации, обеспечивающие блокирование (нейтрализацию) актуальных угроз безопасности информации (далее – система защиты информации информационной системы).

Система защиты информации информационной системы должна обеспечивать конфиденциальность, целостность и (или) доступность информации, содержащейся в информационной системе.

2.1 Формирование требований к системе защиты информации информационной системы

Формирование требований к системе защиты информации информационной системы организуется заказчиком с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

принятие решения о необходимости создания системы защиты информации информационной системы;

классификацию информационной системы по требованиям защиты информации (далее – классификация информационной системы);

определение актуальных угроз безопасности информации и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации информационной системы.

При принятии решения о необходимости создания системы защиты информации осуществляется:

анализ целей создания информационной системы и задач, решаемых этой информационной системой;

определение видов (типов) информации, подлежащей обработке в информационной системе;

анализ нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система;

принятие решения о необходимости создания системы защиты информации, включающее определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций обладателя информации, заказчика, оператора и уполномоченного лица по обеспечению защиты информации.

Решение о необходимости создания системы защиты информации информационной системы является основой для определения требований к системе защиты информации информационной системы.

Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый) и определяет уровень защищенности информации, содержащейся в информационной системе.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов. Требование к классу защищенности включается в техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемое с учетом ГОСТ Р 51583 и ГОСТ Р 51624.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются соответствующим актом классификации.

Актуальные угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) нарушителей (внешних, внутренних), анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении актуальных угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе в целом и в ее отдельных сегментах.

По результатам определения актуальных угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Актуальные угрозы безопасности информации включаются в модель угроз безопасности информации, которая должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание актуальных угроз безопасности информации, включающее описание возможностей нарушителей, возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения актуальности угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы ФСТЭК России, разработанные и утвержденные в пределах ее полномочий.

Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и актуальных угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на ее создание, разрабатываемое с учетом ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения безопасности информации обладателя информации (заказчика) в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента

информационной безопасности. Требования», а также политик обеспечения безопасности информации оператора и уполномоченного лица в части, не противоречащей политикам обеспечения безопасности информации обладателя информации (заказчика).

2.2. Разработка системы защиты информации информационной системы

Разработка системы защиты информации информационной системы организуется заказчиком, проводится в соответствии с техническим заданием на создание системы защиты информации информационной системы, с учетом ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

проектирование системы защиты информации информационной системы;

разработку эксплуатационной документации на систему защиты информации информационной системы;

макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Разрабатываемая система защиты информации не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации учитываются информационное взаимодействие с иными информационными системами, в том числе с информационными системами уполномоченного лица, а также применение компьютерных ресурсов и мощностей, предоставляемых уполномоченным лицом в качестве услуг для обработки информации.

Результаты разработки системы защиты информации информационной системы подлежат согласованию с оператором информационной системы в случае, если оператор не является заказчиком информационной системы, но определен таковым в соответствии с законодательством Российской Федерации к моменту окончания разработки системы защиты информации информационной системы.

Проектирование системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание системы защиты информации информационной системы.

При проектировании системы защиты информации информационной системы:

определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и используемые правила разграничения

доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

осуществляется выбор мер защиты информации, подлежащих реализации в системе защиты информации информационной системы;

определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению актуальных угроз безопасности информации;

формируются требования к защите информации при информационном взаимодействии с иными информационными системами, в том числе с информационными системами уполномоченного лица, а также применение компьютерных ресурсов и мощностей, предоставляемых уполномоченным лицом.

При отсутствии средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) необходимых средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

Разработка эксплуатационной документации на систему защиты информации информационной системы осуществляется с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601) и ГОСТ Р 51624.

Эксплуатационная документация на систему защиты информации информационной системы должна в том числе содержать:

структуру системы защиты информации информационной системы;

состав, места установки, параметры и порядок настройки средств защиты информации, программного обеспечения и технических средств обработки информации;

привила эксплуатации системы защиты информации информационной системы.

При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляется:

проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами обработки информации;

проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы;

корректировка проектных решений по информационной системе и (или) ее системе защиты информации;

корректировка документации на систему защиты информации информационной системы.

Макетирование системы защиты информации информационной системы и ее тестирование проводится, в том числе с использованием средств и методов моделирования информационных систем.

2.3. Реализация системы защиты информации информационной системы

Реализация системы защиты информации информационной системы организуется заказчиком, проводится в соответствии с проектными решениями и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

установку и настройку средств защиты информации в информационной системе;

разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее – организационно-распорядительные документы по защите информации);

внедрение организационных мер в информационной системе;

предварительные испытания системы защиты информации информационной системы;

опытную эксплуатацию системы защиты информации информационной системы;

анализ уязвимостей информационной системы;

приемочные испытания системы защиты информации информационной системы.

