УТВЕРЖДАЮ
Директор МУ Сивинский ЦКД

_____ Е.Л.Новоселова
«02» 02 2021 г.

Инструкция
по действиям пользователей информационной системы персональных данных в нештатных ситуациях в МУ Сивинский ЦКД

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция предназначена для определения порядка действий пользователей информационной системы персональных данных (ИСПДн) МУ Сивинский ЦКД (далее – Учреждение) при возникновении нештатных ситуаций.

Нештатными ситуациям являются:

1) разглашение информации ограниченного доступа, не составляющей государственную тайну (далее защищаемая информация), сотрудниками Учреждения, 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;

4) дефекты, сбои, отказы, аварии ТС и систем ОИ;

5) дефекты, сбои и отказы программного обеспечения ОИ;

6) сбои, отказы и аварии систем обеспечения ОИ;

7) природные явления, стихийные бедствия:
- термические, климатические факторы (пожары, наводнения и т.д.);
- механические факторы (землетрясения и т.д.);
- электромагнитные факторы (грозовые разряды и т.д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей инструкцией администратором информационной безопасности (ИБ) ИСПДн, ответственным за обеспечение безопасности персональных данных (ПДн) Учреждения вырабатывается конкретный план действий с учетом текущей ситуации.

Резервируемые в Учреждении информационные ресурсы и способы их резервирования представлены в Приложении 1 к настоящей Инструкции.

Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении 2 к настоящей Инструкции.
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. Работники Учреждения знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости. Ознакомление с требованиями Инструкции сотрудников Учреждения осуществляет администратор ИБ ИСПДн под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

2 ПОРЯДОК ДЕЙСТВИЙ ПРИ ОБНАРУЖЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

2.1.Классификация нештатных ситуаций
Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице 3.1.
2.2.Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником.
При обнаружении нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником, создается комиссия.
В первую очередь администратором ИБ ИСПДн предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника 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.
Комиссия, дополнительно к общему порядку действий (в соответствии с разделом 3), должна:
- если это возможно, определить организации, в которые произошла утечка конфиденциальной информации;
- определить возможные контрмеры, призванные уменьшить потери от утечки информации.
2.3.Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней.
В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию выполняются следующие действия
1 Администратор ИБ ИСПДн прерывает несанкционированный процесс.
2 Администратор ИБ ИСПДн блокирует доступ к ИСПДн Учреждения для злоумышленника.
3 Администратор ИБ ИСПДн совместно с ответственным за обеспечение безопасности ПДн Учреждения удаляют нарушителя от средств ИСПДн.
4 Ответственным за обеспечение безопасности ПДн совместно с администратором ИБ ИСПДн предпринимаются действия по сбору и обеспечению сохранности улик.
2.3.2. Последующие действия
Создается комиссия для расследования инцидента.
2.4.Подключение технических средств к средствам и системам ОИ в текущий момент времени

В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ОИ в текущий момент времени, выполняются следующие действия.
2.4.1. Первоочередные действия
1 Администратор ИБ ИСПДн прерывает процесс работы нарушителя.
2 В случае если нарушитель – пользователь ИСПДн, администратор ИБ ИСПДн блокирует доступ в ИСПДн Учреждения для нарушителя.
2.4.2. Последующие действия
Создается комиссия для расследования инцидента.
2.5.Установка закладочных устройств злоумышленником в текущий момент времени
В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия.
2.5.1. Первоочередные действия
Администратор ИБ ИСПДн принимает меры к задержанию злоумышленника.
2.5.2. Последующие действия
Создается комиссия для расследования инцидента.
2.6. Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени
В случае обнаружения внешнего злоумышленника маскирующегося под зарегистрированного пользователя выполняются следующие действия.
2.6.1. Первоочередные действия
Администратор ИБ ИСПДн блокирует доступ к ИСПДн Комитета для злоумышленника.
2.6.2. Последующие действия
Создается комиссия для расследования инцидента.
2.7. Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени
В случае обнаружения использования дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени выполняются следующие действия.
2.7.1. Первоочередные действия
Администратор ИБ ИСПДн блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.
2.7.2. Последующие действия
Создается комиссия для расследования инцидента.
2.8.Использование программных закладок внешним нарушителем в текущий момент времени
В случае обнаружения использования программных закладок внешним нарушителем в текущий момент времени выполняются следующие действия.
2.8.1. Первоочередные действия
Администратор ИБ ИСПДн блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка.
2.8.2. Последующие действия
1 Администратор ИБ ИСПДн определяет возможный ущерб, нанесенный программной закладкой.
2 Администратор ИБ ИСПДн проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
3 Составляется акт об инциденте.
2.9 Обнаружение программных вирусов
В случае обнаружения программных вирусов выполняются действия предусмотренные Инструкцией по антивирусной защите.
2.10. Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником
В случае обнаружения злоумышленника нарушающего функционирование ТС обработки информации в текущий момент времени выполняются следующие действия.
2.10.1. Первоочередные действия
1 Администратор ИБ ИСПДн принимает меры по немедленному удалению злоумышленника от средств вычислительной техники.

