Администрация
муниципального района Кинельский
Самарской области

Распоряжение

от 29.07.19 № 553
г. Кинель

Об утверждении инструкций (правил, порядков) в сфере защиты информации

Руководствуясь Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», в соответствии с «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных в администрации муниципального района Кинельский», утверждёнными распоряжением администрации муниципального района Кинельский от 24.03.2015г. № 280, утвердить прилагаемые:

1. Инструкцию по организации парольной защиты информационных систем персональных данных (Приложение - 1);
2. Инструкцию по организации антивирусной защиты (Приложение -2);
3. Порядок организации системы защиты информации (Приложение -3);
4. Правила работы со средствами криптографической защиты информации (Приложение - 4);
5. Порядок резервирования баз данных и хранения резервных копий (Приложение - 5).

Глава муниципального района Кинельский **С.И.Колесник**

Исп. Мойкин 2-12-45

Приложение - 1

Утверждено:
Распоряжением администрации
м.р.Кинельский от 29.07.19 № 553

Инструкция
по организации парольной защиты информационных систем персональных данных

Данная инструкция регламентирует действия пользователей и обслуживающего персонала при работе с паролями.

1. Идентификация и проверка подлинности пользователя при входе в информационную систему персональных данных (далее - ИСПДн) осуществляется по паролю условно-постоянного действия или с использованием аппаратных средств.

2. Процесс генерации, использования, смены и прекращения действия паролей для администрирования систем возлагается на специалиста по информационным технологиям и технической защите информации администрации муниципального района Кинельский, который должен быть включен в список лиц, допущенных к обработке персональных данных.

3. Личные пароли генерируются первоначально централизованно с последующей заменой пользователем на рабочем месте. Личный пароль пользователь не имеет права сообщать никому.

4. Пароли генерируются специализированными программами или создаются с учетом следующих требований:

- длина пароля должна быть не менее шести буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих мест, словарные и жаргонные слова и т.д.), общепринятые сокращения (USER и т.п.), последовательности символов и знаков (111, qwerty, abcdef, 123456, 098765);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

5. Полная плановая смена паролей пользователей должна проводиться регулярно.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. В случае компрометации (утраты, разглашения, кражи, взлома) личного пароля пользователь ИСПДн должен немедленно предпринять меры в соответствии с п.6 настоящей Инструкции.

8. Хранение пользователем значений своих паролей на материальном носителе допускается только в личном, запираемом ящике (сейфе).

9. Список паролей пользователей ИСПДн должен храниться в опечатанном конверте или пенале у специалиста по информационным технологиям и технической защите информации IT-отдела, либо у руководителя подразделения.

Этот список может использоваться при технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.).

После использования работник, чей пароль был использован, обязан сразу после выхода на рабочее место сменить пароль на новые значения и передать на хранение лицу, указанному в первом абзаце данного пункта.

10. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

11. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

12. Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на ответственного за обеспечение безопасности ИСПДн.

Приложение - 2

Утверждено:
Распоряжением администрации
м.р.Кинельский от 29.07.19 № 553

Инструкция
по организации антивирусной защиты

Настоящая Инструкция предназначена для пользователей информационных систем персональных данных, а также – сотрудников, рабочее место которых оборудовано компьютерной техникой.

В целях обеспечения антивирусной защиты автоматизированных рабочих мест (далее – АРМ), в том числе АРМ, на которых установлены информационные системы персональных данных, вводится антивирусный контроль.

Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на специалиста по информационным технологиям и технической защите информации администрации муниципального района Кинельский.

1. Для обеспечения антивирусной защиты должно использоваться сертифицированное лицензионное антивирусное программное обеспечение.
2. **Запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации**.
3. Пользователи (сотрудники) при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
4. Ярлык антивирусной программы, как правило, находится в области уведомления (нижний правый угол экрана), в случае его отсутствия он должен быть вынесен в окно "Рабочий стол" операционной системы.
5. Обновление антивирусной программы, как правило, производится автоматически, в противном случае необходимо обратиться к специалисту по информационным технологиям и технической защите информации.
6. Периодическое тестирование всего установленного программного обеспечения на предмет компьютерных вирусов производится автоматически, в противном случае необходимо обратиться к специалисту по информационным технологиям и технической защите информации. В случае обнаружения подозрительных программ срабатывает антивирус и необходимо прекратить какие-либо действия на АРМ и обратиться к специалисту по информационным технологиям и технической защите информации.
7. В случае обнаружения вируса, не поддающегося лечению, специалист по информационным технологиям и технической защите информации принимает меры по восстановлению работы системы.

