Государственное учреждение здравоохранения «Узловская районная больница»

П Р И К А З

29.04.2019 № 93

Об утверждении Положения об обеспечении безопасности персональных данных в информационной системе персональных данных «Медицинская информационная система ГУЗ «Узловская РБ»»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» п р и к а з ы в а ю :

1. Утвердить Положение об обеспечении безопасности персональных данных в информационной системе персональных данных «Медицинская информационная система **ГУЗ «Узловская РБ»**» (приложение № 1).
2. Ответственность за соблюдение Положения об обеспечении безопасности персональных данных в информационной системе персональных данных «Медицинская информационная система **ГУЗ «Узловская РБ»**» возложить на ответственного за обеспечение безопасности персональных данных в **ГУЗ «Узловская РБ»**.
3. Контроль исполнения приказа оставляю за собой.
4. Приказ вступает в силу со дня подписания.

Главный врач **Федоров С.С.**

28

Приложение №1
к приказу **ГУЗ «Узловская РБ»**
от «29» 04 2019 г. № 73

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных в информационной системе персональных данных «Медицинская информационная система ГУЗ «Узловская РБ»»

г. Тула

2018 год

Содержание

Сокращения, условные обозначения, термины 3
Введение 4
1. Цель и область применения 5
2. Состав мероприятий по обеспечению безопасности ПДн 6
2.1. Организационные мероприятия по обеспечению безопасности ПДн 6
2.2. Технические мероприятия по обеспечению безопасности ПДн 6
3. Порядок реализации мероприятий по обеспечению безопасности ПДн 7
3.1. Распределение ответственности за реализацию мероприятий по обеспечению безопасности ПДн 7
3.2. Определение состава ПДн, ИСПДн, носителей ПДн и технологии обработки ПДн 8
3.3. Определение порядка обработки ПДн в ИСПДн. Определение порядка работы с носителями ПДн 9
3.4. Определение порядка доступа к ПДн работников учреждения 10
3.5. Определение уровня защищенности ИСПДн 10
3.6. Разработка частной модели угроз 11
3.7.Разработка, внедрение, эксплуатация и контроль эффективности СЗПДн 11
3.8.Порядок реагирования на инциденты информационной безопасности 19
3.9.Оценка эффективности реализованных в рамках СЗПДн мероприятий по обеспечению безопасности ПДн 23
4. Порядок пересмотра 23

Сокращения, условные обозначения, термины

АРМ	– автоматизированное рабочее место
БД	– база данных
ИБ	– информационная безопасность
ИС	– информационные системы
ИСПДн	– информационные системы персональных данных
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевое экранирование
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки
СЗПДн	– система защиты персональных данных
СКЗИ	– средства криптографической защиты информации
СУБД	– система управления базами данных
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю Российской Федерации
ФСБ России	– Федеральная служба безопасности Российской Федерации

Введение

Настоящее Положение определяет состав мероприятий по обеспечению безопасности ПДн при их обработке в информационной системе персональных данных «Медицинская информационная система **ГУЗ «Узловская РБ»»** (далее – ИСПДн), а также порядок их реализации и контроля эффективности.

Требования Положения распространяются на все подразделения **ГУЗ «Узловская РБ»** (далее – Учреждение), а также на юридические лица и индивидуальных предпринимателей, осуществляющих сопровождение, обслуживание и обеспечение функционирования ИСПДн Учреждения (далее – Обслуживающие организации).

Данное Положение разработано в соответствии со следующими нормативными документами:

- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации, правовыми и методическими документами ФСТЭК России и ФСБ России.

1. Цель и область применения

Цель Положения – определение состава, порядка организации и проведения мероприятий по защите информации, содержащей персональные данные, обрабатываемые в ИСПДн Учреждения, для предотвращения ущерба в результате разглашения, утраты, утечки, искажения и уничтожения персональных данных, их незаконного использования и иных несанкционированных действий, приводящих к нарушениям работы ИСПДн Учреждения.

Требования настоящего Положения обязательны для всех подразделений Учреждения и распространяются на:

- ИСПДн Учреждения;
- информационно-телекоммуникационную сеть;
- съемные машинные носители ПДн (далее носители ПДн);
- помещения, в которых ведется обработка ПДн;
- работников Учреждения, органы исполнительной власти Тульской области, взаимодействующих с Учреждением в процессе обработки ПДн, обслуживающие организации.

Новые документы, регламентирующие защиту персональных данных в Учреждении, должны разрабатываться с учетом настоящего Положения и не противоречить ему.

2. Состав мероприятий по обеспечению безопасности ПДн

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках существующей СЗПДн.

2.1. Организационные мероприятия по обеспечению безопасности ПДн

Организационные мероприятия по обеспечению безопасности ПДн включают в себя:

- распределение ответственности за реализацию мероприятий по обеспечению безопасности ПДн и контроль их эффективности. Разработка инструкций, регламентирующих функции и обязанности лиц, обеспечивающих безопасность ПДн в ИСПДн;
- определение перечня работников Учреждения, участвующих в обработке ПДн или получивших к ним доступ. Определение необходимых правил доступа работников Учреждения к ПДн;
- определение правил обработки ПДн в ИСПДн. Определение правил использования носителей ПДн;
- мероприятия по обеспечению физической безопасности ИСПДн;
- контроль за выполнением мероприятий по обеспечению безопасности ПДн;
- оказание консультаций работникам Учреждения, обрабатывающим ПДн, а также лицам, ответственным за обеспечение безопасности ПДн.

2.2. Технические мероприятия по обеспечению безопасности ПДн

Технические мероприятия по обеспечению безопасности ПДн включают в себя:

- определение перечней ПДн, ИСПДн, носителей ПДн и технологии обработки ПДн;
- определение уровня защищенности ПДн для выявления базового набора мер по обеспечению безопасности ПДн;
- разработку частной модели угроз для выявления дополнительных мер по обеспечению безопасности ПДн с целью нейтрализации актуальных угроз;
- разработку и внедрение СЗПДн;
- периодические проверки функционирования и корректности настроек компонентов СЗПДн, аудит событий, генерируемых СЗИ;
- обработку инцидентов безопасности;
- регистрацию изменений в ИСПДн и СЗПДн, оценку их влияния на безопасность ПДн;

- восстановление ИСПДн и ПДн в случае возникновения обстоятельств, повлекших потерю данных или сбои в работе ИСПДн;
- оценку эффективности СЗПДн.

3. Порядок реализации мероприятий по обеспечению безопасности ПДн

3.1. Распределение ответственности за реализацию мероприятий по обеспечению безопасности ПДн

В Учреждении должно быть определено лицо, ответственное за обеспечение безопасности ПДн (далее – ответственный за БПДн).

В целях организации работ по защите ПДн ответственный за БПДн осуществляет следующие функции:

- участвует в разработке, согласовании документов Учреждения, регламентирующих защиту ПДн, а также внесении в них изменений;
- организовывает установку и настройку СЗИ с привлечением обслуживающей организации, либо производит самостоятельно;
- самостоятельно либо с привлечением обслуживающей организации проводит контроль функционирования и корректности настроек СЗИ, отслеживает события, генерируемые СЗИ;
- участвует в проведении внутренних проверок по обеспечению безопасности ПДн;
- выявляет и обрабатывает инциденты информационной безопасности;
- выявляет слабые места в СЗПДн и вносит предложения по их устранению;
- иные функции, предусмотренные инструкцией ответственного за БПДн.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждения в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридические лица или индивидуальные предприниматели, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Ответственный за БПДн в рамках проведения работ по обеспечению безопасности ПДн взаимодействует с ответственным за организацию обработки ПДн Учреждения и обслуживающими организациями.

Работники Учреждения, а также обслуживающие организации обязаны выполнять правила обеспечения безопасности, определенные в соответствующих инструкциях.

3.2. Определение состава ПДн, ИСПДн, носителей ПДн и технологии обработки ПДн

На данном этапе осуществляется сбор начальной информации, на основании которой должна строиться СЗПДн. Также необходимо периодическое проведение данных мероприятий для проверки актуальности имеющихся данных о составе ПДн и ИСПДн. В случае изменения в составе, расположении или принципах взаимодействия элементов ИСПДн должна быть проведена оценка влияния данных изменений на безопасность ПДн.

3.2.1. Определение ПДн, обрабатываемых в ИСПДн Учреждения

Устанавливаются все категории ПДн, которые обрабатываются в ИСПДн Учреждения, цели и правовое обоснование обработки ПДн, соответствие содержания и объема обрабатываемых ПДн заявленным целям.

3.2.2. Определение ИСПДн и ее сегментов, участвующих в хранении и обработке ПДн

Перечень информационных систем персональных данных определяется путем составления технического паспорта для каждой информационной системы. Для каждой информационной системы в техническом паспорте определяются, перечень программных и технических средств, схемы взаимодействия технических средств и их расположения.

3.2.3. Определение носителей ПДн

Необходимо определить, на каких носителях ПДн будет обрабатываться и храниться информация, содержащая ПДн. Составляется перечень носителей ПДн с указанием мест их хранения и сотрудников, работающих с данными носителями или имеющих к ним доступ.

