Министерство образования Московской области
Государственное бюджетное профессиональное образовательное учреждение
Московской области «Воскресенский колледж»

УТВЕРЖДАЮ
Директор ГБПОУ МО "Воскресенский колледж"
А.Ю.Лунина

Подписано цифровой подписью:
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
"ВОСКРЕСЕНСКИЙ КОЛЛЕДЖ"
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760,
ОГРН=1047797019830, STREET="Большой Златоустинский переулок,
д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России,
CN=Казначейство России
Дата: 3 Май 2024 г. 16:53:13

ИНСТРУКЦИЯ

пользователям информационных систем персональных данных по действиям в нештатных ситуациях

г. Воскресенск
2024

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция предназначена для определения порядка действий пользователей информационной системы персональных данных (ИСПДн) ГБПОУ МО «Воскресенский колледж» (далее – колледж) при возникновении нештатных ситуаций.

Нештатными ситуациям являются:

1) разглашение информации ограниченного доступа, не составляющей государственную тайну (далее защищаемая информация), сотрудниками колледжа, имеющими к ней право доступа, в том числе:

- разглашение защищаемой информации лицам, не имеющим права доступа к защищаемой информации;
- передача защищаемой информации по открытым линиям связи;
- обработка защищаемой информации на незащищенных технических средствах обработки информации;
- опубликование защищаемой информации в открытой печати и других средствах массовой информации;
- передача носителя с защищаемой информации лицу, не имеющему права доступа к ней;
- утрата носителя с защищаемой информацией.

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

- несанкционированное изменение защищаемой информации;
- несанкционированное копирование защищаемой 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 ИСПДн
- использование программных закладок;
- применение программных вирусов;
- хищение носителя защищаемой информации;
- нарушение функционирования технических средств обработки защищаемой 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 ИСПДН;

5) дефекты, сбои и отказы программного обеспечения ИСПДН;

6) сбои, отказы и аварии систем обеспечения ИСПДН;

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, лицами, ответственным за обеспечение безопасности персональных данных колледжа, вырабатывается конкретный план действий с учетом сложившийся ситуации.

Резервируемые в колледже 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.

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

Ознакомление с требованиями Инструкции сотрудников колледжа осуществляет инженер-программист, или специалисты группы информационных систем колледжа, под роспись, с выдачей электронных копий 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.

Таблица 3.1. Оценки нештатных ситуаций

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		(2.2)
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование конфиденциальной информации	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.3)
	Несанкционированное изменение конфиденциальной информации	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.3)
Несанкционированный доступ к информации	Подключение технических средств к техническим средствам ИСПДн	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.4)
	Установка закладочных устройств	Обнаружение установленных (2.2)
		Устанавливаются в настоящий момент (2.5)
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент (2.6)
		Внутренним злоумышленником, либо производилась в прошлом (2.2)
	Использование дефектов программного обеспечения ИСПДн	Внешним злоумышленником в текущий момент (2.7)
		Внутренним злоумышленником, либо производилось в прошлом (2.2)
	Использование программных закладок	Внешним злоумышленником в текущий момент (2.8)

Нештатная ситуация		Оценка ситуации (раздел Инструкции)
		Внутренним злоумышленником, либо производилось в прошлом (2.2)
	Обнаружение программных вирусов	(2.9)
	Хищение носителя защищаемой информации	(2.2)
	Нарушение функционирования ТС обработки информации злоумышленником	Производится в текущий момент (2.10)
		Обнаружился случившийся факт (2.11)
	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником (2.12)
		Производится в текущий момент внутренним злоумышленником (2.13)
		Обнаружился случившийся факт (2.14)
Ошибки пользователей системы при эксплуатации программных и технических средств, средств и систем защиты информации		Ошибка повлекла утерю или повреждение защищаемой информации (2.15)
		Ошибка привела к нарушению работоспособности ТС и ПО (2.16)
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ИСПДн		(2.17)
Сбои, отказы и аварии систем обеспечения ИСПДн		(2.18)
Природные явления, стихийные бедствия	Несущие угрозу жизни человека	(2.19)
	Не несущие угрозу жизни человека	(2.20)

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 инженером-программистом, и специалистами отдела информационных систем колледжа 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 ИСПДн 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 подразделения, 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.

