Департамент здравоохранения Тюменской области

Государственное автономное учреждение здравоохранения Тюменской области

«ОБЛАСТНОЙ КОЖНО-ВЕНЕРОЛОГИЧЕСКИЙ ДИСПАНСЕР»

ПРИКАЗ

«30» марта 2023г. № 51

г. Тюмень

О назначении ответственного за обеспечение информационной безопасности

В целях исполнения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

п р и к а з ы в а ю:

1. Назначить ответственным за обеспечение информационной безопасности в ГАУЗ ТО «Областной кожно-венерологический диспансер» (далее – Учреждение), в том числе по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты - заместителя главного врача Учреждения.
2. Утвердить положение по организации работ по обеспечению информационной безопасности Учреждения согласно приложению к настоящему приказу.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач П.Н. Жвавый

ТЮМЕНСКИЙ ОБЛАСТНОЙ КОЖНО ВЕНЕРОЛОГИЧЕСКИЙ ДИСПАНСЕР

Приложение к
приказу ГАУЗ ТО «Областной кожно-
венерологический диспансер»
от «___» _____ 202__ г. № _____

Положение
об организации работ по обеспечению безопасности информации
в ГАУЗ ТО «Областной кожно-венерологический диспансер»

2023 год

Термины и определения

Администратор [системный, безопасности] – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) её системы защиты информации (администратор безопасности) в соответствии с установленной ролью.

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аутентификационная информация [информация аутентификации] – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе.

Аутентификация – проверка принадлежность субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Базовый набор мер защиты информации – минимальный набор мер защиты информации, установленный для соответствующего класса защищённости информационной системы.

Виртуализация – технология преобразования формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Виртуальная машина – вычислительная система, эмулируемая с помощью технологии виртуализации, в которую установлена гостевая операционная система и обеспечивается выполнение прикладного программного обеспечения.

Внешняя информационная система – информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Внешняя информационно-телекоммуникационная сеть – информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Временный файл – файл, создаваемый операционной системой или иным программным обеспечением для сохранения промежуточных результатов в процессе функционирования для передачи данных другому программному обеспечению.

Гипервизор – программа (программное обеспечение), создающая среду функционирования других программ (в т.ч. других гипервизоров) за счёт имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

Гостевая операционная система – операционная система, установленная на виртуальной машине.

Демилитаризованная зона – экранированный сегмент информационной системы, размещённый не её внешней границе и выполняющий функции «нейтральной зоны» (буферной зоны безопасности) между защищаемой информационной системой оператора и внешней информационной системой или информационно-телекоммуникационной сетью.

Доверенная загрузка – загрузка операционной системы средств вычислительной техники с заранее определённых постоянных машинных носителей при обязательном успешном прохождении процедур проверки целостности программной и аппаратной среды и идентификации и аутентификации.

Доверенный канал – механизм взаимодействия между средствами защиты информационной системы или между средством защиты информации и программным обеспечением информационной системы.

Доверенный маршрут – механизм взаимодействия между субъектом доступа и средством защиты информации информационной системы.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защищённые линии связи – линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень её защищённости (конфиденциальность, целостность и (или) доступность информации).

Идентификатор – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имён) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Инцидент – непредвиденной или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент программного обеспечения – составная часть (программный модуль) программного обеспечения, выполняющий определённую функцию.

Компонент информационной системы – часть информационной системы, включающая некоторую совокупность информации и обеспечивающих её обработку отдельных информационных технологий и технических средств.

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

Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Локальный доступ – доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация – аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификация.

Мобильный код – несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты), получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах информационной системы (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

Непривилегированная учётная запись – учётная запись пользователя (процесса, выполняемого от его имени) информационной системы.

Объект доступа – единица информационной ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируются правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в т.ч. по обработке информации, содержащейся в её базах данных.

Отказ в обслуживании – препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций операционной системы.

Периметр информационной системы – физическая и (или) логическая граница информационной системы (сегмента информационной системы), в пределах которой

оператором обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты её функционирования.

Потенциал нарушителя – мера усилий, затрачиваемых при реализации угроз безопасности информации в информационной системе.

Привилегированная учётная запись – учётная запись администратора информационной системы.

Программная среда – совокупность программного обеспечения, используемого в информационной системе для решения одной или нескольких задач.

Роль – предопределённая совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Сегмент информационной системы – совокупность нескольких компонентов информационной системы, использующих общую (в т.ч. разделяемую) среду передачи и объединённых для единства решения функциональных задач.