3.2.4. Определение технологии обработки ПДн

Необходимо определить принцип взаимодействия элементов ИСПДн Учреждения между собой, со сторонними ИС, в которых обрабатываются ПДн, а также каналы связи, участвующие в их взаимодействии. Учитываются как цифровые каналы связи, так и физические методы передачи данных на носителях ПДн. Устанавливается и описывается среда передачи данных с указанием используемых технологий, протоколов и лиц, ответственных за обеспечение безопасности ПДн при их передаче по каналам связи.

3.3. Определение порядка обработки ПДн в ИСПДн. Определение порядка работы с носителями ПДн

Необходимо определить стадии жизненного цикла обработки ПДн и требования по порядку обработки ПДн на каждом этапе. Этапы жизненного цикла обработки ПДн включают в себя:

3.3.1. Внесение ПДн в ИСПДн

На данном этапе осуществляется сбор информации, содержащей ПДн, и занесение ее в ИСПДн для последующей обработки.

При этом должны учитываться предъявляемые требования безопасности, в частности:

- собираться и заноситься в ИСПДн должны только те ПДн, которые необходимы для реализации функций Учреждения;
- информация, содержащая ПДн, должна быть получена на законном основании или с согласия субъекта ПДн;
- должны регистрироваться факты внесения ПДн в ИСПДн.

3.3.2. Хранение ПДн

Хранение ПДн должно осуществляться на учтенных носителях ПДн, разрешенных к использованию в ИСПДн.

Должна быть обеспечена безопасность ПДн во время их хранения на носителях ПДн. Защита ПДн во время их хранения обеспечивается:

- подсистемой обеспечения физической защиты, в частности хранением носителей ПДн в защищенном месте (сейф, металлический шкаф);
- хранением ПДн в защищенном виде. Возможно использование криптографических средств защиты информации;
- использованием подсистемы разграничения доступа СЗПДн для исключения несанкционированного доступа к ПДн;
- резервированием ПДн на съемные машинные носители, хранящиеся в защищенном месте.

3.3.3. Предоставление доступа к ПДн

Защита ПДн в ИСПДн Учреждения от НСД обеспечивается подсистемой разграничения доступа. Для возможности обработки ПДн работникам Учреждения должны быть предоставлены необходимые права доступа к ним.

Порядок доступа к ПДн и элементам ИСПДн должен быть регламентирован соответствующим локальным документом.

Доступ к ПДн в ИСПДн предоставляется работникам Учреждения в соответствии с их должностными обязанностями по заявке в обслуживающую организацию, содержащей указание необходимости получения прав доступа и утвержденной руководителем Учреждения.

Права доступа к ПДн должны фиксироваться в разрешительной системе доступа.

3.3.4. Уничтожение ПДн

Уничтожение ПДн осуществляется в соответствии с установленными правилами обработки ПДн.

Факты уничтожения ПДн должны актироваться с указанием сотрудников, осуществлявших уничтожение, перечня удаленных данных, а также причины и даты удаления.

3.4. Определение порядка доступа к ПДн работников учреждения

Необходимо определить, в рамках каких работ и функциональных обязанностей работникам необходимо предоставление доступа к ПДн. Определяется перечень работников, выполняющих данные работы и их роли, в соответствии с которыми назначаются требуемые права доступа. Определяется тип и срок предоставления доступа к ПДн для выполнения функциональных обязанностей.

3.5. Определение уровня защищенности ПДн при их обработке в ИСПДн

На основании постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется уровень защищенности ПДн при их обработке в ИСПДн Учреждения. Для определения уровня защищенности формируется комиссия, состоящая из представителей Учреждения. Допускается включение в состав комиссии сотрудников сторонних организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации.

В соответствии с уровнем защищенности определяется перечень базовых мер по обеспечению безопасности ПДн на основании приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.6. Разработка частной модели угроз

На основании методических документов ФСТЭК России и ФСБ России разрабатывается частная модель угроз безопасности ПДн. Данный документ описывает актуальные угрозы для ИСПДн Учреждения, показатели их опасности и возможность реализации, а также набор дополнительных мер по обеспечению безопасности ПДн, выполнение которых необходимо для нейтрализации актуальных угроз.

3.7. Разработка, внедрение, эксплуатация и контроль эффективности СЗПДн

СЗПДн состоит из следующих подсистем:

- подсистема разграничения доступа субъектов доступа (пользователи и процессы) к объектам доступа (информационные и технические ресурсы), предотвращающая несанкционированный доступ к ПДн;
- подсистема межсетевого экранирования, позволяющая реализовать сегментацию ЛВС и управление сетевым взаимодействием;
- подсистема регистрации и учета действий пользователей в ИСПДн;
- подсистема обеспечения целостности ПДн и ИСПДн;
- подсистема антивирусной защиты, позволяющая выявлять и устранять угрозы, связанные с вредоносным ПО;
- подсистема криптографической защиты ПДн;
- подсистема выявления уязвимостей в СЗПДн ИСПДн;
- подсистема физической защиты ПДн и элементов ИСПДн от несанкционированного доступа к ним.

Используемые в СЗПДн СЗИ должны пройти процедуру оценки соответствия в рамках сертификации ФСТЭК России и ФСБ России. На этапе внедрения и в процессе эксплуатации СЗПДн должен вестись учет используемых средств защиты.

3.7.1. Защита ПДн от НСД

Защита ПДн от НСД обеспечивается использованием мер по ограничению несанкционированного доступа к ПДн. Эффективность используемых мер достигается при условии соблюдения установленного порядка обработки ПДн в ИСПДн, что обеспечивается выполнением требований регламентирующих документов и инструкций по работе в ИСПДн.

3.7.1.1. Подсистема разграничения доступа и подсистема межсетевого экранирования

Система управления доступом позволяет регистрироваться в системе только авторизованным пользователям, при этом для авторизации используется сочетание логина, пароля, а в отдельных случаях и физического (iButton, eToken, RuToken) или программного ключа (файл .dst), что снижает вероятность несанкционированного доступа в случае компрометации каких-либо авторизационных данных.

Дополнительно осуществляется ограничение прав пользователей до минимально необходимых, что снижает возможность использования альтернативных способов получения доступа к ПДн.

Подсистема управления доступом внедряется на АРМ сотрудников, участвующих в обработке ПДн, и в системах, в которых обрабатываются ПДн.

В рамках подсистемы управления доступом используются встроенные механизмы операционной системы Microsoft Windows, позволяющие осуществлять управление доступом сотрудников на рабочие станции, серверы, к файлам и таблицам БД, хранящимся в СУБД, а также встроенные механизмы разграничения доступа в программном обеспечении используемом ИСПДн для обработки ПДн.

Должны быть реализованы системы разграничения доступа к модулям управления подсистем СЗПДн, позволяющие осуществлять безопасную авторизацию, в том числе удаленных пользователей в случае необходимости, и предотвратить получение несанкционированного доступа к средствам администрирования СЗПДн.

Используемые подсистемы МЭ позволяют предотвратить доступ в ИСПДн из других сегментов информационных систем персональных данных Учреждения, из внешней сети Интернет и с неавторизованных узлов. Также подсистема МЭ позволяет установить набор правил доступа, предотвращающих какой-либо вид доступа, кроме установленного и необходимого для функционирования ИСПДн.

Подсистемы межсетевого экранирования используются на границах сегментов ЛВС и АРМ Учреждения.

Внедрение подсистем управления доступом и межсетевого экранирования осуществляется в соответствии со стандартами и правилами их настройки ответственными за БПДн, либо обслуживающей организацией.

3.7.1.2. Подсистема физической защиты ПДн и ИСПДн от НСД к ним

Доступ в помещения, где ведется обработка ПДн и располагаются элементы ИСПДн, должен осуществляется в соответствии с установленным в Учреждении, порядком доступа в помещения, в которых ведется обработка ПДн.

При этом должны выполняться следующие требования по обеспечению физической защиты ПДн:

- определение контролируемой зоны;
- использование мер обеспечения физической защиты охраняемых помещений;
- использование мер обеспечения физической защиты элементов ИСПДн и носителей ПДн.

За выполнение мер обеспечения физической безопасности в Учреждении ответственность несет руководитель Учреждения или лицо, исполняющее его обязанности. Контроль выполнения требований по обеспечению физической безопасности осуществляет лицо, определенное руководителем Учреждения.

3.7.1.3. Подсистема обеспечения целостности ПДн и ИСПДн

Обеспечение целостности ПДн и элементов ИСПДн и СЗПДн обеспечивается с помощью следующих мер:

- осуществление резервного копирования ПДн и критичных данных ИСПДн;
- осуществление мониторинга системных изменений и модификации данных;
- осуществление резервирования критичных узлов и подсистем обеспечения жизнедеятельности ИСПДн.

Необходимо осуществлять регулярное резервное копирование критичной информации. К критичной информации относятся:

- ПДн;
- конфигурационные файлы подсистем ИСПДн и СЗПДн;
- журналы аудита;
- информационное обеспечение ИСПДн и СЗПДн.

Резервные копии данных передаются в центр обработки данных по защищенным каналам связи.

Для осуществления резервного копирования информации в ИСПДн используется сертифицированный программно-аппаратный комплекс резервирования и восстановления, поддерживающий все используемые в

ИСПДн платформы и позволяющий вести библиотеку резервных копий с возможностью оперативного поиска и восстановления данных.

