Приложение 5

к Положению информационной

безопасности об организации

и обеспечении безопасности

персональных данных в администрации

Нефтекумского муниципального округа

Ставропольского края

ИНСТРУКЦИЯ

пользователя по обеспечению безопасности обработки персональных данных,

при возникновении нештатных ситуаций в администрации Нефтекумского муниципального округа Ставропольского края

Список сокращений

|  |  |  |
| --- | --- | --- |
| АВС | - | Антивирусные средства |
| АИС | - | Автоматизированная информационная система |
| АРМ | - | Автоматизированное рабочее место |
| ИСПДн | - | Информационная система персональных данных |
| КЗ | - | Контролируемая зона |
| ЛВС | - | Локальная вычислительная сеть |
| НСД | - | Несанкционированный доступ |
| ОС | - | Операционная система |
| ОИ | - | Объект информатизации |
| ПДн | - | Персональные данные |
| ПМВ | - | Программно-математическое воздействие |
| ПО | - | Программное обеспечение |
| СЗИ | - | Средства защиты информации |
| СЗПДн | - | Система (подсистема) защиты персональных данных |
| ТС | - | Технические средства |
| УБПДн | - | Угрозы безопасности персональных данных |

1. Общие положения

1.1. Настоящая инструкция предназначена для определения порядка действий при возникновении нештатных ситуаций в ИСПДн администрации Нефтекумского муниципального округа Ставропольского края (далее по тексту - Администрация).

В случае наличия нештатной ситуации порядок действий, при которой не регламентируется настоящей Инструкцией, ответственный за обеспечение безопасности персональных данных в Администрации составляет конкретный план действий с учетом текущей ситуации.

Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные тренировки по различным нештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

1.2. Должностные лица Администрации знакомятся с основными положениями и приложениями Инструкции в части их касающейся и по мере необходимости.

Ознакомление с требованиями настоящей Инструкции осуществляет ответственный за обеспечение безопасности персональных данных в Администрации под роспись копий соответствующих разделов Инструкции непосредственно для повседневного использования в работе.

Ознакомление с требованиями Инструкции администраторов ИСПДн Администрации осуществляет администратор информационной безопасности под роспись с выдачей копий соответствующих разделов Инструкции непосредственно для повседневного использования в работе.

1.3. Нештатными (кризисными) ситуациям являются:

1) разглашение информации ПДн, представленных в Перечне ПДн Администрации, работниками Администрации, имеющими к ней право доступа, в том числе:

разглашение информации лицам, не имеющим права доступа к защищаемой информации;

передача информации по открытым линиям связи;

обработка информации на незащищенных технических средствах обработки информации;

опубликование информации в открытой печати и других средствах массовой информации;

передача носителя информации лицу, не имеющему права доступа к ней;

утрата носителя с информацией.

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

несанкционированное изменение информации;

несанкционированное копирование информации.

3) несанкционированный доступ к защищаемой информации:

подключение технических средств к средствам и системам объекта информатизации;

использование закладочных устройств;

маскировка под зарегистрированного пользователя;

использование дефектов программного обеспечения объекта информатизации (ОИ);

использование программных закладок;

применение программных вирусов;

хищение носителя защищаемой информации;

нарушение функционирования технических средств (ТС) обработки информации;

блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

2. Порядок действий при обнаружении нештатных ситуаций

2.1. Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными ниже:

|  |  |
| --- | --- |
| Нештатная ситуация | Оценка ситуации (раздел Инструкции) |
| Разглашение защищаемой информации работниками, имеющими к ней право доступа | (0) |
| Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации | Несанкционированное копирование конфиденциальной информации | Обнаружился случившийся факт (0) |
| Производится в текущий момент (3.2) |
| Несанкционированное изменение конфиденциальной информации | Обнаружился случившийся факт (0) |
| Производится в текущий момент (3.2) |
| Несанкционированный доступ к защищаемой информации  | Подключение технических средств к средствам и системам объекта информатизации (ОИ) | Обнаружился случившийся факт (0) |
| Производится в текущий момент (3.3) |
| Установка закладочных устройств | Обнаружение установленных (0) |
| Устанавливаются в настоящий момент (3.4) |
| Маскировка под зарегистрированного пользователя | Внешним злоумышленником в текущий момент (3.5) |
| Внутренним злоумышленником, либо производилась в прошлом (0) |
| Использование дефектов программного обеспечения ОИ | Внешним злоумышленником в текущий момент (3.6) |
| Внутренним злоумышленником, либо производилось в прошлом (0) |
| Использование программных закладок | Внешним злоумышленником в текущий момент (3.7) |
| Внутренним злоумышленником, либо производилось в прошлом (0) |
| Обнаружение программных вирусов | (3.8) |
| Хищение носителя защищаемой информации | (0) |
| Нарушение функционирования ТС обработки информации злоумышленником | Производится в текущий момент (3.9) |
| Обнаружился случившийся факт (3.10) |
| Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку | Производится в текущий момент внешним злоумышленником (3.11) |
| Производится в текущий момент внутренним злоумышленником (3.12) |
| Обнаружился случившийся факт (3.13) |
| Ошибки пользователей системы при эксплуатации программных средств, ТС, средств и систем защиты информации | Ошибка повлекла утерю или повреждение защищаемой информации (3.14) |
| Ошибка привела к нарушению работоспособности ТС и ПО (3.15) |
| Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ | (3.16) |
| Сбои, отказы и аварии систем обеспечения ОИ | (3.17) |
| Природные явления, стихийные бедствия | Несущие угрозу жизни человека | (3.18) |
| Не несущие угрозу жизни человека | (3.19) |

2.2. Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником.

При обнаружении нештатных ситуаций создается комиссия.

2.3. При нештатных ситуациях, связанных с:

разглашением конфиденциальной информации;

обнаружением несанкционированно скопированной или измененной конфиденциальной информации;

обнаружением подключения технических средств к средствам и системам объекта информатизации;

обнаружением закладочных устройств;

маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);

использованием дефектов программного обеспечения ОИ внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

хищением носителя защищаемой информации.

2.4. В первую очередь администратором ИБ предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника. Комиссия, дополнительно к общему порядку действий должна:

определить организации, в которые произошла утечка конфиденциальной информации;

определить возможные контрмеры, призванные уменьшить потери от утечки информации.

2.5. Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней

2.6. В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию выполняются следующие действия:

1) Первоочередные действия Администратора ИБ:

прерывает несанкционированный процесс;

блокирует доступ к ИСПДн для злоумышленника;

производит удаление нарушителя от средств ИСПДн.

2) Ответственный за обеспечение безопасности персональных данных совместно с администратором ИБ предпринимают действия по сбору и обеспечению сохранности улик.

Последующие действия. Создается комиссия для расследования инцидента.

2.7. В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ОИ в текущий момент времени выполняются следующие действия:

Первоочередные действия:

администратор ИБ прерывает процесс работы нарушителя.

в случае если нарушитель - пользователь ИСПДн администратор ИБ блокирует доступ в ИСПДн для нарушителя;

Последующие действия. Создается комиссия для расследования инцидента.

2.8. В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия:

Первоочередные действия:

ответственный за обеспечение безопасности персональных данных принимает меры к задержанию злоумышленника.

Последующие действия. Создается комиссия для расследования инцидента.

2.9. В случае обнаружения внешнего злоумышленника, маскирующегося под зарегистрированного пользователя, выполняются следующие действия:

Первоочередные действия:

администратор ИБ блокирует доступ к ИСПДн для злоумышленника.

Последующие действия. Создается комиссия для расследования инцидента.

2.10. В случае обнаружения использования дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени выполняются следующие действия:

Первоочередные действия:

администратор ИБ блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.

Последующие действия. Создается комиссия для расследования инцидента.

2.11. В случае обнаружения использования программных закладок внешним нарушителем в текущий момент времени выполняются следующие действия:

1) Первоочередные действия:

администратор ИБ блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

2) Последующие действия:

администратор ИБ определяет возможный ущерб, нанесенный программной закладкой, докладывает об этом Ответственному за обеспечение безопасности персональных данных в Администрации;

администратор ИБ проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

Составляет акт об инциденте.

2.12. В случае обнаружения программных вирусов выполняются действия, предусмотренные Инструкцией по антивирусной защите.

2.13. В случае обнаружения злоумышленника, нарушающего функционирование ТС обработки информации в текущий момент времени выполняются следующие действия:

1) Первоочередные действия:

принимаются меры по немедленному удалению злоумышленника от средств вычислительной техники;

в случае если злоумышленник является пользователем системы, Администратор ИБ блокирует доступ к ИСПДн для злоумышленника.