Приложение - 3

Утверждено:
Распоряжением администрации
м.р.Кинельский от 19.07.19 № 553

Порядок организации системы защиты информации

1. Общие положения

1.1 Настоящий порядок устанавливает организацию системы защиты информации в администрации муниципального района Кинельский.

1.2 Инструкция разработана на основе действующих в Российской Федерации правовых и нормативных документов по защите информации.

1.3 Система защиты информации (далее – СЗИ) представляет собой комплекс организационных мер с применением программно-аппаратных средств защиты информации и средств контроля эффективности защиты информации.

1.4 СЗИ реализуется в процессе создания и эксплуатации ИС. В рамках эксплуатации ИС с целью защиты информации выполняется следующий комплекс эксплуатационных мероприятий:

- осуществление руководства работами по обеспечению защиты информации;
- обеспечение кадровой политики органа (организации) в отношении СЗИ;
- выполнение работ по физической защите технических средств;
- техническое обслуживание и ремонт оборудования;
- сопровождение программного обеспечения;
- устранение неисправностей программных и технических средств;
- контроль выполнения установленных нормативными документами требований к эксплуатации СЗИ.

Эксплуатационные мероприятия должны обеспечивать установленный на этапе создания ИС уровень информационной безопасности ИС.

2. Организация эксплуатации

2.1 Функции эксплуатирующей организации может выполнять:

- администрация муниципального района Кинельский, являющаяся пользователем информационной системы (ИС);
- другая организация, не являющаяся пользователем ИС (привлекаемая, как правило, на конкурсной основе).

2.2 Эксплуатирующая организация осуществляет эксплуатацию ИС и СЗИ в соответствии с нормативной, технической, эксплуатационной документацией и требованиями настоящей инструкции.

2.3 Ответственность за обеспечение защиты информации в процессе эксплуатации ИС возлагается на руководителя эксплуатирующей организации.

2.4 Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИС возлагается на непосредственных исполнителей (пользователей, специалиста по информационным технологиям и защите информации).

2.5 За нарушение установленных требований по защите информации руководитель подразделения, отвечающий за эксплуатацию ИС, и/или непосредственный исполнитель (пользователь) привлекаются к административной или уголовной ответственности в соответствии с действующим законодательством.

2.6 Все виды работ, связанные с автоматизированной обработкой информации, проводятся в регламентном режиме или по разовым запросам, непосредственно пользователями или операторами. Перечень регламентных работ и их исполнители определяются в соответствующей организационно-распорядительной и эксплуатационной документации. В органе (организации) должны быть установлены порядок и должностные лица, имеющие право подписывать разовые запросы на обработку информации.

3. Общие требования по защите информации при эксплуатации информационной системы и системы защиты информации

3.1 Эксплуатация ИС и системы защиты информации в ее составе, должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией.

3.2 С целью предотвращения либо существенного затруднения проникновения в здания, помещения посторонних лиц, хищения технических средств, документов и носителей информации должна быть организована физическая защита помещений и собственно технических средств обработки информации с использованием технических средств охраны.

3.3 Должно быть организовано ограничение доступа персонала в помещения, где размещено коммутационное и серверное оборудование.

3.4 На период обработки защищаемой информации в помещениях, где размещаются средства обработки информации, могут находиться только лица, допущенные к обрабатываемой информации в установленном порядке. Допуск в эти помещения других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться только с санкции руководителя органа (организации) или руководителя подразделения, эксплуатирующего ИС. При этом должны быть соблюдены меры, исключающие ознакомление этих лиц с конфиденциальной информацией.

3.5 С целью исключения предоставления избыточных прав доступа к информации в процессе эксплуатации ИС должен осуществляться периодический пересмотр прав доступа пользователей к информации.

3.6 В случае размещения в одном помещении различных технических средств одной или нескольких ИС должен быть исключен несанкционированный просмотр конфиденциальной информации.

3.7 Учет, хранение и обращение с накопителями и носителями информации на бумажной, магнитной, оптической и иной основе должны осуществляться в соответствии с требованиями Руководящих документов ФСТЭК России и в соответствии с выбранным уровнем защищённости ИС.

Обращение с ключевыми документами средств криптографической защиты информации (СКЗИ), в случае их использования, должно осуществляться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

3.8 При увольнении или изменении должностных обязанностей пользователей, операторов, администраторов ИС по согласованию со специалистом по информационным технологиям и технической защите информации администрации муниципального района Кинельский в установленном в организации порядке должны быть приняты меры по оперативному изменению соответствующих паролей и прав доступа.

3.9 Эксплуатация антивирусных средств защиты должна осуществляться в соответствии с утверждённой Инструкцией по организации антивирусной защиты (см. Приложение – 2) содержащей порядок установки, обновления, использования антивирусных средств защиты, а также меры по восстановлению работоспособности ИС в случае поражения вирусом.