Настройка и использование программно-аппаратного комплекса подсистемы резервного копирования осуществляется сотрудниками обслуживающей организации в соответствии со стандартами настройки и инструкцией по выполнению резервного копирования.

Резервное копирование осуществляется в соответствии с регламентом резервного копирования, который должен определять данные для резервирования, периодичность и время копирования, а также периодичность цикла хранения резервных копий.

Ответственность за выполнение резервного копирования в ИСПДн несут работники обслуживающей организации.

В целях выявления фактов нарушения целостности необходимо осуществлять мониторинг системных изменений и модификации данных.

Подсистемы контроля целостности должны сигнализировать о модификации данных или среды их обработки, позволяя выявлять факты нарушения целостности и производить восстановление информации с резервных копий в случае необходимости.

В качестве подсистемы контроля целостности используется сертифицированный программно-аппаратный комплекс защиты от НСД, позволяющий осуществлять контроль нарушения целостности на всех уровнях ИС.

Для программно-аппаратных подсистем СЗПДн контроль целостности конфигурации должен осуществляться с помощью регулярного аудита, в том числе рассмотрения журналов доступа и изменений, а также проверки контрольных сумм файлов конфигурации.

Должна быть настроена система автоматизированного экстренного оповещения ответственных сотрудников о фактах нарушения целостности.

Настройка подсистемы контроля целостности осуществляется сотрудниками обслуживающей организации в соответствии со стандартами настройки.

В целях предотвращения аппаратных и программных сбоев элементов ИСПДн и возможной потери данных необходимо обеспечить резервирование критичных узлов и систем обеспечения их функционирования.

Специальные категории ПДн и критичные данные должны храниться и обрабатываться на отказоустойчивых электронных массивах хранения информации (применяется технология RAID).

Рекомендуется реализовать резервирование критичных ИС, используемых для обработки ПДн, и каналов связи.

Необходимо использовать источники бесперебойного питания, позволяющие корректно завершить работу ИС без потери данных.

3.7.1.4. Подсистема регистрации и учета

Использование подсистемы регистрации и учета позволяет осуществлять протоколирование фактов и попыток доступа к ПДн, а также осуществлять учет потоков и носителей ПДн. Данные записи могут быть использованы при расследовании инцидентов ИБ, а также в качестве дополнительной защиты от НСД.

Необходимо осуществлять регистрацию всех удачных и неудачных попыток осуществления доступа к ПДн как логическим, так и к физическим компонентам ИСПДн.

Необходима регистрация следующих данных:

- ИС, к которой осуществляется доступ;
- тип доступа;
- лицо, осуществляющее попытку доступа;
- данные или компонент, к которому осуществляется доступ;
- временная метка доступа;
- результат попытки доступа.

Должны регистрироваться и учитываться носители информации, содержащие ПДн. Учет носителей позволяет реализовать требования режима обработки и хранения ПДн, назначать сотрудников, ответственных за обеспечение безопасности конкретных носителей, осуществлять контроль использования и передачи ПДн.

В качестве технических мер в области регистрации и учета используется программно-аппаратный комплекс защиты от несанкционированного доступа, позволяющий вести детальную регистрацию действий пользователей в системе. Также используются встроенные системы протоколирования ОС Windows.

Настройка систем регистрации и учета осуществляется сотрудниками обслуживающей организации в соответствии со стандартами настройки и инструкциями по управлению данными системами.

Для регистрации учета съемных носителей ПДн используются журналы учета машинных носителей (персональных данных).

Учет физического доступа осуществляется в соответствии с порядком предоставления физического доступа. Учет носителей ПДн осуществляется в соответствии с порядком использования носителей ПДн.

За выполнение мер регистрации и учета ответственность несет ответственный за БПДн в Учреждении.

3.7.1.5. Подсистема антивирусной защиты

Необходимо обеспечить защиту ПДн и ИС, участвующих в их обработке и хранении, от вредоносного ПО. Для предотвращения угрозы несанкционированного доступа с использованием вредоносного ПО в ИСПДн используется подсистема антивирусной защиты.

Подсистема антивирусной защиты обеспечивает постоянную защиту ПДн, ПО и среды их обработки от воздействия вредоносного ПО. В рамках антивирусной защиты реализуются следующие действия:

- обнаружение вредоносных объектов в ОС и среде обработки данных;
- обнаружение вредоносных объектов в исполняемых файлах и процессах;
- сканирование и обнаружение вредоносных объектов в файловой системе;
- мониторинг удаленных подключений и обнаружение вредоносных объектов в передаваемых файлах;
- нейтрализация угроз от вредоносных объектов в соответствии с выбранными настройками (лечение, удаление, блокирование).

