УТВЕРЖДАЮ

Директор
ОБУК «Госдирекция»

_____ А.А. Найденов

«01» 04 2021 г.

МП

ИНСТРУКЦИЯ

по действиям персонала в нештатных ситуациях

Липецк 2021

Оглавление

1. Термины, определения и сокращения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Автоматизированная система (АС) - Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку

информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) - материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу(Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Физическая защита информации - защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

2. Назначение

2.1. Инструкция по действиям персонала в нештатных ситуациях предназначена для определения порядка действий сотрудников ОБУК «Госдирекция» (далее - Учреждения) при возникновении нештатных ситуаций.

2.2. В случае наличия нештатной ситуации порядок действий, при которой не регламентируется настоящей Инструкцией, Администратором безопасности совместно с ответственным за обеспечение обработки персональных данных и директором Учреждения вырабатывается конкретный план действий с учетом текущей ситуации.

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

2.4. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении 2 к настоящей Инструкции.

2.5. Все нештатные ситуации учитываются в журнале учета нештатных ситуаций (Приложение 3) или в электронной базе данных нештатных ситуаций (Приложение 4).

2.6. 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.

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

2.8. Ознакомление с требованиями Инструкции сотрудников осуществляет Администратор безопасности под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

2.9. Инструкция хранится у ответственного за конфиденциальное делопроизводство и при необходимости выдается Администратором безопасности.

3. Общие положения

3.1. Нештатными (кризисными) ситуациям являются:

3.1.1. Разглашение персональных данных, представленных в Перечне персональных данных (Приложение № 1 Приказа «О защите персональных данных автоматизированного рабочего места пользователя государственной информационной системы «Единая централизованная система бюджетного (бухгалтерского) учета и отчетности» учреждения «_____» рег. № ____ от ____), и иной конфиденциальной информации, подлежащей защите в Учреждении, сотрудниками, 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 (далее - ТС) обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;
- передача носителя информации (далее – НИ) лицу, не имеющему права доступа к ней;
- утрата НИ.

3.1.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение информации;
- несанкционированное уничтожение информации
- несанкционированное копирование информации.

3.1.3. Несанкционированный доступ к защищаемой информации:

- подключение ТС нарушителя к средствам и системам объекта информатизации (далее - ОИ);
- маскировка под зарегистрированного пользователя;
- использование дефектов программного обеспечения ОИ;
- использование программных закладок;
- применение вредоносного программного обеспечения;
- хищение носителя защищаемой информации;
- нарушение функционирования ТС обработки информации;

3.1.4. Дефекты, сбои, отказы, аварии ТС и систем ОИ.

3.1.5. Дефекты, сбои и отказы программного обеспечения ОИ.

3.1.6. Сбои, отказы и аварии систем обеспечения ОИ.

3.1.7. 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.).

4. Порядок действий при обнаружении нештатных ситуаций

4.1. Нештатная ситуация: Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа

Ситуация	Действия персонала
Обнаружился случившийся факт	1. Создается комиссия по расследованию инцидента.
Производится в текущий момент	1. Сотрудник Учреждения прерывает несанкционированный процесс. 2. Создается комиссия по расследованию инцидента.

4.2. Нештатная ситуация: Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации: несанкционированное копирование, изменение, уничтожение конфиденциальной информации.

Ситуация	Действия персонала
Обнаружился случившийся факт	1. Администратор безопасности блокирует доступ нарушителя в информационную систему (далее – ИС). 2. Начальник Учреждения с Администратором безопасности предпринимает действия по сбору и обеспечению сохранности улик. 3. Создается комиссия для расследования инцидента.
Производится в текущий момент	1. Администратор безопасности прерывает несанкционированный процесс. 2. Администратор безопасности блокирует доступ нарушителя в ИС. 3. Начальник Учреждения с Администратором безопасности предпринимают действия по сбору и сохранению улик. 4. Создается комиссия для расследования инцидента.

4.3. Нештатная ситуация: Несанкционированный доступ к защищаемой информации. Подключение технических средств к средствам и системам объекта информатизации.

Ситуация	Действия персонала
Обнаружился случившийся факт	1. Администратор безопасности блокирует доступ нарушителя в ИС. 2. При необходимости создается комиссия для расследования инцидента.
Производится в текущий момент	1. Администратор безопасности прерывает процесс работы нарушителя. 2. Администратор безопасности блокирует доступ нарушителя в ИС. 3. При необходимости создается комиссия для расследования инцидента.

