|  |
| --- |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**(наименование организации) |
| Адрес:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Тел: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  Факс: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Адрес сайта: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  E-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ИНН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  КПП \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ОКПО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  ОГРН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **УТВЕРЖДАЮ** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  *(должность)* |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
|  *(подпись* |  *(расшифровка подписи)* |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 201\_г. |

**Инструкция пользователям информационных систем персональных данных (полное название предприятия)**

**по действиям в нештатных ситуациях**

г. Краснодар 201\_ г.

**Список сокращений**

|  |  |  |
| --- | --- | --- |
| ИСПДН |  | Информационная система персональных данных |
| ИБ |  | Информационная безопасность |
| ПДн |  | Персональные данные |
| ПО |  | Программное обеспечение |
| ПЭВМ |  | Персональная электронная вычислительная машина |
| САЗ |  | Система антивирусной защиты |
| СВТ |  | Средства вычислительной техники |
| АРМ |  | Автоматизированное рабочее место |
| ТС |  | Технические средства |

**Содержание:**

1. Общие положения 4

2. Порядок действий при обнаружении нештатных ситуаций 5

3. ПроВЕДЕНИЕ расследований 15

4. ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ 16

5. Порядок замещения ответственных лиц 16

6. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ 16

ПРИЛОЖЕНИЕ 1. СРЕДСТВА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ 18

ПРИЛОЖЕНИЕ 2. ПЛАН ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ 19

ПРИЛОЖЕНИЕ 3. ЖУРНАЛ УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ 34

ПРИЛОЖЕНИЕ 4. ВЕДОМОСТЬ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ 35

ПРИЛОЖЕНИЕ 5. ВЕДОМОСТЬ ОЗНАКОМЛЕНИЯ 36

# Общие положения

Настоящая Инструкция предназначена для определения порядка действий пользователей информационной системы персональных данных (ИСПДн) (полное название предприятия) (далее – Предприятие) при возникновении нештатных ситуаций.

**Нештатными ситуациям являются:**

1. разглашение информации ограниченного доступа, не составляющей государственную тайну (далее защищаемая информация), сотрудниками Предприятия, 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;
1. неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
* несанкционированное изменение защищаемой информации;
* несанкционированное копирование защищаемой информации.
1. 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;
1. дефекты, сбои, отказы, аварии ТС и систем ИСПДН;
2. дефекты, сбои и отказы программного обеспечения ИСПДН;
3. сбои, отказы и аварии систем обеспечения ИСПДН;
4. 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 предприятия, вырабатывается конкретный план действий с учетом сложившийся ситуации.

Резервируемые на предприятии 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 предприятия знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции сотрудников предприятия осуществляет инженер-программист, или специалисты группы информационных систем предприятия, под роспись, с выдачей электронных копий Инструкции непосредственно для повседневного использования в работе.

# Порядок действий при обнаружении нештатных ситуаций

## Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице №1.

**Таблица №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 защищаемой 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) |
| 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) |

## 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 предприятия 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 организации, в которые произошла утечка конфиденциальной информации;
* определить возможные контрмеры, призванные уменьшить потери от утечки информации.

## 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.

### Первоочередные действия:

1. Инженером-программистом, и специалистами отдела информационных систем предприятия прерывает несанкционированный процесс;
2. Инженером-программистом, и специалистами отдела информационных систем предприятия блокирует доступ к ИСПДн предприятия для злоумышленника;
3. Инженером-программистом, и специалистами отдела информационных систем предприятия совместно с ответственным за обеспечение безопасности ПДн предприятия отстраняют нарушителя от средств ИСПДн;
4. Ответственным за обеспечение безопасности ПДн совместно с инженером-программистом, и специалистами отдела информационных систем предприятия предпринимаются действия по сбору и обеспечению сохранности улик.

### Последующие действия:

- создается комиссия для расследования инцидента.