2.3.1. Первоочередные действия:

1. Заместитель директора по безопасности и ответственный за защиту информации прерывают несанкционированный процесс.
2. Заместитель директора по безопасности и ответственный за защиту информации блокируют доступ к ИСПДн для злоумышленника.
3. Заместитель директора по безопасности и ответственный за защиту информации колледжа удаляют нарушителя от средств ИСПДн.
4. Взаместителем директора по безопасности и ответственным за защиту информации предпринимаются действия по сбору и обеспечению сохранности улик.

2.3.2. Последующие действия:

создается комиссия для расследования инцидента.

2.4. Подключение технических средств к системам и средствам ИСПДн в текущий момент времени

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

2.4.1. Первоочередные действия:

- заместитель директора по безопасности и ответственный за защиту информации прерывают процесс работы нарушителя.
- в случае если нарушитель – пользователь ИСПДн, заместитель директора по безопасности и ответственный за защиту информации блокируют доступ в ИСПДн предприятия 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:

- заместитель директора по безопасности 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:

- заместитель директора по безопасности блокирует доступ к ИСПДн для злоумышленника.

2.6.2. Последующие действия:

- создается комиссия для расследования инцидента.

2.7. Использование дефектов программного обеспечения ИСПДН внешним нарушителем в текущий момент времени

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

2.7.1. Первоочередные действия:

- ответственный за защиту информации блокируют 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:

- ответственный за защиту информации блокируют доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

2.8.2. Последующие действия:

- ответственный за защиту информации определяют возможный ущерб, нанесенный программной закладкой.
- ответственный за защиту информации проводят мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
- 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:

- ответственный за функционирование ТС и ответственный за защиту информации принимают меры по немедленному удалению злоумышленника от средств вычислительной техники.
- в случае если злоумышленник является пользователем системы, Ответственный за функционирование ТС и ответственный за защиту информации блокируют доступ к ИСПДн колледжа для злоумышленника.

2.10.2. Последующие действия:

- в случае наличия повреждений Ответственный за функционирование ТС и ответственный за защиту информации определяют ущерб, нанесенный ТС и информации.
- ответственный за функционирование ТС и ответственный за защиту информации производят восстановление работоспособности системы.
- 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. Оответственный за функционирование ТС и ответственный за защиту информации определяют возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.
2. Оответственный за функционирование ТС и ответственный за защиту информации производят восстановление работоспособности системы.
3. Ссоздается 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:

- ответственный за функционирование ТС и ответственный за защиту информации выявляют источник ложных заявок.
- ответственный за функционирование ТС и ответственный за защиту информации вырабатывают решение по блокированию потока ложных заявок и реализуют выбранное решение.

2.12.2. Последующие действия:

- ответственный за функционирование ТС и ответственный за защиту информации уведомляют провайдера, от которого идут ложные заявки, планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
- ответственный за функционирование ТС и ответственный за защиту информации составляют 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 ее обработку в текущий момент времени, выполняются следующие действия:

- ответственный за функционирование ТС и ответственный за защиту информации выявляют источник ложных заявок и блокирует доступ к ИСПДн для злоумышленника.
- 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:

- ответственный за функционирование ТС и ответственный за защиту информации выявляют источник ложных заявок.
- в случае если злоумышленник является внешним, Ответственный за функционирование ТС и ответственный за защиту информации уведомляют провайдера, от которого идут ложные заявки. Планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
- в случае если злоумышленник является внешним, ответственный за функционирование ТС и ответственный за защиту информации составляют акт об инциденте.
- 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:

- ответственный за функционирование ТС и ответственный за защиту информации проводят анализ и идентификацию причин инцидента.
- в случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.
- ответственный за функционирование ТС и ответственный за защиту информации определяют ущерб, наносимый нештатной ситуацией.
- ответственный за функционирование ТС и ответственный за защиту информации проводят мероприятия по восстановлению работоспособности системы и информации.