Событие безопасности (информационной) – идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или приём информации в информационной системе.

Технологии мобильного кода – реализованные в программном обеспечении процессы создания и использования мобильного кода (в частности технологии Java, JavaScript, ActiveX, VBSScript).

Удалённый доступ – процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединённым физически или логически с информационной системой, к которой он получает доступа.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Устройство – конструктивно законченный технический элемент, имеющий определённое функциональное назначение в информационной системе.

Уязвимость информационной системы – недостаток (слабость) информационной системы, который (которая) создаёт потенциальные или реально существующие условия для реализации проявления угроз безопасности информации.

Хостовая операционная система – операционная система, в среде которой функционирует гипервизор.

Целостность информации – свойство безопасности информации, при котором отсутствует любое её изменение либо изменение субъектами доступа, имеющими на него право.

Общие положения

1.1. Настоящее Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности информации (далее - ОБИ) в ГАУЗ ТО «Областной кожно-венерологический диспансер» (далее – Учреждения).

1.2. Положение разработано на основании требований законодательства РФ в области информационной безопасности, нормативных и методических документов уполномоченных органов (ФСТЭК России, ФСБ России), а также правовых актов Тюменской области, действующих на момент разработки документа.

1.3. В Положении используются термины и определения, установленные законодательством Российской Федерации, национальными стандартами в области защиты информации.

1.4. В Учреждении обрабатывается общедоступная информация и информация ограниченного доступа, не составляющая государственную тайну, в том числе служебная информация (документы с пометкой «Для служебного пользования» «ДСП») и персональные данные (далее - ПДн).

1.5. Автоматизированная обработка информации осуществляется с использованием средств вычислительной техники (далее - СВТ) и различных информационных систем (далее - ИС) на автоматизированных рабочих местах (далее – АРМ пользователя) и серверах Учреждения.

1.6. Учреждение, как обладатель информации ограниченного доступа, обязан принимать меры по защите информации и ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

1.7. Требования к ОБИ формируются на основании установленных классов защищённости ИС (уровня защищенности ПДн) и перечня актуальных угроз безопасности информации.

1.8. Требования ОБИ реализуются комплексом организационных и технических мер, средств и механизмов защиты информации, определенных в документации системы защиты информации (далее - СЗИ).

1.9. Настоящие Положение обязательно для исполнения всеми работниками Учреждения (далее – работники).

2. Порядок организации работ по обеспечению безопасности информации

2.1. С целью организации работ по защите информации приказом главного Учреждения назначается должностное лицо, ответственное за защиту информации.

2.2. Функции, решаемые задачи и обязанности ответственного за защиту информации определены в Инструкции лица, ответственного за защиту информации, согласно приложению № 1 к настоящему Положению.

2.3. Непосредственное выполнение работ по реализации требований и мер безопасности информации в организации осуществляет администратор безопасности (далее - АБИ), назначаемый приказом главного Учреждения. Функции, решаемые задачи и обязанности АБИ определены инструкцией, согласно приложению № 2 к настоящему Положению.

2.4. Реализация требований ОБИ осуществляется всеми работниками Учреждения (администраторами, пользователями, эксплуатационным персоналом).

2.5. Обязанности и ответственность пользователей по ОБИ при ее обработке определены в Инструкции пользователя согласно приложению № 3 к настоящему Положению.

2.6. Работы по ОБИ в Учреждении осуществляются согласно Плану проведения мероприятий ОБИ Учреждения согласно приложению № 11 к настоящему Положению.

2.1. Все работы ОБИ подлежат учету в Журнале учета мероприятий по ОБИ согласно приложению № 12 к настоящему Положению.

3. Технологический процесс обработки информации

3.1. Технические средства и системы обработки информации (далее - ТС), места их размещения, программное обеспечение, используемое для обработки информации, а также используемые средства защиты информации и их характеристики подлежат учёту в Техническом паспорте объекта информатизации (далее - ОИ). Ответственность за ведение Технического паспорта ОИ и актуализацию сведений в нём возлагается на АБИ.

3.2. Все ТС Учреждения размещены в пределах контролируемой зоны (далее - КЗ). Режим обработки информации многопользовательский с разграничение прав доступа.

3.3. Обработка информации в Учреждении осуществляется в соответствии с Положением о порядке работы с информационными ресурсами согласно приложению № 4 к настоящему Положению.