4.4. Нештатная ситуация: Маскировка под зарегистрированного пользователя

Ситуация	Действия персонала
Внешним злоумышленником в текущий момент	1. Администратор безопасности прерывает процесс работы нарушителя. 2. Администратор безопасности предпринимает действия для задержания нарушителя. 3. Создается комиссия для расследования инцидента с привлечением правоохранительных органов.
Внутренним злоумышленником, либо производилась в прошлом	1. Администратор безопасности прерывает процесс работы нарушителя. 2. Создается комиссия для расследования инцидента

4.5. Нештатная ситуация: Использование дефектов программного обеспечения объекта информатизации

Ситуация	Действия персонала
Внешним злоумышленником в текущий момент. Внутренним злоумышленником, либо производилась в прошлом	1. Администратор безопасности прерывает процесс работы нарушителя. 2. Администратор безопасности блокирует доступ нарушителя в ИС. 3. При необходимости создается комиссия для расследования инцидента.

4.6. Нештатная ситуация: Использование программных закладок

Ситуация	Действия персонала
Внешним злоумышленником в текущий момент. Внутренним злоумышленником, либо производилась в прошлом.	1. Администратор безопасности прерывает процесс работы нарушителя. 2. Администратор безопасности блокирует доступ нарушителя в ИС. 3. Администратор безопасности определяет возможный ущерб, нанесенный программной закладкой. 4. Администратор безопасности составляет акт об инциденте.

4.7. Нештатная ситуация: Нарушение функционирования технических средств обработки информации злоумышленником

Ситуация	Действия персонала
Производится в текущий момент	1. Администратор безопасности принимает меры по немедленному удалению злоумышленника от средств вычислительной техники. 2. В случае если злоумышленник является пользователем системы, Администратор безопасности блокирует его доступ к ИС. 3. В случае наличия повреждений Администратор безопасности определяет ущерб, нанесенный ТС и информации. 4. Администратор безопасности производит восстановление работоспособности системы. 5. Создается комиссия для расследования инцидента
Обнаружился случившийся факт	1. В случае наличия повреждений Администратор безопасности определяет возможный круг лиц, причастных к нарушению, ущерб, нанесенный ТС и информации. 2. Администратор безопасности производит восстановление работоспособности системы. 3. Создается комиссия для расследования инцидента

4.8. Нештатная ситуация: Ошибки пользователей системы при эксплуатации программных средств, технических средств, средств и систем защиты информации

Ситуация	Действия персонала
Ошибка повлекла утерю, повреждение защищаемой информации или привела к	1. Администратор безопасности проводит анализ и идентификацию причин инцидента. 2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции. 3. Администратор безопасности определяет ущерб, нанесенный

нарушению работоспособности	нештатной ситуацией. 4. Администратор безопасности проводит мероприятия по восстановлению работоспособности системы и информации. 5. Проводится проверка знаний сотрудника виновного в инциденте, а в случае необходимости его обучение. 6. Администратор безопасности составляет акт об инциденте, в случае необходимости выносят предложение директору Учреждения о применении дисциплинарной меры в отношении нарушителя.

4.9. Нештатная ситуация: Хищение носителя защищаемой информации.

Действия персонала:

4.9.1. Создается комиссия для расследования инцидента.

4.10. Нештатная ситуация: Обнаружение программных вирусов.

Действия персонала:

4.10.1. Администратор безопасности прерывает процесс работы ИС.

4.10.2. Администратор безопасности определяет возможный ущерб, нанесенный программно-математическим воздействием.

4.10.3. Администратор безопасности проводит контроль ИС в соответствии с требованиями по организации антивирусной защиты.

4.10.4. Администратор безопасности составляет акт об инциденте.

4.11. Нештатная ситуация: Дефекты, сбои, отказы, аварии технических средств, программных средств и систем объекта информатизации.

Действия персонала:

4.11.1. Администратор безопасности выявляет возможные причины проявления дестабилизирующих факторов.

4.11.2. В случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции.

4.11.3. Администратор безопасности восстанавливает работоспособность систем.

4.11.4. В случае потери данных Администратором безопасности по возможности проводится восстановление их из резервных копий.

4.11.5. Администратором безопасности ИС составляется акт об инциденте.