3.10 Резервное копирование (архивирование) баз данных должно осуществляться в соответствии с Порядком резервирования баз данных и хранения резервных копий (см. Приложение – 5). Восстановление функционирования ИС и обеспечение доступности информации на требуемом уровне и в требуемые сроки после сбоя или отказа оборудования и/или программного обеспечения должны осуществляться в соответствии с порядком, указанным в эксплуатационной документации. Неисправности должны регистрироваться, анализироваться, и в их отношении должны приниматься соответствующие действия.

3.11 Все пользователи и эксплуатационный персонал ИС должны сообщать в отдел информационных технологий администрации муниципального района Кинельский о любых наблюдаемых или предполагаемых событиях, связанных с возможными нарушениями и недостатками защиты информации.

3.12 В случае нарушений безопасности при эксплуатации ИС к нарушителям должны применяться соответствующие меры.

3.13 Контроль состояния и эффективности защиты информации осуществляется специалистом по информационным технологиям и технической защите информации администрации муниципального района Кинельский и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер, в проверке выполнения норм эффективности защиты информации ограниченного доступа.

4. Организационное обеспечение эксплуатации системы защиты информации.

4.1 Руководство администрации муниципального района Кинельский должно поддерживать обеспечение защиты информации в администрации с помощью эффективного управления СЗИ, четкого назначения и распределения обязанностей персонала по обеспечению защиты информации. При этом руководство должно проводить регулярную проверку

СЗИ и ее реализации (т.е. целей управления, правил, процессов и процедур по обеспечению защиты информации).
4.2 В договоре найма на работу и/или в должностной инструкции сотрудника администрации муниципального района Кинельский должны быть определены обязанности по обеспечению безопасности информации при обработке данных организации, а также меры, принимаемые в отношении сотрудника, если он нарушает требования безопасности. При заключении трудового договора сотрудник должен принять обязательства о выполнении оговоренных требований в течение определенного времени после увольнения.
4.3 Сотрудники администрации муниципального района Кинельский должны быть ознакомлены с требованиями и правилами по обеспечению защиты информации в части, их касающейся.
4.4 Права доступа сотрудников к информации должны изменяться при изменении их должности. После увольнения сотрудника все его права на доступ к какой-либо информации ИС должны быть аннулированы, все ранее предоставленные сотруднику технические средства и материалы должны быть возвращены.
4.5 Администрация муниципального района Кинельский устанавливает порядок подготовки и переподготовки кадров в области защиты информации.

5. Обслуживание и ремонт технических средств.

5.1 Обслуживание технических средств ИС, СЗИ (техническое обслуживание) организуется в целях предотвращения неисправностей, обеспечения долговечности компонентов системы.
5.2 При проведении технического обслуживания (ТО) и ремонта необходимо руководствоваться следующими правилами:
- технические средства необходимо обслуживать в соответствии с рекомендуемыми поставщиком периодичностью и инструкциями;
- ТО и ремонт должны проводиться только уполномоченным персоналом (уполномоченной организацией);
- необходимо регистрировать информацию обо всех видах ТО, ремонта и всех выявляемых в ходе работ неисправностях, а также об ошибочных сообщениях о неисправностях (когда на самом деле технические средства исправны); регистрационные журналы хранить в установленном порядке;
- на период выполнения ТО должны задействоваться соответствующие меры защиты с учётом выполнения работ персоналом эксплуатирующей или иной организации; где необходимо, конфиденциальная информация должна быть удалена;
- должны соблюдаться все требования, устанавливаемые гарантийными обязательствами поставщика технических средств.
5.3 Для технических средств должно быть предусмотрено проведение следующих видов ТО:
- ежедневное обслуживание;
- ежемесячное обслуживание;
- ежегодное обслуживание.
5.4 Процедура ежедневного ТО включает в себя:

- визуальный осмотр элементов устройств, входящих в состав технических средств (системного блока, монитора, клавиатуры, периферийного оборудования и т.д.);
- очистка поверхности элементов устройств от пыли и грязи;
- проверку состояния соединительных кабелей и разъемов (кабели должны быть уложены аккуратно и без сильных перегибов, а их разъемы надежно соединены с разъемами устройств).

Ежедневное обслуживание технических средств, размещенных на автоматизированных рабочих местах ИС, выполняют пользователи, а других средств – специалистом по информационным технологиям и защите информации.

5.5 Объемы ежемесячного и ежегодного ТО определяются в эксплуатационной документации.