3.4. Работа с информационными ресурсами Учреждения осуществляется в соответствии с правами разграничения доступа. Правила разграничения доступа назначаются администраторами. Доступ к информационным ресурсам осуществляется при помощи учётных записей пользователей.

3.5. Обработка информации предусматривает следующие действия с данными: сбор, накопление, хранение, использование, уточнение, передача, удаление (уничтожение). Новые данные вводятся вручную, посредством клавиатурного ввода, а также путём считывания в электронном виде.

3.6. Пользователи имеют право постоянного хранения файлов с данными на:

- жёстком диске АРМ пользователя;
- учтённом съёмном носителе информации (USB-накопители, оптические диски, гибкие магнитные диски).

3.7. Доступ к жесткому диску АРМ пользователя разрешен только АБИ. Учтенные съёмные носители информации выдаются пользователю под роспись.

3.8. Доступ к АРМ пользователей производится по идентификатору (логину) и паролю в соответствии с требованиями Инструкция по организации парольной защиты согласно приложению № 5 к настоящему Положению.

3.9. На АРМ пользователей устанавливается лицензионное либо свободно распространяемое общесистемное программное обеспечение (далее – ПО.

3.10. Обработка информации на АРМ пользователей осуществляется с использованием специализированного прикладного ПО и web-браузера.

3.11. Пользователи имеют доступ к ресурсам сети «Интернет» со своих АРМ.

3.12. В качестве вспомогательного средства для разработки документов на АРМ пользователей установлен программный пакет семейства «Мой офис» или «Р7.Офис».

3.13. Копии установленного на АРМ пользователей ПО хранятся у АБИ.

3.14. Обработка служебной информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (документов с пометкой «для служебного пользования») производится только на учтённых съёмных машинных носителях информации (далее - МНИ). Порядок и условия обработки служебной информации ограниченного доступа на АРМ пользователей определены положением по организации и проведению работ по защите служебной информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну в Учреждении.

4. Система защиты информации

4.1. Перечень объектов доступа

Объектами доступа являются:

–ТС, включая средства отображения информации;

–помещения, в которых размещены ТС;

–носители информации, включая съёмные носители информации и жёсткие магнитные диски (далее – ЖМД);

–базы данных (далее – БД) и каталоги файлов на съёмных носителях информации и ЖМД;

–общесистемное и специальное ПО, предназначенное для обработки информации и разработки документов;

–программные средства, осуществляющие функции по защите информации, а также функции контроля безопасности;

–каналы информационного обмена и телекоммуникации.

4.2. Перечень субъектов доступа

Субъектами доступа к защищаемой информации на ОИ являются:

–администратор безопасности информации;

–системный администратор;

–пользователи, работающие на АРМ;

–процессы, выполняемые от имени АБИ, системного администратора и пользователей при обработке информации и настройке средств защиты информации.

4.3. Штатные средства доступа к информации

В качестве штатных средств доступа на ОИ предусмотрены:

–стандартные средства операционной системы Windows;

–программные из пакета «Мои офис» или «Р7.Офис»;

–система управления базами данных (далее – СУБД) Directum;

–web-браузер;

–программы из пакета антивируса;

–средства настройки и контроля функций СЗИ.

4.4. Объекты защиты организации:

–ТС (в т.ч. СВТ, МНИ, средства и системы связи передачи данных);

–информация, хранящаяся и обрабатываемая на ТС;

–общесистемное, прикладное, специальное ПО;

–средства защиты информации.

4.5. Требования к средствам защиты информации

4.5.1. Все используемые программные и аппаратные СЗИ имеют действующие сертификаты на соответствие требованиям по безопасности информации, установленные Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю России.

4.5.2. Класс защищённости применяемых средств защиты информации должен соответствовать классу защищенности средств и систем обработки информации.

4.5.3. При обмене информацией между Учреждением и внешними по отношению к нему информационными системами, а также при передаче данных по кабельным системам, расположенным в пределах КЗ и не защищённым от НСД к информации организационно-техническими мерами, для обеспечения конфиденциальности информации требуется применение средств криптографической защиты информации (далее – СКЗИ).

4.5.4. Установку и настройку СЗИ разрешается проводить только АБИ.

4.5.5. Эксплуатация СЗИ должна осуществляться в строгом соответствии с правилами, установленными в Положении о применении шифровальных (криптографических) средств защиты информации в Учреждении.