## 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.

### Первоочередные действия:

- специалисты отдела информационных систем предприятия прерывают процесс работы нарушителя;

- в случае если нарушитель – пользователь ИСПДн, специалисты отдела информационных систем предприятия блокируют доступ в ИСПДн предприятия для нарушителя.

### Последующие действия:

- создается комиссия для расследования инцидента.

## Установка закладочных устройств злоумышленником в текущий момент времени

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

### Первоочередные действия:

- специалисты отдела информационных систем предприятия принимают меры к задержанию злоумышленника.

### Последующие действия:

- создается комиссия для расследования инцидента.

## Маскировка под зарегистрированного пользователя, внешним злоумышленником в текущий момент времени

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

### Первоочередные действия:

- специалисты отдела информационных систем предприятия блокируют доступ к ИСПДн Предприятия для злоумышленника.

### Последующие действия:

- создается комиссия для расследования инцидента.

## 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.

### Первоочередные действия:

- специалисты отдела информационных систем предприятия блокируют доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.

### Последующие действия:

- создается комиссия для расследования инцидента.

## Использование программных закладок внешним нарушителем в текущий момент времени

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

### Первоочередные действия:

- специалисты отдела информационных систем предприятия блокируют доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

### Последующие действия:

- специалисты отдела информационных систем предприятия определяют возможный ущерб, нанесенный программной закладкой.

- специалисты отдела информационных систем предприятия проводят мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

- составляется акт об инциденте.

## Обнаружение программных вирусов

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

## 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.

### Первоочередные действия:

- специалисты отдела информационных систем предприятия принимают меры по немедленному удалению злоумышленника от средств вычислительной техники.

- в случае если злоумышленник является пользователем системы, специалисты отдела информационных систем предприятия блокируют доступ к ИСПДн Предприятия для злоумышленника.

### Последующие действия:

- в случае наличия повреждений специалисты отдела информационных систем предприятия определяют ущерб, нанесенный ТС и информации.

- специалисты отдела информационных систем предприятия производят восстановление работоспособности системы.

- создается комиссия для расследования инцидента.

## Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником

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

1. Специалисты отдела информационных систем предприятия определяют возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.
2. Специалисты отдела информационных систем предприятия производят восстановление работоспособности системы.
3. Создается комиссия для расследования инцидента.

## 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.

### Первоочередные действия:

- специалисты отдела информационных систем предприятия выявляют источник ложных заявок.

- специалисты отдела информационных систем предприятия вырабатывают решение по блокированию потока ложных заявок и реализуют выбранное решение.

### Последующие действия:

- специалисты отдела информационных систем предприятия уведомляют провайдера, от которого идут ложные заявки, планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

- специалисты отдела информационных систем предприятия составляют акт об инциденте.

## 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:

- специалисты отдела информационных систем предприятия выявляют источник ложных заявок, и блокирует доступ к ИСПДн Предприятия для злоумышленника.

- создается комиссия для расследования инцидента.

## Блокировка доступа к защищаемой информации, произошедшая в прошлом

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

- специалисты отдела информационных систем предприятия выявляют источник ложных заявок.

- в случае если злоумышленник является внешним, специалисты отдела информационных систем предприятия уведомляют провайдера, от которого идут ложные заявки. Планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

- в случае если злоумышленник является внешним, специалисты отдела информационных систем предприятия составляют акт об инциденте.

- создается комиссия для расследования инцидента.

## 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.

### Первоочередные действия:

- специалисты отдела информационных систем предприятия проводят анализ и идентификацию причин инцидента.

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

- специалисты отдела информационных систем предприятия определяют ущерб, нанесенный нештатной ситуацией.

- специалисты отдела информационных систем предприятия проводят мероприятия по восстановлению работоспособности системы и информации.

### Последующие действия:

- проводится проверка знаний сотрудника, виновного в инциденте, а в случае необходимости его обучение.

- специалисты отдела информационных систем предприятия составляют акт об инциденте, в случае необходимости выносит предложение директору о применении дисциплинарных мер в отношении нарушителя.