Должно выполняться регулярное обновление базы сигнатур вредоносных объектов для обеспечения требуемого уровня защиты.

В качестве подсистемы антивирусной защиты используется программный комплекс защиты от вредоносного ПО.

Настройка подсистемы антивирусной защиты осуществляется сотрудниками обслуживающей организации в соответствии со стандартами настройки и инструкциями по управлению данными системами.

Ответственность за обеспечение защиты ПДн от воздействия вредоносного ПО несет ответственный за БПДн.

3.7.1.6. Подсистема криптографической защиты

В целях защиты ПДн от НСД при их хранении и передаче используется подсистема криптографической защиты. Данная подсистема позволяет обеспечить безопасность ПДн даже в случае получения несанкционированного доступа к ним во время хранения и передачи.

В качестве подсистемы криптографической защиты используются сертифицированные средства.

Использование данных средств защиты позволяет реализовать безопасную передачу и хранение ПДн.

Настройка и использование подсистемы криптографической защиты осуществляется ответственными сотрудниками в соответствии со

стандартами настройки и инструкциями по управлению данными системами, либо сотрудниками обслуживающей организации.

Управление криптографическими ключами осуществляется обслуживающей организацией в соответствии с установленным регламентом.

3.7.2. Защита ПДн от ПЭМИН и утечек по техническим каналам

Для исключения утечки ПДн за счет ПЭМИН в ИСПДн реализуются следующие мероприятия:

- использование сертифицированных средств защиты информации;
- размещение объектов защиты на максимально возможном расстоянии относительно границы защищаемой территории;
- контроль защищаемой территории на предмет обнаружения устройств несанкционированного съема информации.

В ИСПДн для обработки информации рекомендуется использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности и эргономическим требованиям к средствам отображения информации, и санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Для исключения просмотра текстовой и графической видовой информации, выводимой устройствами отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн, рекомендуется оборудовать помещения, в которых они установлены, шторами (жалюзи).

3.7.3. Проверка функционирования и корректности настроек компонентов СЗПДн, аудит событий, генерируемых компонентами СЗПДн

Проверка функционирования и корректности настроек компонентов СЗПДн, аудит событий, генерируемых компонентами СЗПДн, позволяют заблаговременно выявить и своевременно устранить потенциальные уязвимости СЗПДн. Необходимо проводить регулярный мониторинг состояния СЗПДн, полноты и достаточности мер по защите ПДн.

3.7.3.1. Мониторинг состояния СЗПДн

Мониторинг состояния СЗПДн позволяет своевременно выявить и предотвратить сбои в работе компонентов СЗПДн, а также обнаружить

нарушения ИБ, связанные с некорректной настройкой подсистем СЗПДн. Данный процесс включает в себя:

- мониторинг состояния компонентов СЗПДн. Позволяет выявлять отклонения в условиях функционирования аппаратных или программных компонентов СЗПДн и осуществляется сотрудниками обслуживающей организации с помощью ПО, предназначенного для контроля отклонений в функционировании СЗПДн;
- аудит настроек компонентов СЗПДн. Осуществляется сотрудниками обслуживающей организации на ежеквартальной основе и представляет собой процесс проверки соответствия реальных настроек компонентов СЗПДн установленным требованиям.

3.7.3.2. Аудит событий, генерируемых компонентами СЗПДн

Аудит событий, генерируемых компонентами СЗПДн, направлен на обнаружение фактов и попыток (преднамеренного и непреднамеренного) нарушения информационной безопасности ПДн пользователями. Данная мера позволяет выявить нарушителей, создает информационную базу, необходимую для расследования инцидентов безопасности, и позволяет обнаруживать потенциальные уязвимости в ИСПДн.

Аудит событий, генерируемых компонентами СЗПДн, осуществляется автоматизировано с использованием подсистем регистрации и учета, подсистемы контроля целостности, а также подсистем управления доступом и межсетевого экранирования. В данной подсистеме должны быть настроены автоматизированные действия по информированию ответственных за БПДн о событиях, важных с точки зрения ИБ. Настройка оповещений осуществляется в соответствии со стандартами конфигурации данных подсистем. Необходимо осуществлять регулярную проверку событий в СЗПДн для выявления событий, не учтенных автоматизированной системой оповещения.

3.7.3.3. Тестирование средств и процедур безопасности

Тестирование средств и процедур безопасности направлено на выявление существующих или потенциальных уязвимостей ИСПДн и СЗПДН, определение полноты применяемых мер по защите ПДн. Тестирование состоит из анализа защищенности ИСПДн с помощью автоматизированных средств, а также системного анализа состояния ИСПДн и СЗПДн и мер по обеспечению безопасности ПДн.