4.12. Нештатная ситуация: Сбои, отказы и аварии систем обеспечения ОИ.

Действия персонала:

4.12.1. В случае если наблюдается продолжительное отключение электропитания. Администратором безопасности производится отключение серверов до момента истечения резервов системы бесперебойного питания.

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

4.12.3. В случае потери защищаемых данных Администратором безопасности по возможности проводится восстановление их из резервных копий.

4.12.4. Ответственный за материально-техническое обеспечение составляет акт об инциденте.

5. Порядок действий по защите информации и ее носителей при возникновении пожара

5.1. В целях противопожарной подготовки сотрудников ответственный за противопожарные мероприятия по согласованию со своим непосредственным руководителем:

5.1.1. разрабатывает план эвакуации носителей информации, средств вычислительной техники и имущества;

5.1.2. определяет очередность эвакуации (с учетом первоочередности эвакуации и охраны носителей защищаемой информации и технических средств ее обработки);

5.1.3. определяет места складирования эвакуированного имущества и порядок его охраны;

5.1.4. разрабатывает пожарный расчет сотрудников подразделения в соответствии со штатным расписанием и инструкции на случай пожара;

5.1.5. организует взаимодействие с ответственными за противопожарное состояние других подразделений, размещаемых в здании, по оповещению руководства в случае возникновения пожара (особенно в нерабочее время);

5.1.6. организует обучение сотрудников.

6. Порядок действий при возникновении пожара в помещениях в рабочее время:

6.1. Обязанности сотрудника:

6.1.1. немедленно сообщает об этом руководителю подразделения (в его отсутствии — старшему по штатному расписанию);

6.1.2. оповещает сотрудников подразделения;

6.1.3. приступает в соответствии с обязанностями по пожарному расчету или по указанию руководства к ликвидации очага возгорания, эвакуации закрепленных за ним носителей информации и средств вычислительной техники, их охране.

6.2. Обязанности администратора безопасности:

6.2.1. руководит действиями сотрудников в соответствии с утвержденным пожарным расчетом;

6.2.2. контролирует очередность эвакуации имущества и непосредственно организует его охрану на месте эвакуации.

6.3. Обязанности руководителя подразделения или лица, его замещающего:

6.3.1. осуществляет общее руководство тушением пожара, эвакуацией имущества и персонала;

6.3.2. контролирует организацию охраны носителей защищаемой информации и технических средств ее обработки.

7. Порядок действий при возникновении пожара в помещениях в нерабочее время:

7.1. Обязанности руководителя подразделения или лица, его замещающего (первый из прибывших или старший по штатному расписанию):

7.1.1. вызывает должностное лицо соответствующего подразделения и сотрудников согласно пожарному расчету;

7.1.2. уточняет место складирования и организует во взаимодействии с пожарным подразделением эвакуацию носителей защищаемой информации и технических средств ее обработки;

7.1.3. организует их охрану;

7.1.4. назначает комиссию по проверке наличия служебных документов;

7.1.5. сообщает о происшествии и результатах проверки администратору безопасности.

8. Общий порядок действий при обнаружении нештатных ситуаций

8.1. При обнаружении любых нештатных ситуаций сотрудники Учреждения или Администратор безопасности сообщают об инциденте директору Учреждения. При обнаружении нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником, созывается постоянно действующая техническая комиссия.

8.2. При нештатных ситуациях, связанных с:

8.2.1. разглашением конфиденциальной информации;

8.2.2. обнаружением несанкционированно скопированной или измененной конфиденциальной информации;

8.2.3. обнаружением подключения технических средств к средствам и системам объекта информатизации;

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

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

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

8.2.7. хищением носителя защищаемой информации.

8.3. В первую очередь, Администратором безопасности предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника.

8.4. Комиссия, дополнительно к общему порядку действий, должна, если это возможно, определить организации, в которые произошла утечка конфиденциальной информации и определить возможные контрмеры, призванные уменьшить потери от утечки информации.

9. Проведение расследований

9.1. Для расследования опасных ситуаций в случаях предусмотренных настоящей Инструкцией может созываться постоянно действующая техническая комиссия или комиссия, составленная из других сотрудников организации по решению директора Организации.