4.6. Правила разграничения доступа

4.6.1. средствами СЗИ реализованы правила разграничения доступа, при которых каждый пользователь имеет доступ к:

- средствам ОС, обеспечивающим запуск и функционирование АРМ;
- средствам разработки документов;
- средствам антивирусного контроля;
- прикладному ПО;
- персональному каталогу на ЖМД, предназначенному для хранения информации;
- внешним накопителям данных, предназначенных для хранения информации;
- устройствам и средствам их программной поддержки, необходимым для работы с документами.

4.6.2. Доступ к средствам настройки и изменения полномочий доступа в СЗИ имеет только АБИ. Операции доступа к объектам доступа документируются средствами регистрации и учёта.

5. Средства защиты информации

5.1. Для защиты информации от несанкционированного доступа и воздействия вредоносных программ, на всех ТС Учреждения применяются сертифицированные средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД) и средства антивирусной защиты (далее - САВЗ).

5.2. Для защиты информации передаваемой по незащищенным каналам связи за пределы КЗ (во внешние системы) применяются СКЗИ. В установленных случаях могут использоваться средства электронной подписи.

5.3. СКЗИ и их носители подлежат учету в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. При этом программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

5.4. В локальной вычислительной сети (далее - ЛВС) Учреждения для обеспечения безопасности периметра ЛВС применяются сертифицированные средства межсетевого экранирования.

5.5. Для контроля защищенности ЛВС используется сетевой сканер безопасности.

5.6. Контроль настройки и работы используемых в Учреждении средств защиты информации осуществляет АБИ.

6. Реализация мер защиты

6.1. Идентификация и аутентификация субъектов доступа и объектов доступа

6.1.1. Применяемые на ОИ меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

6.1.2. Идентификация и проверка подлинности субъектов доступа при входе в систему осуществляется СЗИ от НСД с использованием персональных идентификаторов, а также по имени (логину) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

6.1.3. СЗИ от НСД не позволяет использовать для входа в систему незарегистрированные идентификаторы.

6.1.4. Правила и требования к парольной защите определены в Инструкции по организации парольной защиты согласно приложению № 5 к настоящему Положению.

6.1.5. Программы, тома, каталоги, файлы, записи, поля записей, терминалы, компьютеры (АРМ), узлы сети, каналы связи, внешние устройства, подключённые к АРМ, идентифицируются по именам при обращении к ним при помощи средств операционной

системы и СЗИ. Правильность предоставления доступа в соответствии с установленными правами субъектов по отношению к конкретным объектам (каталогам, устройствам) обеспечивается СЗИ и используемыми на ОИ сетевыми политиками безопасности.

6.2. Управление доступом субъектов доступа к объектам доступа

6.2.1. Применяемые меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных на ОИ правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

6.2.2. Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей на ОИ и выдача (замена) пользовательских персональных идентификаторов для СЗИ от НСД, осуществляется АБИ и системным администратором в соответствии с правилами и процедурами, определёнными в Положении о порядке работы с информационными ресурсами (Приложение № 4).

6.2.3. На ОИ реализован дискреционный метод разграничения доступа. В системе задействована функция блокирования органов управления АРМ при временном оставлении рабочего места. При использовании незарегистрированного пароля, либо пароля, зарегистрированного не для текущего пользователя, разблокировка системы невозможна. В системе применяется ограничение неуспешных попыток входа в систему. При превышении установленного количества неуспешных попыток входа система блокируется.

6.3. Ограничения программной среды

6.3.1. Цель принятия мер по ограничению программной среды – обеспечение установки и (или) запуска только разрешённого к использованию в организации программного обеспечения и исключения возможности установки и (или) запуска запрещённого к использованию на ОИ программного обеспечения.

6.3.2. Контроль установки (инсталляции) разрешённого к использованию ПО и (или) его компонентов осуществляется АБИ и системным администратором на основе журналов регистрации событий операционной системы и средств антивирусного контроля АРМ.

6.3.3. Пользователи АРМ не имеют права самостоятельно устанавливать ПО.

6.3.4. Установка ПО на АРМ пользователей производится в соответствии с требованиями и правилами, установленными в Инструкции по модификации технических и программных средств согласно приложению № 6 к настоящему Положению.

6.4. Защита машинных носителей информации

6.4.1. Защита машинных носителей информации (средства обработки (хранения) информации, съёмные машинные носители информации) обеспечивается организационно-режимными мероприятиями. Цель принятия мер по защите МНИ – исключение возможности несанкционированного доступа к МНИ и хранящейся на них информации, а также несанкционированное использование съёмных МНИ.