2 В случае если злоумышленник является пользователем системы,
Администратор ИБ ИСПДн блокирует доступ к ИСПДн Комитета для злоумышленника.
2.10.2. Последующие действия
1 В случае наличия повреждений Администратор ИБ ИСПДн определяет ущерб, нанесенный ТС и информации.
2 Администратор ИБ ИСПДн производит восстановление работоспособности системы.
3 Создается комиссия для расследования инцидента.
2.11. Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником
В случае обнаружения нарушений в функционировании ТС обработки информации, выполняются следующие действия.
1 Администратор ИБ ИСПДн определяет возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.
2 Администратор ИБ ИСПДн производит восстановление работоспособности системы.
3 Создается комиссия для расследования инцидента.
2.12. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени
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.
2.12.1. Первоочередные действия
1 Администратор ИБ ИСПДн выявляет источник ложных заявок.
2 Администратор ИБ ИСПДн вырабатывает решение по блокированию потока ложных заявок и реализует выбранное решение
2.12.2. Последующие действия
1 Администратор ИБ ИСПДн уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
2 Администратор ИБ ИСПДн составляет акт об инциденте.
2.13. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени
В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на еообработку в текущий момент времени, выполняются следующие действия:
1 Администратор ИБ ИСПДн выявляет источник ложных заявок и блокирует доступ к ИСПДн Комитета для злоумышленника.
2 Создается комиссия для расследования инцидента.
2.14. Блокировка доступа к защищаемой информации, произошедшая в прошлом
При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия.
1 Администратор ИБ ИСПДн выявляет источник ложных заявок.
2 В случае если злоумышленник является внешним, администратор ИБ ИСПДн уведомляет провайдера, от которого идут ложные заявки. Планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
3 В случае если злоумышленник является внешним, администратор ИБ ИСПДн составляет акт об инциденте.
4 Создается комиссия для расследования инцидента.
2.15. Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации

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.
2.15.1. Первоочередные действия
1 Администратор ИБ ИСПДн проводит анализ и идентификацию причин инцидента.
2 В случае возможности злоумышленных действий выполняется последовательностьдействий, предусмотренная в соответствующем разделе Инструкции.
3 Администратор ИБ ИСПДн определяет ущерб, нанесенный нештатной ситуацией.
4 Администратор ИБ ИСПДн проводит мероприятия по восстановлению работоспособности системы и информации.
2.15.2. Последующие действия
1 Проводится проверка знаний сотрудника, виновного в инциденте, а в случае необходимости его обучение.
2 Администратор ИБ ИСПДн составляет акт об инциденте, в случае необходимости выносит предложение руководителю Учреждения о применении дисциплинарной меры в отношении нарушителя.
2.16. Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО
В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО, выполняются следующие действия.
2.16.1. Первоочередные действия
1 Администратор ИБ ИСПДн проводит анализ и идентификацию причин инцидента.
2 В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.
2.16.2. Последующие действия
1 Администратор ИБ ИСПДн определяет ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы.
2 Администратор ИБ ИСПДн составляет акт об инциденте, в случае необходимости выносит предложение руководителю Учреждения о применении дисциплинарной меры в отношении нарушителя.
3 Проводится проверка знаний сотрудника виновного в инциденте, ав случае необходимости его обучение.
2.17. Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ
В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ОИ выполняются следующие действия.
2.17.1. Первоочередные действия
1 Администратор ИБ ИСПДн выявляют возможные причины проявления дестабилизирующих факторов.
2 В случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции.
2.17.2. Последующие действия
1 Администратор ИБ ИСПДн восстанавливает работоспособность систем.
2 В случае потери данных администратором ИБ ИСПДн по возможности проводится восстановление их из резервных копий.
3 Администратором ИБ ИСПДн производится составление акта.
2.18. Сбои, отказы и аварии систем обеспечения ОИ
В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий.
1 В случае если наблюдается продолжительное отключение электропитания.
Администратором ИБ ИСПДн производится отключение серверов до момента истечения резервов системы бесперебойного питания.
2 Ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения.