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

9.3. В общем случае комиссия проводит:

9.3.1. анализ и идентификацию причин инцидента, определение виновных лиц;

9.3.2. определение ущерба, нанесенного нештатной ситуацией;

9.3.3. планирование мер для предотвращения повторения нештатной ситуации и нейтрализации последствий (если это возможно);

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

9.3.5. определение меры взыскания с виновного;

9.3.6. взаимодействие, при необходимости с правоохранительными органами.

9.4. При сохранении улик:

9.4.1. если есть возможность, Администратором безопасности производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая журналы событий (контрольные записи).

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

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

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

9.7.1. можно ли было предусмотреть нештатную ситуацию?

9.7.2. вызвана ли она слабостью средств защиты и регистрации?

9.7.3. это первая кризисная ситуация такого рода?

9.7.4. достаточно ли имеющегося резерва?

9.7.5. есть ли необходимость пересмотра системы защиты?

9.7.6. есть ли необходимость пересмотра настоящей инструкции?

10. Ответственные за контроль выполнения инструкции

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

10.1.1. Администратор безопасности в части задач, возложенных на него настоящей инструкцией.

10.1.2. Начальник Учреждения в части общего контроля.

10.1.3. Ответственный за материально-техническое обеспечение в части задач, возложенных на него настоящей инструкцией.

11. Порядок пересмотра инструкции

11.1. Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИС, 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 ИС Учреждения.

11.2. Инструкция подлежит частичному пересмотру в следующих случаях:

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

11.2.2. при определении такой необходимости комиссией по результатам расследования нештатной ситуации;

11.2.3. в целях повышения эффективности мероприятий определенных в настоящей инструкции;

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

11.3. Полный пересмотр данного документа проводится Администратором безопасности, руководителем Учреждения с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИС Учреждения.

11.4. Частичный пересмотр данного документа проводится Администратором безопасности. 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 5) без переутверждения всей Инструкции.

Приложение 1.

Средства обеспечения непрерывной работы и восстановления

Резервному копированию (далее - РК) подлежит следующая информация:

- все файлы операционной системы и установленных приложений - не возобновляемому (однократному, эталонному) РК (РК должно производиться, в том числе, после установки новых приложений или обновления самой операционной системы);
- наборы данных, генерируемые в течение рабочего дня и содержащие ценную информацию (базы данных; папки, содержащие важные документы; журналы транзакций; системный журнал и т.д.) — периодическому возобновляемому РК.

Резервному копированию в организацию подлежат следующие программные и информационные ресурсы указанные в таблице:

Наименование инф. ресурса	Где размещается ресурс в системе	Вид резервного копирования	Ответственный исполнитель резервного копирования	Расположение резервных копий и используемые средства	Частота периодического резервирования
Операционная система и установленное программное обеспечение		Однократное			При изменении состава ОС и ПО
Журналы целостности специализированного ПО		Периодическое			Еженедельно в конце рабочей недели
Персональные данные граждан Липецкой области		Периодическое			Еженедельно в конце рабочей недели

Приложение 2.

План обеспечения непрерывной работы и восстановления информации

Тип кризисной ситуации	Критерии кризисной ситуации	Кому 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	Руководителю, администратору безопасности сразу после обнаружения инцидента	Сразу после обнаружения инцидента	не позднее 8 часов после инцидента	в дневное время но не позднее 8 часов после инцидента
	Обнаружение несанкционировано скопированной или измененной конфиденциальной информации	Руководителю, администратору безопасности сразу после обнаружения инцидента	Сразу после обнаружения инцидента		в дневное время, но не позднее 8 часов после инцидента
	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц не имеющих право доступа к ней	Руководителю, администратору безопасности сразу после обнаружения инцидента	Сразу после обнаружения инцидента	10 минут	1 час
Несанкционированный доступ к информации	Обнаружение подключения технических средств к средствам и системам объекта информатизации	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, но не позднее 8 часов после инцидента	10 минут	1 час
	Подключение технических средств к средствам и системам ОИ в текущий момент времени	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента	10 минут	1 час

	Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента	5 минут	1 час
Несанкционированный доступ к информации	Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	3 часа
	Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента	3 часа	8 часов
	Использование программных закладок внешним нарушителем в текущий момент времени	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента	1 час	8 часов
	Использование программных закладок внутренним злоумышленником или обнаружение факта использования	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	8 часов
	Обнаружение программных вирусов	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	10 мин	1 час
	Хищение носителя защищаемой информации	Руководителю, администратору безопасности сразу после	Администратором безопасности как можно скорее, в	1 час	3 часа