Автоматизированный анализ защищенности ИСПДн осуществляется с помощью сетевого сканера безопасности, позволяющего выявлять уязвимости в используемых ИС. Данная процедура выполняется

сотрудниками обслуживающей организации в соответствии с регламентом анализа защищенности.

Анализ состояния ИСПДн и СЗПДн включает в себя:

- мониторинг актуальности используемого ПО и появления новых уязвимостей в нем для своевременного обновления и принятия необходимых мер по обеспечению безопасности;
- анализ существующих рекомендаций и стандартов по обеспечению безопасности используемых ИС и поддержание имеющихся стандартов по настройке и оперированию ИС в актуальном состоянии;
- регулярный анализ и пересмотр имеющихся процедур обеспечения безопасности ПДн.

3.8. Порядок реагирования на инциденты информационной безопасности

В целях защиты ПДн при выявлении инцидента безопасности определяется порядок реагирования на угрозы нарушения безопасности, который позволит максимально снизить возможные последствия и своевременно устранить инцидент.

Процедура реагирования на инциденты информационной безопасности состоит из следующих стадий:

- обнаружение инцидента;
- регистрация инцидента;
- обработка инцидента;
- уведомление необходимых лиц о произошедшем инциденте;
- устранение инцидента информационной безопасности;
- анализ инцидента.

3.8.1. Обнаружение инцидента ИБ

Инцидент информационной безопасности может быть обнаружен и зафиксирован следующими лицами:

- системным администратором ИС в ходе анализа недоступности информационной системы или отдельных сервисов;
- ответственным за БПДн;
- сотрудниками обслуживающей организации.

Предположение об инциденте информационной безопасности делается на основе следующих событий:

- об инциденте сообщают сотрудники;
- в ходе мониторинга или аудита ИСПДн или СЗПДн обнаруживается явный инцидент ИБ;

- в ходе анализа файлов журнала регистрации событий делается вывод о возможности инцидента ИБ;
- сообщений подсистемы аудита событий, генерируемых компонентами СЗПДн, или подсистемы обнаружения вторжений.

Обо всех событиях, которые пользователь классифицирует как нарушение нормального функционирования информационной системы, сотрудник сообщает ответственному за БПДн.

3.8.2. Регистрация инцидента ИБ

Инцидент должен быть зарегистрирован в Акте регистрации инцидента информационной безопасности.

При регистрации инцидента должны быть зафиксированы следующие сведения:

- Ф.И.О. сотрудника, обнаружившего инцидент;
- дата обнаружения;
- время обнаружения;
- сервис информационной безопасности, к которому относится инцидент;
- краткое описание инцидента.

3.8.3. Обработка инцидента ИБ

Под обработкой инцидента ИБ понимаются следующие действия:

- сбор дополнительной информации об инциденте ИБ;
- определение приоритета зарегистрированного инцидента ИБ.

Ответственный за БПДн обязан осуществить сбор дополнительной информации о зарегистрированном инциденте. К такой информации относятся:

- журналы событий;
- описание последовательности действий, которые привели к возникновению инцидента;
- статистика по аналогичным инцидентам, в том числе зарегистрированным за последний месяц (квартал).

Ответственный за БПДн обязан установить приоритет зарегистрированного инцидента, в соответствии с которым определяется время реагирования на инцидент и устранения его последствий, а также определяется план действий.

В случае регистрации инцидента, повлекшего разглашение ПДн, формируется комиссия для анализа, расследования и устранения инцидента.

3.8.4. Уведомление заинтересованных лиц о произошедшем инциденте ИБ

После регистрации инцидента производится уведомление ответственного за организацию обработки персональных данных в Учреждении, руководителя Учреждения, а также лиц, ответственных за устранение инцидента информационной безопасности. В зависимости от приоритета инцидента и возможных последствий нарушения информационной безопасности руководителем Учреждения дополнительно извещаются заинтересованные лица.

3.8.5. Устранение инцидента ИБ

Согласно выполненной классификации инцидента выбирается соответствующая процедура по устранению данного инцидента (предварительно разработанная и задокументированная).

Определяются сотрудники, ответственные за устранение инцидента.

Если процедуры устранения данного вида инцидентов не существует, то ответственный работник обязан ликвидировать его на основе имеющихся знаний, умений и навыков либо подключить других компетентных работников. При этом все действия, необходимые для устранения инцидента информационной безопасности, документируются.