2) Последующие действия:

в случае наличия повреждений администратор ИСПДн определяет ущерб, нанесенный ТС;

администратор ИБ и администратор АС определяет ущерб, нанесенный информации;

администратор ИБ и/или администратор ИСПДн производят восстановление работоспособности системы.

Создается комиссия для расследования инцидента.

2.14. В случае обнаружения нарушений в функционировании ТС обработки информации, выполняются следующие действия:

Первоочередные действия:

администратор ИБ определяет возможный круг лиц, причастных к нарушению функционирования ТС;

администратор ИБ и администратор ИСПДн определяют объем повреждений (как техническим, так и информационным ресурсам);

администратор ИСПДн производит восстановление работоспособности системы.

Создается комиссия для расследования инцидента.

2.15. В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

1) Первоочередные действия Администратора ИБ:

совместно с администратором ИСПДн выявляет источник ложных заявок.

совместно с администратором ИСПДн вырабатывают решение по блокированию потока ложных заявок и реализует выбранное решение.

2) Последующие действия:

администратор ИБ уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента;

администратор ИБ составляет акт об инциденте.

2.16. В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

администратор ИБ совместно с Администратором сетевой защиты выявляет источник ложных заявок и блокирует доступ к ИСПДн для злоумышленника.

Создается комиссия для расследования инцидента.

2.17. При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия:

Администратор ИБ совместно с администратором сетевой защиты выявляет источник ложных заявок.

В случае если злоумышленник является внешним, ИБ уведомляет провайдера, от которого идут ложные заявки. Планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

В случае если злоумышленник является внешним, администратор ИБ составляет акт об инциденте.

Создается комиссия для расследования инцидента.

2.18. В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации, выполняются следующие действия:

1) Первоочередные действия:

администратор ИБ совместно с администратором ИСПДн проводят анализ и идентификацию причин инцидента.

в случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции;

администратор ИБ и администратор ИСПДн определяют ущерб, нанесенный нештатной ситуацией;

администратор ИСПДн проводит мероприятия по восстановлению работоспособности системы и информации.

2) Последующие действия:

проводится проверка знаний работника виновного в инциденте, а в случае необходимости его обучение;

администратор ИБ и администратор ИСПДн составляют акт об инциденте, в случае необходимости выносят предложение руководству о применении дисциплинарной меры в отношении нарушителя.

2.19. В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО

1) Первоочередные действия:

администратор ИБ совместно с администратором ИСПДн проводят анализ и идентификацию причин инцидента;

в случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

2) Последующие действия:

администратор ИБ совместно с администратором ИСПДн;

определяют ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы;

составляет акт об инциденте, в случае необходимости выносят предложение руководителю о применении дисциплинарной меры в отношении нарушителя.

Проводится проверка знаний работника виновного в инциденте, а в случае необходимости его обучение.

2.20. В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ОИ выполняются следующие действия:

1) Первоочередные действия:

администратор ИБ и администратор ИСПДн выявляют возможные причины проявления дестабилизирующих факторов;

в случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции.

2) Последующие действия:

администратор ИСПДн восстанавливает работоспособность систем;

в случае потери данных администратором ИСПДн по возможности проводится восстановление их из резервных копий.

Администратором ИСПДн производится составление акта.

2.21. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий:

1) если наблюдается продолжительное отключение электропитания, администратором ИСПДн производится отключение серверов до момента истечения резервов системы бесперебойного питания.

Ответственный за материально-техническое обеспечение организует работы по максимально быстрому восстановлению систем обеспечения.

2) в случае потери защищаемых данных администратором ИСПДн по возможности проводится восстановление их из резервных копий.

Ответственный за материально-техническое обеспечение производит составление акта.

2.22. В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:

1) Все работники (руководители подразделений в том числе) обязаны личные реквизиты защиты (например, металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.) собрать и упаковать в водонепроницаемый пакет (непосредственный руководитель обеспечивает заранее) и лично обеспечивать сохранность этого пакета во время эвакуации.