К реализации системы защиты информации информационной системы привлекается оператор информационной системы в случае если оператор не является заказчиком информационной системы и он определен в соответствии с законодательством Российской Федерации к моменту реализации системы защиты информации информационной системы.

Установка и настройка средств защиты информации в информационной системе должна проводиться в соответствии с

эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

Разрабатываемые организационно-распорядительные документы по защите информации должны определять:

правила и процедуры идентификации и аутентификации субъектов доступа и объектов доступа, в том числе предусматривающие управление учетными записями пользователей, установление полномочий пользователей, правила генерации, смены и восстановления паролей пользователей;

правила и процедуры управления доступом субъектов доступа к объектам доступа, в том числе устанавливающие перечень лиц, имеющих доступ к объектам доступа информационной системы, и их права (привилегии) доступа к этим объектам;

правила и процедуры защиты машинных носителей информации, в том числе устанавливающие порядок вывода информации на внешние носители информации, учета, хранения и использования съемных машинных носителей информации, процедуры архивирования информации, порядок стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации;

правила и процедуры регистрации событий безопасности, в том числе предусматривающие порядок контроля за действиями пользователей (администраторов) в информационной системе;

правила и процедуры обеспечения целостности информационной системы и информации, в том числе предусматривающие контроль целостности системы защиты информации информационной системы, порядок периодического анализа уязвимостей информационной системы и принятия первоочередных мер по устранению вновь выявленных уязвимостей, восстановления работоспособности и настроек системы защиты информации информационной системы в случае нарушения функционирования информационной системы;

правила и процедуры защиты технических средств, в том числе определяющие перечень лиц, имеющих доступ в помещения, в которых расположены технические средства, и порядок их доступа в помещения и к техническим средствам;

правила и процедуры защиты информационной системы, ее средств и систем связи и передачи данных, в том числе определяющие порядок использования периферийных устройств, которые могут активироваться удаленно, технологий мобильного кода, технологий передачи речи и видеоинформации, порядок защиты внутренних и внешних беспроводных соединений, порядок использования и защиты мобильных устройств;

правила и процедуры управления конфигурацией, в том числе определяющие порядок обновления программного обеспечения, управления параметрами настройки средств защиты информации, составом и

конфигурацией технических средств обработки информации и программного обеспечения, контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения;

правила и процедуры анализа угроз безопасности информации и принятия дополнительных мер защиты информации от вновь возникших угроз безопасности информации, выявления и устранения недостатков в системе защиты информации информационной системы, внесения изменений в документацию на систему защиты информации информационной системы;

правила и процедуры выявления реагирования на инциденты, связанные с защитой информации;

правила и процедуры обслуживания системы защиты информации информационной системы;

порядок обучения и информирования пользователей о правилах эксплуатации системы защиты информации информационной системы и средств защиты информации, а также информирования об угрозах безопасности информации.

При внедрении организационных мер осуществляется:

реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа), и введение ограничений на действия пользователей, а так же на изменение условий эксплуатации, состава и конфигурации технических средств обработки информации и программного обеспечения;

проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер;

отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.

Предварительные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем» (далее – ГОСТ 34.603) и включают проверку работоспособности системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.

Опытная эксплуатация системы защиты информации информационной системы проводится с учетом ГОСТ 34.603 и включает проверку функционирования системы защиты информации информационной системы, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения, в том числе на основе информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств обработки информации и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами обработки информации и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования выявленных уязвимостей.

Приемочные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.

2.4. Аттестация информационной системы на соответствие требованиям о защите информации и ввод ее в действие

Аттестация информационной системы на соответствие требованиям о защите информации организуется заказчиком или оператором (уполномоченным лицом) и включает оценку соответствия организации защиты информации и системы защиты информации информационной системы настоящим Требованиям.

В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы по требованиям защиты информации, техническое задание на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы приемочных (предварительных) испытаний системы защиты информации

информационной системы, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями.

Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации в информационной системе. Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы ФСТЭК России, разработанные и утвержденные в пределах ее полномочий.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний и заключение о соответствии информационной системы требованиям о защите информации.

8.3. Допускается аттестация информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

Особенности аттестации информационной системы на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты информационной системы определяются в программе и методиках аттестационных испытаний и аттестате соответствия.

В этом случае распространение аттестата соответствия на другие сегменты информационной системы осуществляется при условии их соответствия сегментам информационной системы, прошедшим аттестационные испытания.