## 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.

### Первоочередные действия:

- специалисты отдела информационных систем предприятия проводят анализ и идентификацию причин инцидента.

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

### Последующие действия:

- специалисты отдела информационных систем предприятия определяют ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы.

- специалисты отдела информационных систем предприятия составляют 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.

## Дефекты, сбои, отказы, аварии ТС, программных средств и систем ИСПДн

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

### Первоочередные действия:

- специалисты отдела информационных систем предприятия выявляют возможные причины проявления дестабилизирующих факторов.

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

### Последующие действия:

- специалисты отдела информационных систем предприятия восстанавливает работоспособность систем.

- в случае потери данных специалистами отдела информационных систем предприятия по возможности проводится восстановление их из резервных копий.

- специалистами отдела информационных систем предприятия производится составление акта.

## 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, специалистами отдела информационных систем предприятия производится отключение серверов до момента истечения резервов системы бесперебойного питания.

- ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения.

- в случае потери защищаемых данных специалистами отдела информационных систем предприятия по возможности проводится восстановление их из резервных копий.

- ответственным за материально-техническое обеспечение производится составление акта.

## 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 (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 заранее разработанному и постоянно хранящемуся 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 Предприятия, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.

Руководители подразделений обязаны собрать в помещениях подразделения и лично упаковать, реквизиты защиты и документы согласно спискам первой очереди, сотрудников своего подразделения, отсутствующих на момент эвакуации на рабочих местах (болезнь, командировка, учеба, отпуск и т.д.).

Руководители обязаны:

* при подготовке к эвакуации проверить обеспеченность (а при отсутствии – обеспечить) сотрудников 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 сотрудников о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества подразделения и/или ИСПДн к эвакуации.

## 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 предприятия выключают свои персональные компьютеры.
2. Специалисты отдела информационных систем предприятия выключают серверы и сетевое оборудование.
3. Специалисты отдела информационных систем предприятия принимают 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, лицом, ответственным за материально-техническое обеспечение организуются работы по ликвидации нештатной ситуации и ее последствий.

# 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;
* инженер-программист;
* юрист;
* 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?

# ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:

* инженер – программист, а так же специалисты отдела информационных систем предприятия в части задач, возложенных на них 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.

# 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. Ответственный за обеспечение безопасности ПДн
2. Инженер - программист
3. Техник - программист.
4. Главный инженер.

Ответственные за материально-техническое обеспечение:

1. Инженер-программист.
2. Техник - программист.
3. Главный инженер.

# ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИСПДн Предприятия. 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 предприятия.

Инструкция подлежит частичному пересмотру в следующих случаях:

* изменений местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;
* определении такой необходимости в выводах комиссии по результатам расследования нештатной ситуации;
* необходимости повышения эффективности мероприятий, определенных в настоящей инструкции;
* изменения состава, обязанностей и полномочий должностных лиц предприятия, которые задействованы в мероприятиях настоящей Инструкции.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн предприятия и инженером - программистом, с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Предприятия.

Частичный пересмотр данного документа проводится инженером - программистом. Частичный пересмотр должен проводиться регулярно, не реже одного раза в полгода. 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.

Инженер по защите информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 *(подпись) (расшифровка подписи)*

**Приложение №1**

**к Инструкции пользователям информационных систем**

**персональных данных по действиям в нештатных ситуациях**

**СРЕДСТВА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ**

Резервному копированию (РК) подлежит следующая информация:

* системные программы и наборы данных -  *не возобновляемому (однократному, эталонному) РК*;
* прикладное программное обеспечение и наборы данных - *не возобновляемому 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 | Ведущий инженер – программист, или техник-программист |  | Каждую пятницу |
| Эталонное программное обеспечение |  | Не возобновляемое | Ведущий инженер – программист, или техник-программист |  | Обновляется при появлении нового ПО |