2.15.2. Последующие действия:

- проводится проверка знаний сотрудника, виновного в инциденте, а в случае необходимости его обучение.
- составляется акт об инциденте, в случае необходимости выносит предложение директору о применении дисциплинарных мер 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:

- ответственный за функционирование ТС и ответственный за защиту информации проводят анализ и идентификацию причин инцидента.
- в случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

2.16.2. Последующие действия:

- определяются ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы.
- составляется акт об инциденте, в случае необходимости выносит предложение директору о применении дисциплинарных мер в отношении нарушителя.
- проводится проверка знаний сотрудника виновного в инциденте, а в случае необходимости его обучение.

2.17. Дефекты, сбои, отказы, аварии ТС, программных средств и систем ИСПДн

В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ИСПДн выполняются следующие действия.

2.17.1. Первоочередные действия:

- ответственный за функционирование ТС и ответственный за защиту информации выявляют возможные причины проявления дестабилизирующих факторов.
- в случае наличия злоумышленных действий, выполняется порядок действий соответствующего раздела Инструкции.

2.17.2. Последующие действия:

- ответственный за функционирование ТС и ответственный за защиту информации восстанавливают работоспособность систем.
- в случае потери данных специалистами отдела информационных систем колледжа по возможности проводится восстановление их из резервных копий.
- производится составление акта.

2.18. Сбои, отказы и аварии систем обеспечения ИСПДн

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

- в случае если наблюдается продолжительное отключение электропитания ответственным за функционирование ТС и ответственным за защиту информации производится отключение серверов до момента истечения резервов системы бесперебойного питания.
- заместителем директора по АХЧ организуются работы по максимально быстрому восстановлению систем обеспечения.

- в случае потери защищаемых данных по возможности проводится восстановление их из резервных копий.
- заместителем директора по АХЧ 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 заранее разработанному и постоянно хранятся на рабочем месте «Списку имущества и документов, подлежащего эвакуации в первую очередь»(2 экз.), произвести сбор документов и технических средств в водонепроницаемую 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 колледжа, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.

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 колледжа выключают свои персональные компьютеры.
2. Ответственный за функционирование ТС выключают серверы и сетевое оборудование.
3. Ответственный за защиту информации 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, заместителем директора по АХЧ 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 защиты информации;
- заместитель директора по АХЧ;
- ответственный за функционирование ТС;
- другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме конфиденциальности.

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 мер воздействия на виновного;
- взаимодействие, при необходимости, с правоохранительными органами.

При сохранении улик, если есть возможность, инженером – программистом или специалистами отдела информационных систем производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая логи (контрольные записи).

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

По результатам расследования инженером-программистом 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:

- ответственные за функционирование ТС, в части задач, возложенных на них настоящей инструкцией;
- ответственный за защиту информации в части общего контроля информационной безопасности;
- заместитель директора по АХЧ, в части задач, возложенных на него настоящей инструкцией.

Заместитель директора ГБПОУ МО
«Воскресенский колледж» по безопасности М.И. Милашук

Приложение 1

СРЕДСТВА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

Резервному копированию (РК) подлежит следующая информация:

- системные программы и наборы данных - *невозобновляемому (однократному, эталонному) РК*;
- прикладное программное обеспечение и наборы данных - *невозобновляемому РК*;
- наборы данных, генерируемые в течение рабочего дня и содержащие ценную информацию (журналы транзакций, системный журнал и т.д.) - *периодическому возобновляемому РК.*

Резервному копированию в ИСПДн подлежат следующие программные и информационные ресурсы:

Наименование информационного ресурса	**Где размещается ресурс в системе**	**Вид резервного копирования**	**Ответственный за резервное копирование (используемые технические средства)**	**Где хранится резервная копия**	**Частота периодического резервирования**
Информация ИСПДн		Периодическое, возобновляемое	Ответственный за защиту информации, ведущий программист		Каждую пятницу
Эталонное программное обеспечение		Невозобновляемое	Ответственный за защиту информации, ведущий программист		Обновляется при появлении нового ПО