2) По "Списку имущества и (или) документов в личном пользовании работника, подлежащего эвакуации в первую очередь" (разрабатываются работниками заранее и постоянно хранятся на рабочем месте) произвести сбор, упаковку, опись (в двух экз. - 1 экз. в тару) документов и технических средств в водонепроницаемую тару (обеспечивает заранее непосредственный руководитель). Упакованное имущество работник передает под роспись (на своем экз. описи) лицам, обеспечивающим доставку имущества на эвакопункт, иначе - лично сопровождает груз во время его транспортировки.

3) Работник вкладывает в вышеназванный пакет картонную табличку с указанием текущей даты, своих персональных данных (Ф.И.О., наименование организации, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.

4) Руководители обязаны собрать в помещениях подразделения и лично упаковать, (и далее лично хранить, как свои) реквизиты защиты и документы (согласно спискам первой очереди) тех работников, которых на момент эвакуации нет на рабочем месте (болезнь, командировка, учеба, отпуск и т.д.).

5) Руководители обязаны:

при подготовке к эвакуации проверить обеспеченность (а при отсутствии - обеспечить) работников подразделения и/или администраторов упаковочным материалом, списками документов, дел и имущества, подлежащих эвакуации в первую очередь;

перед выездом в эвакопункт - проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от работников о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества подразделения и/или АС к эвакуации.

2.23. В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:

работники выключают свои персональные компьютеры;

администратор ИСПДн выключает серверы и сетевое оборудование;

администратор ИБ принимает меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества. В первую очередь эвакуируется имущество по "Списку имущества и (или) документов в личном пользовании работника, подлежащего эвакуации в первую очередь".

2.24. В случае локальных пожаров и частичных затоплений Ответственный за материально-техническое обеспечение организует работы по ликвидации нештатной ситуации и ее последствий.

3. Производство расследований

3.1. Для расследования опасных ситуаций в случаях предусмотренных настоящей Инструкцией может создаваться комиссия. В состав комиссии должны входить:

председатель;

администратор ИБ;

администратор ИСПДн;

юрист;

другие лица по решению председателя комиссии.

3.2. Деятельность комиссии должна по возможности происходить в режиме строгой конфиденциальности.

В общем случае комиссия проводит:

анализ и идентификацию причин инцидента, определение виновных;

определение ущерба, нанесенного нештатной ситуацией;

планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);

анализ и сохранение доказательств, следов инцидента, улик и свидетельств;

определение меры взыскания с виновного;

взаимодействие, при необходимости с правоохранительными органами.

3.3. При сохранении улик:

если есть возможность, Администратором ИСПДн производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая логи (контрольные записи);

ответственным за обеспечение безопасности персональных данных в Администрации совместно с администратором ИБ производится сохранение цепи событий по сбору улик.

3.4. По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

3.5. По результатам расследования администраторами организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления, подобных инцидентов в дальнейшем.

3.6. При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

можно ли было предусмотреть нештатную ситуацию;

вызвана ли она слабостью средств защиты и регистрации;

это первая кризисная ситуация такого рода;

достаточно ли имеющегося резерва;

есть ли необходимость пересмотра системы защиты;

есть ли необходимость пересмотра настоящей инструкции.

4. Ответственные за контроль выполнения инструкции

4.1. Ответственным за постоянный контроль выполнения требований данной Инструкции является:

ответственный за обеспечение безопасности персональных данных в Администрации в части задач возложенных в настоящей инструкции на это должностное лицо;

администратор ИБ в части задач, возложенных в настоящей инструкции на это должностное лицо;

ответственный за материально-техническое обеспечение, в части задач, возложенных в настоящей инструкции на него.

5. Порядок пересмотра инструкции

5.1. Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИСПДн Администрации, кроме того, полный плановый пересмотр данного документа проводится регулярно, не реже одного раза в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Администрации.

5.2. Инструкция подлежит частичному пересмотру в следующих случаях:

при изменении местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;

при определении такой необходимости комиссией по результатам расследования нештатной ситуации;

в целях повышения эффективности мероприятий, определенных в настоящей инструкции;

при изменении состава, обязанностей и полномочий должностных лиц, которые задействованы в мероприятиях настоящей Инструкции.

5.3. Полный пересмотр данного документа проводится Ответственным за обеспечение безопасности персональных данных в Администрации с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Администрации.

5.4. Частичный пересмотр данного документа проводится администратором ИБ. Частичный пересмотр должен проводиться регулярно, не реже одного раза в полгода. При частичном пересмотре инструкции в обязательном порядке вносятся изменения без переутверждения всей Инструкции.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_