		обнаружения инцидента	дневное время, но не позднее 8 часов после инцидента		
	Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента.	1.день	2дня
	Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента.	1 день	2 дня
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 внутренним злоумышленником в текущий момент времени	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут 20 минут	1 час 1 час
	Обнаружение произошедшего факта блокировки доступа к защищаемой информации	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 день	1 день
Ошибки пользователей системы, неквалифицированные действия пользователей или	При эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа	12 часов

обслуживающего персонала	При эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО. Нарушена работа одного пользователя	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности в первый рабочий день после инцидента	20 минут	1 час
	При эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО. Нарушена работа группы пользователей	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности сразу после обнаружения инцидента в1 день	3 часа	8 часов
Объективные факторы	Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ Сбой ТС и систем ОИ	Руководителю, администратору безопасности сразу после инцидента	Администратором безопасности сразу после инцидента 2 дня	1 час	8 часов
	Отказ ТС и систем ОИ, затронувший работу группы пользователей	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента 1 день	1 час	8 часов
	Отказ ТС и систем ОИ, затронувший работу одного пользователя	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности в первый рабочий день после инцидента.	1 час	3 часа
	Авария ТС и систем ОИ	Руководителю, администратору безопасности сразу после обнаружения инцидента	Администратором безопасности как можно скорее, в дневное время, но не позднее 8 часов после инцидента	3 часа	8 часов

			1 день		
	Сбои, отказы и аварии систем обеспечения ОИ	Руководителю, ответственному за материально-техническое обеспечение (далее – МТО) сразу после обнаружения инцидента	Ответственным за МТО в первый рабочий день после инцидента	1 день	1 день
	Отказ систем обеспечения ОИ, затронувший Работу группы пользователей Работу одного пользователя	Руководителю, ответственному за МТО и администратору безопасности сразу после обнаружения инцидента	Ответственным за МТО и администратором БИ сразу после обнаружения инцидента 1 день 2 дня	1 день	1 день
	Авария систем обеспечения ОИ	Руководителю, ответственному за МТО и администратору безопасности сразу после обнаружения инцидента	Ответственным за МТО, администратором БИ как можно скорее, в дневное время, но не позднее 8 часов после инцидента 1 день	1 день	1 день
Объективные факторы	Природные явления, стихийные бедствия, несущие угрозу жизни человека	Руководителю, заместителю директора, которые оповещают всех своих сотрудников сразу после получения информации	Директором, заместителем директора, которые оповещают всех своих сотрудников сразу после получения информации	30 минут	
	Природные явления, стихийные бедствия, не несущие угрозу жизни человека	Руководителю, заместителям руководителя, администратору безопасности	Руководителем, заместителем Руководителя, Администратором безопасности	30 минут	

Приложение 3.

ТИПОВАЯ ФОРМА

журнала по учету контроля обеспечения защиты персональных данных и нештатных ситуаций ИС

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение 4.

База данных о нештатных ситуациях

1. Для ведения единой базы информации о нештатных ситуациях Администратором безопасности создается электронная база данных.

2. Доступ к созданной базе данных должны иметь Администратор безопасности и другие должностные лица ОБУК «Госдирекция» задействованные в выполнении положений настоящей Инструкции.

3. Участвовавшим в нейтрализации нештатной ситуации Администратором безопасности, а в случае его неучастия, либо отсутствия другими лицами создается запись в электронной базе данных нештатных ситуаций. Запись создается по происшествию не более 8 часов после инцидента.

4. Электронная база данных ежегодно анализируется Администратором безопасности и директором ОБУК «Госдирекция».

5. Записи о нештатных ситуациях должны иметь следующую форму:

5.1. Вид нештатной ситуации: В соответствии с Приложением 2 могут быть указаны следующие виды нештатной ситуации:

- неправомерные действия со стороны лиц допущенных к защищаемой информации;
- несанкционированный доступ к информации;
- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками;
- ошибки пользователей системы;
- объективные факторы.

5.2. Тип: «Общее название нештатной ситуации в соответствии с названием подраздела настоящей Инструкции».

5.3. Описание: «Детализация нештатной ситуации, например, обрыв канала связи в Internet и т.п.».

Приложение 5.

Лист ознакомления

№ п/п	Ф.И.О.	Роспись	Дата
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			