Приложение 2

ПЛАН

Обеспечения непрерывной работы и восстановления информации

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Неправомерные действия со стороны лиц допущенных к защищаемой информации					
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение несанкционированно скопированной или измененной конфиденциальной информации			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней			Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Несанкционированный доступ к информации					

[1] В случае отсутствия лиц, которые должны оповещаться, их замещают лица, определенные в разделе «Порядок замещения ответственных лиц» настоящей Инструкции. Либо могут быть оповещены непосредственные руководители

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Обнаружение подключения технических средств к средствам и системам объекта информатизации		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Подключение технических средств к средствам и системам ИСПДн в текущий момент времени			Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Обнаружение закладочных устройств			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Установка закладочных устройств злоумышленником в текущий момент времени			Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени			Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	5 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Использование дефектов программного обеспечения ИСПДн внешним нарушителем в текущий момент времени		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внешним нарушителем в текущий момент времени			Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внутренним злоумышленником или обнаружение факта использования			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение программных вирусов			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		12 часов
Хищение носителя защищаемой информации			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
	Нарушена работа группы пользователей	Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента		2 дня
	Нарушена работа группы пользователей		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента		1 день
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку					
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени			Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Ошибки пользователей системы					
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя		Ответственному за защиту информации (или лицу его замещающему) в первый рабочий день после инцидента	20 минут	2 дня
	Нарушена работа группы пользователей		Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	20 минут	1 день
Объективные факторы					
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ИСПДн	Сбой ТС и систем ИСПДн	Ответственному за защиту информации (или лицу его замещающему) сразу после инцидента	Ответственному за защиту информации (или лицу его замещающему) сразу после инцидента	1 час	2 дня

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
	Отказ ТС и систем ИСПДн, затронувший работу группы пользователей	Ответственному за защиту информации (или лицу его замещающему) сразу после обнаружения инцидента	Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
	Отказ ТС и систем ИСПДн, затронувший работу одного пользователя		Ответственному за защиту информации (или лицу его замещающему) в первый рабочий день после инцидента	1 час	2 дня
	Авария ТС и систем ИСПДн		Ответственному за защиту информации (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	1 день
Сбои, отказы и аварии систем обеспечения ИСПДн	Сбой систем обеспечения ИСПДн	Заместителем директора по АХЧ сразу после инцидента	Заместителем директора по АХЧ в первый рабочий день после инцидента		
	Отказ систем обеспечения ИСПДн, затронувший работу группы пользователей	Заместителю директора по АХЧ и ответственному за защиту информации (или лицам их замещающим) сразу после обнаружения инцидента	Заместителю директора по АХЧ и ответственному за защиту информации (или лицам их замещающим) сразу после обнаружения инцидента		1 день

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
	Отказ систем обеспечения ИСПДн, затронувший работу одного пользователя	Заместителю директора по АХЧ сразу после инцидента	Заместителю директора по АХЧ в первый рабочий день после инцидента		2 дня
	Авария систем обеспечения ИСПДн	Заместителю директора по АХЧ, ответственному за защиту информации (или лицам их замещающим) сразу после обнаружения инцидента	Заместителю директора по АХЧ, ответственному за защиту информации (или лицам их замещающим) как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Природные явления, стихийные бедствия, несущие угрозу жизни человека		Директору, заместителям директора, которые оповещают всех своих сотрудников сразу после получения информации	Директору, заместителям директора, которые оповещают всех своих сотрудников сразу после получения информации		30 минут
Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Директору, заместителям директора, ответственному за защиту информации (или лицу его замещающему)	Директору, заместителям директора, ответственному за защиту информации (или лицу его замещающему)		30 минут

Приложение 3

ЖУРНАЛ
учета нештатных ситуаций

№ п/п	Дата, ИСПДн, ПЭВМ, описание ситуации, выполненные работы	Подпись исполнителя	Подпись администратора

Приложение 4

Ведомость регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение 5

Ведомость ознакомления с Инструкцией

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении