ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат
13EC3501E99A05A8FAD13660404BAD029E3BD18B
Владелец Щеголева Оксана Валерьевна
Действителен с 19.11.2020 по 19.02.2022

УТВЕРЖДАЮ
Заведующий МБДОУ ДС № 67 «Умка»
_____О.В.Щеголева
14 декабря 2020 года

ИНСТРУКЦИЯ

ответственных за защиту информации муниципального бюджетного дошкольного образовательного учреждения детского сада № 67 «Умка»

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет права и функциональные обязанности лиц, ответственных за защиту сведений ограниченного доступа (в том числе персональных данных) информационных систем (далее – ИС, объект информатизации) муниципального бюджетного дошкольного образовательного учреждения детского сада № 67 «Умка» (далее –Учреждение). Положения настоящей Инструкции являются дополнением к должностным обязанностям ответственных лиц.

Инструкция разработана на основании действующих нормативных документов по вопросам защиты сведений ограниченного доступа, в том числе персональных данных, (далее – защищаемая информация) и направлена на обеспечение безопасности информации.

Лица, ответственные за защиту информации:

– ответственный за организацию обработки персональных данных;

– ответственный за обеспечение безопасности персональных данных в части организационного обеспечения безопасности персональных данных (ответственный за эксплуатацию информационной системы);

– ответственный за обеспечение безопасности персональных данных в части технического обеспечения безопасности персональных данных (администратор безопасности);

– ответственный за учет и хранение средств криптографической защиты информации (далее – ответственный за учет и хранение СКЗИ),

в своей работе должны руководствоваться настоящей Инструкцией, утвержденными документами Учреждения, регламентирующими порядок обеспечения безопасности защищаемой информации, законными, подзаконными, руководящими документами по защите информации, а также документами, поступившими из вышестоящих и контролирующих органов.

Ответственные за защиту информации в вопросах защиты информации взаимодействуют между собой.

1.1 Назначение ответственных лиц

Администратором безопасности назначаются сотрудники Учреждения, организующие обслуживание программных и технических средств, входящих в состав объекта информатизации.

Ответственным за учет и хранение СКЗИ назначаются отдельные работники из числа инженерно-технического персонала Учреждения, имеющие высшее профессиональное образование и опыт работы с шифровальными (криптографическими) средствами либо имеющие достаточные знания в области обеспечения безопасности информации.

Ответственным за организацию обработки персональных данных, ответственным за эксплуатацию информационной системы назначаются лица из числа сотрудников Учреждения, которые имеют широкие полномочия и от имени руководителя, способные организовать работы, необходимые для реализации требований законодательства, и имеющие достаточный опыт работы по основной деятельности Учреждения.

Лица, ответственные за защиту информации, должны знать:

– действующее законодательство о защите информации;

– руководящие, нормативные и методические материалы по вопросам, связанным с организацией защиты информации;

– перспективы и направления развития средств защиты информации.

Лица, ответственные за защиту информации, назначаются руководителем Учреждения. На период отпуска или в случае временной нетрудоспособности лиц, ответственных за защиту информации, назначаются должностные лица, временно исполняющие их обязанности.

2. ОРГАНИЗАЦИЯ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

2.1 Организация доступа пользователей к ресурсам информационной системы

Доступ пользователей к работе на ПЭВМ, входящих в состав информационной системы, должен осуществляться в строгом соответствии с утвержденными журналом учета доступа. Организация оформления (ведения) журнала учета доступа возлагается на администратора безопасности.

Все изменения в журнале учета доступа согласуются с ответственным за эксплуатацию информационной системы, на основании которых администратор безопасности производит корректировку учетных записей пользователей и устанавливает права доступа к информационным ресурсам новым пользователям.

С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в системе. В случае необходимости пользователю могут быть сопоставлены несколько уникальных имен (учетных записей).

Создание и управление учетными записями пользователей (заведение, активация, блокирование и уничтожение), назначение прав и установление полномочий доступа к информационным ресурсам, порядок регистрации (входа) в ОС производится администратором безопасности средствами ОС и установленными средствами защиты.

Администратор безопасности осуществляет организацию создания и управления учетными записями пользователей (заведение, активация, блокирование и уничтожение), назначения прав и установление полномочий доступа к информационным ресурсам, порядок регистрации (входа) в ОС.

Доступ пользователя к ресурсам ИС осуществляется посредством личного идентификатора, в качестве идентификатора используется логин-пароль и/или электронный ключ. Персональные атрибуты доступа выдаются только после ознакомления пользователя с базой нормативно-методических документов, подготавливаемой ответственным за организацию обработки персональных данных, а также с разработанными организационно-распорядительными и техническими документами, применяемыми для защиты информации в ИС.

2.2 Проведение инструктажа пользователей

Перед допуском пользователя к работе в информационной системе лицами, ответственными за защиту информации, должно организовываться обязательное обучение пользователя правилам работы с установленными средствами защиты, а также ознакомление с разработанными организационно-распорядительными и техническими документами, применяемыми для защиты информации.

Инструктаж по работе с установленными средствами защиты должен организовываться администратором безопасности при первичном допуске пользователя к работе на ПЭВМ. Администратор безопасности организует помощь в части применения СЗИ и консультирования по вопросам установленного режима защиты.

Контроль ознакомления сотрудников, допущенных к работе в ИС, с разработанными организационно-распорядительными и техническими документами, применяемыми для защиты информации (положениями, приказами, инструкциями и т.д.), возлагается на администратора безопасности.

Администратор безопасности обязан ознакомить всех лиц, допущенных к обработке защищаемой информации, с предоставленными нормативно-методическими документами под роспись в Журнале учета доступа.

Ответственный за организацию обработки персональных данных должен осуществлять периодическое уточнение и дополнение базы нормативно-методических документов (мониторинг изменений в законодательных и нормативных актах Российской Федерации, касающихся обработки и защиты информации).

2.3 Общие требования по организации обработки защищаемой информации

Организация обработки защищаемой информации на объекте информатизации должна предусматривать неизменность состава технических средств, используемых для обработки такой информации, структуры защищенной локальной сети, конфигурации информационной системы.

В случае необходимости замены установленных ОТСС, изменения топологии защищенной сети (включение нового сетевого оборудования и т.д.), конфигурации информационной системы, такие изменения отражаются в Техническом паспорте ИС.

Администратором безопасности должен организовываться периодический (не реже одного раза в квартал) контроль состава основных технических средств и систем ИС согласно Техническому паспорту объекта информатизации.

Контроль наличия и целостности пломб (печатей, специальных защитных знаков) на корпусах ПЭВМ и устройствах, входящих в состав объекта информатизации, должен организовываться администратором безопасности не реже одного раза в квартал. В случае обнаружения нарушения целостности пломб администратор безопасности организует выяснение причин, приведших к такому нарушению, и принимает меры по их устранению.

В целях исключения случайного (преднамеренного) ознакомления с защищаемой информацией посторонними лицами в помещениях ИС должны быть реализованы специальные меры по организации безопасной обработки такой информации (размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр, контроль хранения бумажных документов и т.д.).

2.4 Парольная защита

В целях предотвращения несанкционированного доступа к ресурсам ПЭВМ и повышения уровня надежности идентификации пользователей в информационной системе должны быть установлены дополнительные требования к сложности пароля:

– пароль не должен содержать имя учетной записи пользователя или его фрагменты длиной больше двух символов;

– пароль должен состоять не менее чем из шести символов;

– пароль должен содержать символы, относящиеся к трем из следующих четырех категорий: латинские заглавные буквы (A - Z), латинские строчные буквы (a - z), цифры (0 - 9), отличные от букв и цифр символы (например !, $, #, %);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, клички домашних животных, наименования ПЭВМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.)), а также другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

– не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

Смена всех паролей доступа в ИС должна производиться пользователями под контролем администратора безопасности не реже одного раза в год.

Удаление (в том числе внеплановая смена) личного пароля пользователя информационной системы производится:

– при подозрении на дискредитацию пароля;

– по указанию администратора безопасности.

В случае прекращения полномочий пользователя (увольнение, переход на другую работу внутри Учреждения и др.) администратором безопасности организуется блокирование учетной записи пользователя.

2.5 Антивирусный контроль

В целях обеспечения защиты от деструктивных воздействий вредоносного программного обеспечения в Учреждении проводится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на ПЭВМ, входящие в состав ИС, в том числе информация, предоставляемая на внешних носителях информации.