3 В случае потери защищаемых данных Администратором ИБ ИСПДн по возможности проводится восстановление их из резервных копий
4 Ответственным за материально-техническое обеспечение производится составление акта.
2.19. Природные явления, стихийные бедствия, несущие угрозу жизни человека
В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:
1 Все сотрудники 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 сотрудника, подлежащего эвакуации в первую очередь» (разрабатываются сотрудниками заранее и постоянно хранятся на рабочем месте) произвести сбор, упаковку, опись (в двух экз. – 1 экз. в тару) документов и технических средств в водонепронецаемую тару (обеспечивает заранее непосредственный руководитель). Упакованное имущество сотрудник передает под роспись (на своем экз. описи) лицам, обеспечивающим доставку имущества на эвакопункт, иначе - лично сопровождает груз во время его транспортировки.
3 Сотрудник вкладывает в вышеназванный пакет картонную табличку с указанием текущей даты, своих персональных данных (ФИО, наименование организации, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.
Руководители обязаны собрать в помещениях отделов и лично упаковать, (и далее лично хранить, как свои) реквизиты защиты и документы (согласно спискам первой очереди) тех сотрудников, которых на момент эвакуации нет на рабочем месте (болезнь, командировка, учеба, отпуск и т.д.).
Руководители обязаны:
- при подготовке к эвакуации проверить обеспеченность (а при отсутствии–обеспечить) сотрудников упаковочным материалом, списками документов, дел и имущества, подлежащих эвакуации в первую очередь;
- перед выездом в эвакопункт – проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от сотрудников о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества ИСПДн к эвакуации.
2.20. Природные явления, стихийные бедствия, не несущие угрозу жизни человека
В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:
1 Сотрудники Учреждения выключают свои персональные компьютеры.
2 Администратор ИБ ИСПДн выключает сетевое оборудование.
3 Администратор ИБ ИСПДн 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 сотрудника, подлежащего эвакуации в первую очередь».
4 В случае локальных пожаров и частичных затоплений
Ответственным за материально-техническое обеспечение организуются работы по ликвидации нештатной ситуации и ее последствий.
3 ПРОВЕДЕНИЕ РАССЛЕДОВАНИЙ
Для расследования опасных ситуаций в случаях, предусмотренных настоящей Инструкцией может создаваться комиссия. В состав комиссии должны входить:
- председатель,
- ответственный за обеспечение безопасности ПДн;
- администратор ИБ ИСПДн;
- другие лица по решению председателя комиссии.
Деятельность комиссии должна по возможности происходить в режиме 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.

При сохранении улик, если есть возможность, Администратором ИБ ИСПДн производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая логин

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

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

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:
- можно ли было предупредить 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

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:
- администратор ИБ ИСПДн в части задач, возложенных на него настоящей инструкцией;
- ответственный за обеспечение безопасности ПДн в части общего контроля информационной безопасности;
- ответственный за материально-техническое обеспечение, в части задач, возложенных на него настоящей инструкцией.

5 ПОРЯДОК ЗАМЕЩЕНИЯ ОТВЕТСТВЕННЫХ ЛИЦ

В случае отсутствия кого-либо из ответственных лиц при нештатной ситуации (отпуск, болезнь и т.п.) производится их замещение в соответствии с последовательностями определенными ниже. Ответственное лицо замещает следующий идущий по списку сотрудник.

Ответственные за информационную безопасность и ИСПДн
1 Администратор ИБ ИСПДн.
2 Ответственный за обеспечение безопасности ПДн.

Ответственные за материально-техническое обеспечение
1 Руководитель .
2 Заведующий хозяйственным отделом.

6 ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИСПДн Учреждения, 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 Учреждении.

И- 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 Учреждения , которые задействованы в мероприятиях настоящей Инструкции.

Полный пересмотр данного документа проводится администратором ИБ ИСПДн, ответственным за обеспечение безопасности ПДн Учреждения с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Учреждения.

Частичный пересмотр данного документа проводится администратором ИБ ИСПДн.

Частичный пересмотр должен проводиться регулярно, не реже одного раза в год. При этом могут быть добавлены, удалены или изменены приложения Инструкции с обязательным указанием оснований и внесенных изменений в «Листе регистрации изменений в Инструкции» (Приложение 4) без переутверждения всей Инструкции