6.4.2. При передаче МНИ межу пользователями или в сторонние организации для ремонта или утилизации производится уничтожение (стирание) информации, а также контроль уничтожения (стирания).

6.4.3. Порядок учёта, хранения и использования съёмных МНИ (ГМД, USB-накопители и т.д.) определён в Положении о порядке работы с информационными ресурсами Учреждения согласно приложению № 4 к настоящему Положению.

6.5. Регистрация событий безопасности

6.5.1. Принимаемые меры по регистрации событий безопасности позволяют обеспечить сбор, запись, хранение и защиту информации о событиях безопасности, а также возможности просмотра и анализа информации о таких событиях.

6.5.2. Регистрация событий безопасности обеспечивается сертифицированными средствами защиты информации АРМ и серверов.

6.5.3. Регистрация, учёт и порядок реагирования на события безопасности регламентируются Положением о порядке выявления и реагирования на инциденты информационной безопасности согласно приложению № 7 к настоящему Положению.

6.6. Антивирусная защита

6.6.1. Целью принятия мер по антивирусной защите является обеспечение обнаружения компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СЗИ, а также реагирование на обнаружение этих программ и информации.

6.6.2. САВЗ установлены на всех АРМ и серверах, обрабатывающих информацию.

6.6.3. Применение САВЗ решает следующие задачи:

- автоматическое сканирование АРМ на наличие вирусных программ;
- автоматическое блокирование обнаруженных вирусных программ путём их удаления из программных модулей или уничтожения;
- проведение регулярного сканирования АРМ на наличие вирусов;
- реализация механизма обновления базы данных признаков вредоносных компьютерных программ (вирусов);
- ведение журналов событий безопасности.

6.6.4. Все используемые в организации МНИ подвергаются обязательному контролю на наличие компьютерных вирусов при помощи антивирусной программы. ЖМД находится под контролем антивирусной программы постоянно. При обнаружении вирусного кода он удаляется из программы. АБИ и (или) системным администратором периодически проводится антивирусный контролю ЖМД по расширенному алгоритму.

6.6.5. Обновление БД САВЗ производится по мере выпуска данных обновлений производителем.

6.6.6. Правила и требования, регламентирующие антивирусную политику определены в Инструкции по организации антивирусной защиты согласно приложению № 8 к настоящему Положению.

6.7. Контроль (анализ) защищённости информации

6.7.1. Мероприятия, проводимые в целях контроля и анализа защищённости информации, включают в себя:

- контроль состава ТС, ПО и СЗИ;
- выявление, анализ и устранение уязвимостей ПО и СЗИ;
- контроль установки обновлений ПО, включая ПО СЗИ;
- контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
- контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации полномочий пользователей и правил разграничения доступа пользователей в системе.

6.7.2. Используемые средства регистрации и учёта событий безопасности СЗИ позволяют АБИ контролировать неизменность конфигурации серверов, АРМ, файлов и реестров используемого ПО.

6.7.3. АБИ проводит периодическое обслуживание и тестирование функций СЗИ.

6.7.4. Порядок выполнения работ по выявлению, анализу и устранению уязвимостей ПО и СЗИ определён в Положении по организации контроля эффективности защиты информации согласно приложению № 9 к настоящему Положению.

6.8. Обеспечение целостности программного обеспечения и информации

6.8.1. Контроль целостности ПО (в т.ч. ПО СЗИ), установленного на АРМ пользователей и серверах, осуществляется средствами сертифицированных СЗИ и функциональными возможностями операционной системы (далее – ОС) АРМ и серверов.

6.8.2. В целях обеспечения возможности восстановления ПО, в случае возникновения нештатных ситуаций, организовано хранение:

- дистрибутивов используемого системного и прикладного ПО;
- дистрибутивов с ПО для СЗИ;
- файлов, содержащих конфигурации и настройки СЗИ.

6.8.3. Для обеспечения возможности восстановления информации, содержащейся в файлах, папках и БД, выполняется периодическое резервное копирование критически важных информационных ресурсов на внешние системы хранения данных.

6.9. **Обеспечение доступности информации**

6.9.1. Доступность информации обеспечивается:

- использованием отказоустойчивых ТС;
- выявлением, анализом и устранением уязвимостей ПО;
- резервированием ТС, ПО и каналов передачи информации;
- периодическим резервным копированием информации.