Мероприятия по устранению последствий реализации угроз безопасности ПДн и проведению работ по восстановлению нормального функционирования ИСПДн могут включать в себя:

- восстановление данных и ПО с резервных копий;
- антивирусные мероприятия при возникновении вирусных заражений;
- смену паролей;
- восстановление настроек ИС (права доступа, настройки безопасности, настройки обеспечения взаимодействия ИС и т.д.);
- анализ и устранение выявленных уязвимостей;
- восстановление или замену аппаратных элементов ИСПДн.

Сотрудник, назначенный ответственным за устранение инцидента, обязан внести информацию о его ликвидации в Журнал регистрации инцидентов информационной безопасности.

Инцидент считается исчерпанным, когда ответственный сотрудник согласно своей компетентной оценке выполнил все необходимые действия для устранения возможных и текущих проблем, связанных с инцидентом, а заявитель получил извещение о решении инцидента и подтвердил его успешное решение.

3.8.6. Анализ инцидента ИБ

Анализ инцидентов информационной безопасности проводит ответственный за БПДн. Под анализом инцидента информационной безопасности понимаются следующие действия:

- поиск причины возникновения инцидента;
- классификация инцидента как умышленного или неумышленного;
- идентификация нарушителя;
- сбор доказательств совершения инцидента;
- привлечение правоохранительных органов (в случае необходимости);
- анализ статистики подобных инцидентов;
- определение последствий инцидента информационной безопасности.

Для поиска причины возникновения инцидента, а также для дальнейшего расследования документируются все факты и доказательства произошедшего инцидента информационной безопасности, в том числе следующие данные:

- технические – информация, полученная от технических средств сбора и анализа данных (снифферы, IDS/IPS и др.);
- операционные – данные, собранные в процессе опроса сотрудников Учреждения.

Сбор доказательств совершения инцидента необходим для:

- привлечения к ответственности лиц за умышленные или непреднамеренные действия;
- анализа уязвимости информационной системы;
- ликвидации последствий инцидента информационной безопасности.

При классификации инцидента как умышленного производятся мероприятия по идентификации личности нарушителя.

Определение последствий инцидента информационной безопасности подразумевает оценку нанесенного ущерба, если его возможно представить в количественном виде.

После завершения устранения и анализа инцидента информационной безопасности по инициативе ответственного сотрудника может проводиться обсуждение его результатов совместно со всеми привлеченными и заинтересованными сторонами. По итогам обсуждения комиссия по расследованию инцидента делает соответствующие выводы об уязвимостях и угрозах информационной безопасности, а также определяет необходимые мероприятия по недопущению подобных инцидентов в будущем. Соответствующие выводы документируются и хранятся у ответственного за БПДн в Учреждении.

Ответственный за БПДн в Учреждении обеспечивает надежное защищенное хранение информации о произошедших инцидентах информационной безопасности. Доступ к данным сведениям других сотрудников возможен только в соответствии с их должностными обязанностями.

3.9. Оценка эффективности реализованных в рамках СЗПДн мероприятий по обеспечению безопасности ПДн

В соответствии с пунктом 4 части 2 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в рамках мероприятий по обеспечению безопасности необходимо провести оценку эффективности СЗПДн. Оценка эффективности проводится в форме первичной аттестации информационной системы по требованиям защиты информации и периодических проверок эффективности СЗПДн.

4. Порядок пересмотра

Внесение изменений в Положение может носить как регламентный характер, так и быть вызвано изменениями в системе информационной безопасности или нормативных документах.

Пересмотр Положения производится в следующих случаях:

- изменение законодательства в области защиты ПДн;
- регламентный пересмотр Положения;
- внесение изменений в регламентные документы Учреждения;
- внесение изменений в ИСПДн.

В случае внесения изменений в законодательство в области защиты ПДн необходимо провести пересмотр Положения для оценки его соответствия новым требованиям.

Регламентный пересмотр Положения производится раз в год и обусловлен необходимостью соответствия Положения текущему состоянию ИСПДн и используемых методов защиты ПДн.

Положение разрабатывается на основе концептуальных документов по информационной безопасности. В случае изменения взглядов на проблему защиты ПДн или целей обеспечения безопасности ПДн вносятся поправки в концептуальные нормативные документы и, как следствие, требуется пересмотр Положения.

В случае внесения изменений в ИСПДн Положение должно быть дополнено и/или исправлено, чтобы отвечать текущему состоянию ИСПДн.

При внесении изменений в Положение проводятся следующие мероприятия:

- обследование и анализ изменений в ИСПДн в целом, в СЗПДн, в системе нормативных и регламентных документов;
- внесение изменений в перечень защищаемых объектов и ресурсов (при необходимости);
- формулировка и описание дополнительных (измененных) требований к СЗПДн, мер и процедур защиты ПДн;
- утверждение изменений в Положении.