**Приложение №2**

**к Инструкции пользователям информационных систем**

**персональных данных по действиям в нештатных ситуациях**

**План**

**Обеспечения непрерывной работы и восстановления информации**

| **Тип кризисной ситуации** | **Критерии кризисной ситуации** | **Кому [[1]](#footnote-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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента |  |  |
| Обнаружение несанкционированно скопированной или измененной конфиденциальной информации |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) |  |
| **Несанкционированный доступ к информации** |
| Обнаружение подключения технических средств к средствам и системам объекта информатизации |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) |  |
| Обнаружение закладочных устройств |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента |  |  |
| Использование дефектов программного обеспечения ИСПДН внешним нарушителем в текущий момент времени |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента |  |  |
| Обнаружение программных вирусов |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента |  | 12 часов |
| Хищение носителя защищаемой информации |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 2 дня |
| Нарушена работа группы пользователей | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента |  | 2 дня |
| Нарушена работа группы пользователей | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |
| Обнаружение произошедшего факта блокировки доступа к защищаемой информации |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 |  | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 | Ведущему инженеру - программисту (или лицу его замещающему) сразу после инцидента | Ведущему инженеру - программисту (или лицу его замещающему) в первый рабочий день после инцидента | 20 минут | 2 дня |
| Нарушена работа группы пользователей | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 | Ведущему инженеру - программисту (или лицу его замещающему) сразу после инцидента | Ведущему инженеру - программисту (или лицу его замещающему) сразу после инцидента | 1 час | 2 дня |
| Отказ ТС и систем ИСПДН, затронувший работу группы пользователей | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 | Ведущему инженеру - программисту (или лицу его замещающему) сразу после инцидента | Ведущему инженеру - программисту (или лицу его замещающему) в первый рабочий день после инцидента | 1 час | 2 дня |
| Авария ТС и систем ИСПДН | Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ведущему инженеру - программисту (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 | Ответственному за материально-техническое обеспечение сразу после инцидента | Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента |  |  |
| Отказ систем обеспечения ИСПДН, затронувший работу группы пользователей | Ответственному за материально-техническое обеспечение и Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ответственному за материально-техническое обеспечение и Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента |  | 1 день |
| Отказ систем обеспечения ИСПДН, затронувший работу одного пользователя | Ответственному за материально-техническое обеспечение сразу после инцидента | Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента |  | 2 дня |
| Авария систем обеспечения ИСПДН | Ответственному за материально-техническое обеспечение, Ведущему инженеру - программисту (или лицу его замещающему) сразу после обнаружения инцидента | Ответственному за материально-техническое обеспечение, Ведущему инженеру - программисту (или лицу его замещающему) как можно скорее, в дневное время, но не позднее 8 часов после инцидента  |  | 1 день |
| Природные явления, стихийные бедствия, несущие угрозу жизни человека |  | Руководителю, заместителям Руководителю, которые оповещают всех своих сотрудников сразу после получения информации  | Руководителю, заместителям Руководителю, которые оповещают всех своих сотрудников сразу после получения информации |  | 30 минут |
| Природные явления, стихийные бедствия, не несущие угрозу жизни человека |  | Руководителю, заместителям Руководителю, Ведущему инженеру - программисту (или лицу его замещающему) | Руководителю, заместителям Руководителю, Ведущему инженеру - программисту (или лицу его замещающему) |  | 30 минут |

**Приложение №3**

**к Инструкции пользователям информационных систем**

**персональных данных по действиям в нештатных ситуациях**

**Журнал**

**учета нештатных ситуаций**

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

**Приложение №4**

**к Инструкции пользователям информационных систем**

**персональных данных по действиям в нештатных ситуациях**

**Ведомость регистрации изменений в Инструкции**

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

**Приложение №5**

**к Инструкции пользователям информационных систем**

**персональных данных по действиям в нештатных ситуациях**

**Ведомость ознакомления с Инструкцией**

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

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 [↑](#footnote-ref-1)