На рабочих местах пользователей информационных систем запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации для каждой информационной системы. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения администратор безопасности выполняет антивирусную проверку всех ПЭВМ, входящих в состав ИС.

К использованию в информационных системах допускаются только сертифицированное, лицензионное антивирусное программное обеспечение. Системные требования антивирусного программного обеспечения должны полностью соответствовать платформам, характеристикам и комплектации ПЭВМ, входящих в состав ИС.

Установка, конфигурирование и управление средствами антивирусной защиты проводится исключительно администратором безопасности. Для пользователей ИС запрещена возможность изменения настроек и параметров защиты антивирусных средств на своих рабочих местах. Настройка параметров, режимов и функций антивирусного программного обеспечения осуществляется администратором безопасности в соответствии с Руководством по применению антивирусного программного обеспечения.

Для поддержания требуемого уровня безопасности администратором безопасности должен организовываться периодический контроль обновления антивирусных баз, а также соблюдения пользователями порядка и правил проведения антивирусной проверки ресурсов ПЭВМ, входящих в состав информационной системы, в соответствии с утвержденной Инструкцией пользователя.

В случае обнаружения вредоносного программного обеспечения на ПЭВМ, входящей в состав ИС, администратор безопасности выполняет следующие действия:

– централизованно обновляет антивирусные базы сервера администрирования и всех объектов антивирусной защиты;

– проверяет состояние всех объектов антивирусной защиты, а также наличие зараженных рабочих станций (в случае обнаружения пораженных узлов);

– оперативно принимает меры по предотвращению распространения заражения вредоносными программами, отключает от сети зараженную ПЭВМ (при необходимости);

– проводит действия, направленные на устранение вредоносного программного обеспечения на всех пораженных узлах.

После завершения всех необходимых мероприятий по устранению последствий заражения администратор безопасности восстанавливает работоспособность рабочей станции и передает ее пользователю ИС.

Уничтожение вредоносных программ выполняется только администратором безопасности. Если вредоносная программа поразила какое-либо программное обеспечение, то уничтожение вредоносного программного обеспечения выполняется путем уничтожения зараженного программного обеспечения на жестком диске. После уничтожения зараженной программы производится процесс восстановления программного обеспечения путем использования ее резервной копии. Если вредоносное программное обеспечение поразило файлы, то уничтожение вредоносного программного обеспечения производится путем стирания зараженных файлов или путем использования специального «лечащего» режима антивирусного ПО. Использование такого режима допустимо только в тех случаях, когда отсутствует резервная копия зараженного файла либо восстановление уничтоженного файла с помощью резервной копии является довольно трудоёмким процессом.

После уничтожения вредоносного программного обеспечения и/или восстановления зараженных программ (файлов) выполняется повторная проверка наличия вредоносных программ, используя антивирусную программу с установленными обновлениями.

При выявлении неподдающегося «лечению» вируса администратор безопасности должен организовать уведомление об этом организацию-разработчика антивирусного программного обеспечения с целью выработки совместных действий по устранению последствий заражения.

2.6 Работа с внешними носителями информации

Для разработки и хранения документов, содержащих защищаемую информацию, могут применяться машинные носители информации.

Администратор безопасности организует регистрацию всех машинных носителей информации, регистрируемых в Журнале учета защищаемых машинных носителей до момента записи на них такой информации. Обработка и хранение сведений ограниченного доступа на неучтенных машинных носителях информации запрещена.

Администратором безопасности должен организовываться контроль соблюдения порядка обращения и хранения учтенных в установленном порядке машинных носителей информации. Все учтенные машинные носители информации выдаются пользователям под роспись в журнале учета защищаемых машинных носителей информации и должны храниться в запираемых шкафах или сейфах, расположенных в местах, исключающих доступ к ним посторонних лиц, оборудованных замками или устройствами для опломбирования.

При передаче учтенных машинных носителей информации между пользователями, а также в сторонние организации для ремонта или утилизации, администратором безопасности в обязательном порядке организовывается уничтожение данных, содержащихся на носителе.

Машинные носители информации не снимаются с учета при удалении с них защищаемой информации. Непригодные для дальнейшего использования учтенные носители подлежат уничтожению путем необратимого механического разрушения с составлением Акта уничтожения.

2.7 Обеспечение неизменности программной среды

В процессе функционирования информационной системы должна быть обеспечена неизменность технологии обработки защищаемой информации, а также состава установленного программного обеспечения.

Пользователям ИС запрещается устанавливать программное обеспечение, не связанное с выполнением функций, предусмотренных технологическим процессом обработки информации для каждой информационной системы. Права пользователей на установку программного обеспечения должны быть ограничены.

Манипуляции с BIOS/UEFI может осуществлять только администратор безопасности. Пользователям ИС запрещены любые действия с BIOS/UEFI, в том числе «откат» версии.

В случае необходимости обновления программного обеспечения, устанавливаемые программные компоненты проверяются на работоспособность и отсутствие вирусов, а также на совместимость с другими программными и техническими средствами ИС.

Все изменения, внесенные в состав штатного программного обеспечения, заносятся в Технический паспорт объекта информатизации согласно Инструкции по внесению изменений.

Контроль соответствия общесистемной программной среды утвержденному Перечню программного обеспечения должен организовываться администратором безопасности не реже одного раза в полгода.

2.8 Организация работы в сети Интернет

В случае применения в ИС беспроводных соединений необходимо обеспечить защиту таких соединений.

Защита беспроводных соединений включает:

– ограничение на использование в ИС беспроводных соединений в соответствии с задачами (функциями) ИС, для решения которых такие соединения необходимы;

– регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к ИС через беспроводные соединения;

– предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администратору безопасности;

– обеспечение возможности реализации беспроводных соединений через контролируемые интерфейсы;

– применение средств защиты информации, средств криптографической защиты информации, а также программно-технических средств обнаружения, анализа и блокирования несанкционированного использования беспроводных соединений и подключений к ИС;

– обеспечение блокирования несанкционированных беспроводных подключений к ИС.

При обеспечении защиты беспроводных соединений (в зависимости от их типов) должны реализовываться меры по идентификации и аутентификации, отраженные в приказах ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 года № 21 и «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года № 17 (далее – приказы ФСТЭК).

При передаче защищаемой информации по каналам связи, имеющим выход за пределы контролируемой зоны, должны приниматься меры защищенного удаленного доступа в соответствии с приказами ФСТЭК.

2.9 Резервное копирование и восстановление защищаемой информации

В целях оперативного восстановления обрабатываемой защищаемой информации в случае ее модификации или уничтожения администратором безопасности должно организовываться периодическое резервирование такой информации.

Порядок проведения резервного копирования и восстановления защищаемой информации, а также условия хранения носителей резервных копий и порядок их учета определены в утвержденном Регламенте резервного копирования.

2.10 Техническое обслуживание, ремонт и модернизация технических средств

При необходимости проведения ремонта или модернизации ПЭВМ, входящих в состав объекта информатизации, необходимо внести изменения в Технический паспорт.

В случае проведения технического обслуживания на месте установки ПЭВМ, администратор безопасности организует контроль вскрытия и ремонта (модернизации) защищенных ПЭВМ, а также ограничение допуска посторонних лиц к проводимым работам. Запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

При необходимости выноса ПЭВМ за пределы территории здания (контролируемой зоны) с целью ремонта, замены комплектующих и т.п., такие работы должны быть согласованы с руководителем Учреждения. При принятии решения о выносе ПЭВМ, жесткий магнитный диск демонтируется и убирается на хранение в запираемый шкаф (сейф). В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж машинных носителей информации должны быть предварительно согласованы с ней.

Запрещается вторичное использование жестких магнитных дисков, замененных по каким-либо причинам. Все неисправные демонтированные жесткие диски подлежат уничтожению методом механического разрушения с составлением Акта уничтожения машинных носителей информации.

Вскрытый системный блок ПЭВМ, подвергшийся ремонту или модернизации, подлежит обязательному опечатыванию с составлением соответствующих актов с отметкой о вскрытии и результатом проведенных ремонтных работ в Техническом паспорте объекта информатизации.

2.11 Контроль за функционированием средств защиты информации

Периодический контроль функционирования установленных СЗИ должен организовываться администратором безопасности не реже одного раза в квартал согласно эксплуатационным документам. В ходе проверки администратором безопасности осуществляется просмотр и анализ зарегистрированных событий безопасности, а также реагирование на них. Пользователям ИС запрещается изменять настройки установленных средств защиты, а также вносить изменения в установленные режимы работы таких средств.

Контроль актуальности сертификатов соответствия ФСТЭК России (ФСБ России) на СЗИ, установленные в ИС, должен организовываться администратором безопасности не реже одного раза в полгода.

2.12 Контроль соблюдения правовых мер по обеспечению безопасности защищаемой информации

Ответственным за организацию обработки защищаемой информации/ ответственным за организацию обработки персональных данных должен организовываться внутренний контроль соблюдения сотрудниками, допущенными к обработке таких данных в ИС, требований к защите информации.

Все лица, которым в рамках должностных обязанностей предоставлен допуск к сведениям ограниченного доступа, ***обязаны подписать соглашение о неразглашении*** таких сведений. Контроль получения и хранения обязательств о неразглашении возлагается на ответственного за организацию обработки защищаемой информации и/или ответственного за организацию обработки персональных данных.

3. ПРАВА И ОБЯЗАННОСТИ ЛИЦ, ОТВЕТСТВЕННЫХ ЗА ЗАЩИТУ ИНФОРМАЦИИ

3.1. Права и обязанности ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных обязан:

– организовывать внутренний контроль соблюдения сотрудниками, допущенными к обработке защищаемой информации, требований к защите информации/персональных данных;

– периодически уточнять и дополнять базу нормативно-методических документов (проводить мониторинг изменений в законодательных и нормативных актах Российской Федерации, касающихся обработки и защиты информации/персональных данных);

– организовывать контроль взаимодействия ИС с информационными системами сторонних организаций (внешние информационные системы);

– поддерживать в актуальном состоянии организационно-распорядительную документацию, определяющую порядок обработки и обеспечения безопасности защищаемой информации/персональных данных;

– организовывать проведение мероприятий по контролю защищенности информации (внутренние проверки);

– уведомлять контролирующие органы об организации обработки и защиты информации/персональных данных;

– информировать руководство о фактах нарушения установленного порядка работ;

– содействовать регулирующим органам в случае проведения проверки (в части сбора и предоставления необходимой информации).

Ответственный за организацию обработки персональных данных имеет право:

– требовать от пользователей информационной системы соблюдения установленной технологии обработки защищаемой информации/персональных данных, требований утвержденных документов, регламентирующих порядок обеспечения безопасности информации, законных, подзаконных, руководящих документов по защите информации/персональных данных, а также документов, поступивших из вышестоящих и контролирующих органов;

– приостанавливать работу пользователей в случае нарушения предъявляемых требований к защите информации/персональных данных;

– участвовать в анализе ситуаций, касающихся функционирования системы защиты объекта информатизации и расследования фактов несанкционированного доступа к защищаемой информации/персональным данным;

– содействовать в проведении аттестационных испытаний, внепланового и периодического контроля объекта информатизации, а также анализа защищенности информации;

– предлагать способы и методы совершенствования системы защиты информации.

3.2. Права и обязанности ответственного за эксплуатацию информационной системы

Ответственный за эксплуатацию информационной системы обязан:

– осуществлять контроль соблюдения сотрудниками, допущенными к обработке защищаемой информации, требований к защите информации/персональных данных

– организовать прием, обработку и учет обращений и запросов субъектов персональных данных, осуществлять контроль обработки таких обращений и запросов;

– совместно с администратором безопасности осуществлять документирование информации об изменениях в конфигурации информационной системы и системы защиты информации (согласно Инструкции по внесению изменений Технического паспорта объекта информатизации);

– информировать руководство и ответственного за организацию обработки персональных данных о фактах нарушения установленного порядка работ;

– осуществлять контроль получения письменного согласия от субъектов персональных данных на обработку их персональных данных.

Ответственный за эксплуатацию информационной системы имеет право:

– требовать от пользователей информационной системы соблюдения установленной технологии обработки защищаемой информации/персональных данных, требований

утвержденных документов, регламентирующих порядок обеспечения безопасности информации, законных, подзаконных, руководящих документов по защите информации/персональных данных, а также документов, поступивших из вышестоящих и контролирующих органов;

– приостанавливать работу пользователей в случае нарушения предъявляемых требований к защите информации/персональных данных;

– участвовать в анализе ситуаций, касающихся функционирования системы защиты объекта информатизации и расследования фактов несанкционированного доступа к защищаемой информации/персональным данным;

– предлагать способы и методы совершенствования системы защиты информации.

3.3. Права и обязанности администратора безопасности

Администратор безопасности обязан:

– своевременно проводить работу с учетными записями пользователей информационной системы (регистрация новых учетных записей пользователей, удаление учетной записи пользователя), согласно утвержденному Журналу учета доступа;

– оказывать помощь пользователям информационной системы в части применения средств защиты и консультирования по вопросам введенного режима защиты;

– обеспечивать неизменность состава технических средств, используемых для обработки защищаемой информации, осуществлять периодический контроль их состава согласно Техническому паспорту объекта информатизации;

– осуществлять периодический мониторинг информационной системы с использованием сертифицированного сканера безопасности и оперативно устранять выявленные уязвимости;

– производить периодические проверки (не реже одного раза в квартал) наличия уязвимостей системного и прикладного программного обеспечения, в том числе средств защиты информации, в Банке данных уязвимостей ФСТЭК России.

– контролировать соблюдение парольной политики пользователями ИС;

– проводить плановые проверки ресурсов информационной системы на отсутствие компьютерных вирусов;

– организовывать учет и выдачу защищаемых машинных носителей информации, контролировать соблюдение порядка обращения и хранения таких носителей (управление доступом к МНИ);

– обеспечивать работоспособность элементов ИС и локальной вычислительной сети, проводить обслуживание и ремонт технических средств информационной системы, восстановление систем защиты информации при сбоях;

– организовывать периодические контрольные проверки ПЭВМ, журналов регистрации событий безопасности, а также осуществлять тестирование правильности функционирования средств защиты ИС;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт;

– организовывать контроль целостности пломб (печатей, специальных защитных знаков) на корпусах ПЭВМ и устройствах, входящих в состав объекта информатизации;

– обеспечивать неизменность процессов обработки защищаемой информации (состава оборудования, конфигурации информационной системы), а также состава установленного системного и прикладного программного обеспечения (контроль установки, настройки, обновления, работоспособности программного обеспечения);

– производить все необходимые действия с BIOS/UEFI;

– контролировать актуальность сертификатов соответствия на установленные средства защиты информации;

– организовывать резервное копирование и восстановление защищаемой информации;

– совместно с ответственным за организацию обработки защищаемой информации и/или ответственным за организацию обработки персональных данных осуществлять

документирование информации об изменениях в конфигурации информационной системы и системы защиты информации (согласно Инструкции по внесению изменений);

– информировать руководство и ответственного за организацию обработки защищаемой информации и/или ответственного за организацию обработки персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам информационной системы.

Администратор безопасности имеет право:

– требовать от пользователей информационной системы соблюдения установленной технологии обработки защищаемой информации, требований утвержденных документов, регламентирующих порядок обеспечения безопасности информации, законных, подзаконных, руководящих документов по защите информации, а также документов, поступивших из вышестоящих и контролирующих органов;

– приостанавливать работу пользователей в случае нарушения предъявляемых требований к защите информации;

– участвовать в анализе ситуаций, касающихся функционирования системы защиты объекта информатизации и расследования фактов несанкционированного доступа к защищаемой информации;

– содействовать в проведении аттестационных испытаний, внепланового и периодического контроля, а также анализа защищенности объекта информатизации;

– при изменении (модернизации) действующих программных комплексов, появлении нового программного обеспечения – разрабатывать предложения по изменению и/или дополнению перечня прав и полномочий пользователей, согласовывать их с руководителем Учреждения.

3.4. Права и обязанности ответственного за учет и хранение СКЗИ

Для выполнения возложенных на него функций, ответственный за учет и хранение СКЗИ обязан:

− принимать поступающие в Учреждение средства криптографической защиты информации;

− организовывать поэкземплярный учёт используемых СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (типовая форма журнала учета криптографических средств защиты информации в информационных системах утверждена в Учреждении);

− выдавать под роспись СКЗИ сотрудникам Учреждения для выполнения своих профессиональных обязанностей;

− контролировать соблюдение условий хранения журналов учета СКЗИ и криптосредств, установленных эксплуатационной и технической документацией к СКЗИ, актуальность сертификатов ФСБ России.

Ответственный за учет и хранение СКЗИ имеет право:

− вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией;

− подписывать документы в пределах своей компетенции;

− осуществлять взаимодействие с сотрудниками Учреждения;

− требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.

4. КОНТРОЛЬ ВЫПОЛНЕНИЯ КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Контроль выполнения комплекса организационно-технических мероприятий по защите сведений ограниченного доступа, обрабатываемых в ИС, в пределах своих должностных

обязанностей, осуществляют лица, ответственные за обеспечение безопасности защищаемой информации и пользователи информационной системы.

В целях осуществления внутреннего контроля в Учреждении должно осуществляться плановое проведение периодических проверок соблюдения условий обработки защищаемой информации согласно утвержденному Плану мероприятий по контролю за обеспечением безопасности информации Учреждения и Правилам осуществления внутреннего контроля соответствия обработки защищаемой информации требованиям безопасности информации Учреждения. Руководителем Учреждения должен проводиться периодический контроль выполнения проверок и в случае необходимости пересмотр утвержденного плана.

Рекомендуется проводить периодический контроль объекта информатизации на соответствие требованиям безопасности информации. Данные испытания должны проводиться в соответствии с Программой, разработанной организацией-лицензиатом, определяющей порядок и методы проведения таких испытаний. Результаты контроля заносятся в Технический паспорт объекта информатизации. Выявленные в ходе контроля нарушения и замечания подлежат устранению.

5. ВЫЯВЛЕНИЕ ФАКТОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ И ПРОВЕДЕНИЕ СЛУЖЕБНЫХ РАССЛЕДОВАНИЙ

По фактам и попыткам несанкционированного доступа к защищаемой информации, в случаях обнаружения утечки обрабатываемой защищаемой информации, утраты учтенных машинных носителей информации, несоблюдения условий их хранения, использования программных средств, способных привести к нарушению конфиденциальности защищаемой информации, компрометации паролей, а также выявления иных нарушений, приводящих к снижению уровня защищенности информации, проводится служебное расследование в порядке, установленном в Учреждении.

Служебное расследование проводится комиссией, в состав которой входят лица, ответственные за обеспечение безопасности защищаемой информации. В процессе расследования выявляются причины и виновные в нарушении безопасности защищаемой информации, устраняются выявленные нарушения и выносится решение о достаточности принятых мер по защите информации.

6. ОТВЕТСТВЕННОСТЬ

На лиц, ответственных за организацию безопасности защищаемой информации, возлагается персональная ответственность за качество, полноту и своевременность проводимых им работ по обеспечению защиты информации в соответствии с их функциональными обязанностями.

Лица, ответственные за обеспечение безопасности защищаемой информации, несут ответственность в полном объеме по действующему законодательству Российской Федерации за разглашение ставших им известных сведений, содержащих информацию ограниченного доступа, утерю учтенных МНИ и документов, содержащих защищаемую информацию, а также преднамеренную модификацию, копирование с целью распространения защищаемой информации, обрабатываемой в ИС.

Невыполнение ответственными лицами предъявленных требований может повлечь наступление гражданской, административной, дисциплинарной, либо иной ответственности.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности – субъект доступа, ответственный за защиту информационной системы от несанкционированного доступа к информации.

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация криптографических ключей – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность информации – состояние защищённости информации, характеризуемое способностью информационной системы обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий для ознакомления с ней.

Криптографический ключ – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых автоматизированной системой.

Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи защищаемой информации.

Пользователь средств криптографической защиты информации – физическое лицо, непосредственно допущенное к работе со средствами криптографической защиты информации.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам доступа.

Сертификат защиты – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование таких средств.

Система защиты информации – комплекс организационных мер и программно-аппаратных (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированной системе.

Средство защиты от несанкционированного доступа – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Штатное программное обеспечение – программное обеспечение, посредством которого осуществляется обработка защищаемых данных на объекте информатизации.