5.6 Ответственность за своевременное и качественное проведение еженедельного и годового ТО, ремонта возлагается на пользователей и специалиста по информационным технологиям и защите информации.

6. Сопровождение программного обеспечения.

6.1 Сопровождение программного обеспечения СЗИ (ПО) включает мероприятия по анализу качества, устранению выявленных ошибок, внесению изменений в ПО и документацию, извещение пользователей об изменениях, ведение эталонной версии ПО.

6.2 При сопровождении ПО необходимо руководствоваться следующими правилами:
- проводить работы по сопровождению ПО только силами уполномоченного персонала;
- выполнять требования лицензионных соглашений на использование ПО в соответствии с законодательством в области прав на результаты интеллектуальной деятельности;
- руководствоваться документацией поставщиков при сопровождении общесистемного программного обеспечения, такого, как операционные системы и системы управления базами данных;
- при использовании сертифицированного по требованиям безопасности информации ПО, его настройку осуществлять и поддерживать в соответствии с техническими условиями или формуляром;
- проводить проверки целостности ПО периодически или после устранения неисправностей в порядке, установленном эксплуатационной документацией;
- регистрировать информацию обо всех случаях неисправностей и всех видах профилактических и восстановительных работ, а также об ошибочных сообщениях о неисправностях (когда в действительности ПО функционирует корректно);
- хранить регистрационные журналы в установленном порядке;
- принимать дополнительные меры по исключению несанкционированного доступа к конфиденциальной информации, хранящейся в системе, при участии в сопровождении организаций – соисполнителей работ;
- устанавливать режим изолированной программной среды, исключающей возможность изменения пользователем состава ПО, если это не противоречит эксплуатационной документации;

- пересматривать объем и содержание работ по сопровождению ПО при изменении состава и настроек программного обеспечения и технических средств СЗИ, а также при изменении требований безопасности информации.

7. Устранение неисправностей технических средств и программного обеспечения

7.1 Специалист по информационным технологиям и защите информации обеспечивает анализ, устранение и ведет учет неисправностей технических средств и программного обеспечения СЗИ, принимает соответствующие действия по их предупреждению.

7.2 После выявления неисправности, отказа СЗИ специалистом по информационным технологиям и защите информации или специалистами, поставщиками технических средств (при гарантийном обслуживании) должны выполнятся необходимые работы по восстановлению работоспособности: ремонт (настройка, юстировка, пайка и т.п.), замена составных частей, автономные и комплексные проверки.

8. Контроль состояния и эффективности системы защиты информации

8.1 Контроль состояния и эффективности защиты информации ИС в процессе ее эксплуатации осуществляется специалистом по информационным технологиям и защите информации, государственными и ведомственными органами контроля и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер, проверке выполнения норм эффективности защиты информации.

Приложение - 4

Утверждено:
Распоряжением администрации
м.р.Кинельский от 20.07.19 № 553

Правила работы со средствами криптографической защиты информации

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ).

Функции органа криптографической защиты информации для проведения мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа, возложены на отдел информационных технологий администрации муниципального района Кинельский.

Инструкция в своем составе, терминах и определениях основывается на положениях «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152) и «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (алее - Положение ПКЗ-2005), утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.

2. Термины и определения

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Орган криптографической защиты (ОКЗ) – организация (структура), разрабатывающая и осуществляющая мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов,

предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Работа с СКЗИ

Обладатели конфиденциальной информации, если они приняли решение о необходимости криптографической защиты такой информации или если решение о необходимости ее криптографической защиты принято государственными органами или государственными организациями, обязаны выполнять указания соответствующих органов криптографической защиты по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат учету.

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего ознакомления с правилам работы со СКЗИ. Ознакомление пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Пользователи СКЗИ обязаны:

1. не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;
2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
3. сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
4. сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
5. немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от

помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

1. обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
2. собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
3. ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

Приложение - 5

Утверждено:
Распоряжением администрации
м.р.Кинельский от 29.07.19 № 553

Порядок резервирования баз данных и хранения резервных копий

1.Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Порядок), связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данного Порядка является:
- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации;
- определение мер хранения информации.

Действие настоящего Порядока распространяется на всех пользователей оператора, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается пользователь ИСПДн (сотрудник, осуществляющий обработку персональных данных).

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается специалист по информационным технологиям и технической защите информации.

2. Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:
- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудник (сотрудник, осуществляющий

обработку персональных данных) своими силами, либо совместно со специалистом по информационным технологиям и технической защите информации, предпринимают меры по восстановлению работоспособности ИСПДн. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3.Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1 Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

а) Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

б) Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

в) Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- для баз данных – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения. Носители должны храниться не менее года, для возможности восстановления данных.