Сегмент считается соответствующим аттестованному сегменту информационной системы, если для обоих сегментов установлены одинаковые классы защищенности, актуальные угрозы безопасности информации, реализованы одинаковые проектные решения по системе защиты информации информационной системы.

Соответствие сегмента, на который распространяется аттестат соответствия, аттестованному сегменту информационной системы подтверждается в ходе приемочных испытаний информационной системы или сегментов информационной системы.

В сегментах информационной системы, на которые распространяется аттестат соответствия, оператором обеспечивается соблюдение эксплуатационной документации на систему защиты информации информационной системы и организационно-распорядительных документов по защите информации.

Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия, изменения класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы.

Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601.

2.5. Эксплуатация системы защиты информации информационной системы

Эксплуатация системы защиты информации информационной системы осуществляется оператором при наличии аттестата соответствия требованиям о защите информации в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и должна в том числе включать:

обеспечение безопасности среды эксплуатации информационной системы;

администрирование системы защиты информации информационной системы;

реагирование на инциденты, связанные с защитой информации;

управление конфигурацией системы защиты информации информационной системы;

управление защитой информации в информационной системе.

Безопасность среды эксплуатации информационной системы обеспечивается:

организацией контролируемой зоны, в пределах которой постоянно размещаются технические средства, обрабатывающие информацию, и средства защиты информации, а также средства, обеспечивающие функционирование информационной системы (далее – средства обеспечения функционирования);

контролем и управлением доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

защитой технических средств, средств защиты информации и средств обеспечения функционирования.

В ходе администрирования системы защиты информации информационной системы осуществляется:

заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;

управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей;

централизованное управление системой защиты информации информационной системы (при необходимости);

внесение изменений в организационно-распорядительные документы по защите информации (при необходимости);

анализ событий в информационной системе, относящихся к безопасности информации;

информирование пользователей о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации и их обучение, а также об угрозах безопасности информации.

В ходе реагирования на инциденты, связанные с защитой информации, осуществляется:

обнаружение, квалификация и регистрация инцидентов, связанных с защитой информации, в том числе сбоев в работе технических средств, программного обеспечения и средств защиты информации, внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иные событий, связанных с защитой информации;

своевременное информирование структурного подразделения или должностного лица, ответственных за защиту информации, пользователями информационной системы об инцидентах, связанных с защитой информации;

выявление причин возникновения инцидентов, связанных с защитой информации, оценка их последствий, планирование и принятие мер по предупреждению и устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов после сбоев, выявлению и устранению последствий внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с защитой информации.

В ходе управления конфигурацией системы защиты информации информационной системы осуществляется:

обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации;

установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками (по поручению разработчиков);

управление параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, составом и конфигурацией технических средств и программного обеспечения, а также контроль за несанкционированными подключениями технических средств и установкой программного обеспечения.

Перед реализацией планируемых в процессе управления конфигурацией изменений в информационной системе и ее системе защиты информации проводится оценка их потенциального воздействия на обеспечение защиты информации и работоспособность информационной системы.

Изменения в информационной системе и ее системе защиты информации, внесенные в процессе управления конфигурацией, подлежат документированию оператором.

В ходе управления защитой информации в информационной системе осуществляется:

выполнение организационных мер защиты информации;

контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы;

анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности;

периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе;

доработка (модернизация) системы защиты информации информационной системы и ее повторная аттестация при изменении класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы;

сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.

Результаты контроля состояния защиты информации, анализа и оценки функционирования системы защиты информации информационной системы, анализа уязвимостей и изменения угроз безопасности информации в информационной системе подлежат документированию оператором.

2.6. Защита информации в ходе снятия с эксплуатации информационной системы или после окончания обработки информации

Защита информации в ходе снятия с эксплуатации информационной системы или после окончания обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и включает:

архивирование информации, содержащейся в информационной системе;

уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Архивирование информации, содержащейся в информационной системе, обеспечивается при необходимости ее дальнейшего использования в деятельности оператора.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости их передачи между пользователями информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшей утилизации.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется уничтожение этих машинных носителей информации.

3. Требования к системе защиты информации информационной системы

Система защиты информации, реализуемая в информационной системе, в зависимости от актуальных угроз безопасности информации и структурно-функциональных характеристик информационной системы включает следующие меры защиты информации:

- обеспечение доверенной загрузки;
- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- обеспечение целостности информационной системы и информации;

защиту среды виртуализации;

- защиту технических средств;
- защиту информационной системы, ее средств и систем связи и передачи данных.