6.9.2. На основе мониторинга и анализа сообщений в электронных журналах учёта событий СЗИ проводится периодическая проверка работоспособности серверного и телекоммуникационного оборудования, каналов связи, средств обработки и защиты информации (в т.ч. направлением текстовых сообщений и принятием «ответов», визуального контроля, контроля трафика, контроля «поведения» системы и иными методами).

6.9.3. В целях восстановления доступности информационных ресурсов после аппаратных или программных сбоев организовано периодическое резервное копирование информации на систему хранения данных.

6.9.4. Контроль за выполнением резервного копирования возложен на АБИ и системного администратора. Восстановление системы и информации осуществляется АБИ и системным администратором.

6.9.5. Реализация мер, направленных на поддержание непрерывности работы средств и систем обработки информации осуществляется в соответствии с Порядком резервирования и восстановления работоспособности ТС, ПО и СЗИ согласно приложению № 10 к настоящему Положению.

6.10. **Защита технических средств**

6.10.1. Помещения, в которых размещены средства и системы обработки информации (ТС), расположены в пределах КЗ. Доступ в помещения имеет ограниченный круг лиц. Реализуемые в организации меры по защите ТС направлены на исключение НСД:

- к стационарным ТС, обрабатывающим информацию;
- к средствам, обеспечивающим функционирование ОИ;
- в помещения, в которых постоянно расположены ТС.

6.10.2. Порядок доступа в помещения организации осуществляется в соответствии с Положении о порядке работы с информационными ресурсами Учреждения согласно приложению № 4 к настоящему Положению.

6.11. **Защита средств и систем связи и передачи данных**

6.11.1. Для обеспечения безопасного межсетевого взаимодействия используются сертифицированные средства межсетевого экранирования (далее - СМЭ). СМЭ выполняют фильтрацию входящего и исходящего трафика на различных уровнях стека протоколов, регистрацию и учёт событий системы, а также обеспечивает установление защищённых (шифрованных) соединений между узлами, принадлежащими разным организациям и (или) разным информационным системам.

6.11.2. Для обеспечения защиты информации при передаче по незащищённым каналам связи применяются сертифицированные СКЗИ.

6.11.3. Порядок и правила, определяющие действия пользователей при использовании ресурсов и сервисов сети Интернет, установлены в Инструкции по обеспечению безопасности при работе в сети Интернет (Приложение № 13).

6.11.4. Эксплуатация СКЗИ осуществляется в соответствии с Положением о применении шифровальных (криптографических) средств защиты информации в Учреждении).

6.12. **Управление конфигурацией систем обработки и защиты информации**

6.12.1. Управление конфигурацией ОИ, а также СЗИ, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений обеспечивается АБИ и системным администратором.

7. Информирование по вопросам обеспечения безопасности информации

7.1. Ознакомление работников с правилами работы с информацией осуществляется:

–путем проведения руководителями структурных подразделений Учреждения первичных инструктажей с вновь принятыми работниками по соблюдению установленных правил обработки и защиты информации;

–путем проведения обучения работников (пользователей средств вычислительной техники) администратором безопасности правилам работы с используемыми средствами защиты информации;

–путем самостоятельного изучения работником документов, регламентирующих вопросы ОБИ в Учреждении.

7.2. Допуск работников к информационным ресурсам Учреждения осуществляется только после прохождения первичного инструктажа и ознакомления с документами по вопросам обеспечения ИБ.

7.3. При проведении первичного инструктажа нового пользователя должны быть разъяснены:

–права и обязанности пользователя при работе с информационными ресурсами Учреждения;

–действия, которые запрещены в отношении информации, составляющей информационные ресурсы Учреждения

–порядок и условия работы с информацией ограниченного доступа;

–возможные последствия и ответственность в случае нарушения правил работы с информационными ресурсами Учреждения (информацией ограниченного доступа).

8. Контроль принятых мер по обеспечению безопасности информации

8.1. Организация контроля выполнения мероприятий информационной безопасности возлагается на ответственного за ОБИ в Учреждении.

8.2. Руководители структурных подразделений Учреждения осуществляют повседневный контроль выполнения требований по ОБИ в своих подразделениях.

8.3. АБИ Учреждения осуществляет текущий контроль выполнения требований по ОБИ в рамках выполнения своих обязанностей.

8.4. Мероприятия по контролю ОБИ в Учреждении проводятся в соответствии с Планом внутренних проверок состояния защиты информации.

8.5. Контроль эффективности принятых мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации согласно приложению № 11 к настоящему Положению