Утверждено приказом
ООО «ЛОУДЕР ЭСПИИКС»
№ ____ от «09» января 2023 г.

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2023 год
Москва

СОДЕРЖАНИЕ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Термины и определения**

В настоящем документе использованы следующие термины и определения:

1.1.1. **Безопасность персональных данных** – состояние защищенности персональных данных от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке, независимо от формы их представления.

1.1.2. **Вредоносное программное обеспечение** – программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

1.1.3. **Доступность персональных данных** – возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

1.1.4. **Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1.1.5. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.1.6. **Инцидент безопасности персональных данных** – любое непредвиденное или нежелательное событие, которое может нарушить безопасность персональных данных, что может повлечь за собой нарушение деятельности Компании.

1.1.7. **Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта персональных данных или иного законного основания.

1.1.8. **Криптографическая защита** – защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

1.1.9. **Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

1.1.10. **Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

1.1.11. **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.

1.1.12. **Объем обрабатываемых персональных данных** – количество субъектов персональных данных, чьи данные обрабатываются в Компании.

1.1.13. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.1.14. **Пользователь персональных данных** – лицо, участвующее в процессе обработки персональных данных или использующее результаты такой обработки.

1.1.15. **Процесс обработки персональных данных** – бизнес-процесс Компании, в рамках которого осуществляется обработка персональных данных.

1.1.16. **Средство вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

1.1.17. **Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.1.18. **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

1.1.19. **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.

1.1.20. **Целостность персональных данных** – способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного их искажения (разрушения).

1.2. Используемые сокращения

В настоящем документе использованы сокращения, приведенные в Таблице 1.

Таблица 1.

Сокращения

Сокращение	Описание
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных
СКС	Структурированная кабельная система
СКУД	Система контроля управления доступом
УБПДн	Угроза безопасности персональных данных

2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ ДОКУМЕНТА

2.1. Настоящее Положение об обеспечении безопасности персональных данных (далее – "Положение") предназначено для применения при организации и проведении следующих работ:

– поддержание порядка обеспечения безопасности ПДн в Обществе с ограниченной ответственностью «ЛОУДЕР ЭСПИИКС» (далее – "Компания") в соответствии с требованиями нормативных документов РФ, регламентирующих данную область;

– обеспечение целостности, конфиденциальности и доступности ПДн при их обработке в Компании;

– определение мер по защите ПДн, обрабатываемых в т. ч. без использования средств автоматизации.

2.2. Требования настоящего Положения распространяются на структурные подразделения Компании и должностных лиц, принимающих участие в обеспечении безопасности ПДн, в т. ч. на Комиссию по обеспечению безопасности ПДн (далее – "Комиссия").

2.3. Настоящее Положение не распространяется на обеспечение безопасности сведений ограниченного доступа (в т. ч. конфиденциальной информации), не содержащих ПДн.

2.4. Настоящее Положение должен быть доведено до всех лиц, участвующих в обеспечении безопасности ПДн в Компании, под подпись.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Мероприятия по обеспечению безопасности ПДн в Компании осуществляются в рамках Системы защиты персональных данных (далее – "СЗПДн"). Мероприятия по обеспечению безопасности ПДн состоят из следующих работ:

- работы по обеспечению безопасности ПДн в рамках жизненного цикла ИСПДн;
- мониторинг и планирование;
- модернизация;
- эксплуатация;
- реагирование на инциденты безопасности;
- внутренние контрольные мероприятия;
- корректирующие действия.

3.2. Состав, последовательность и периодичность проведения указанных работ описаны в настоящем Положении и могут меняться при изменении процессов обработки и обеспечения безопасности ПДн в Компании, а также ИТ-инфраструктуры.

4. МЕРОПРИЯТИЯ В РАМКАХ ЖИЗНЕННОГО ЦИКЛА ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ, выполняемых в рамках жизненного цикла ИСПДн. Работы по обеспечению безопасности ПДн привязаны к жизненному циклу ИСПДн, а именно, к следующим этапам:

- инициализация проекта по созданию ИСПДн;
- проектирование ИСПДн;
- реализация ИСПДн;
- эксплуатация ИСПДн;
- вывод ИСПДн из эксплуатации.

Необходимые работы по защите ПДн с привязкой к этапам жизненного цикла ИСПДн приведены в Таблице 2.

Таблица 2.

Описание необходимых работ по защите ПДн на отдельных этапах жизненного цикла ИСПДн

№ п/п	Стадия существования ИСПДн, необходимые мероприятия	Детализация проводимых работ
1	***Инициализация проекта по созданию ИСПДн***	
1.1	Определение ИСПДн	При создании новой информационной системы (или существенном изменении существующей) определяется необходимость обработки ПДн. Если обработка ПДн необходима, то система объявляется информационной системой персональных данных, либо включается в состав уже существующей ИСПДн
1.2	Определение ключевых сведений об ИСПДн	На данном этапе производится: - определение перечня и категории ПДн, которые будут обрабатываться в ИСПДн; - определение целей обработки ПДн, перечня основных процессов обработки ПДн в рамках ИСПДн; - определение перечня прикладного программного обеспечения, аппаратных средств обработки и защиты ПДн, предполагаемых к использованию в составе ИСПДн

№ п/п	Стадия существования ИСПДн, необходимые мероприятия	Детализация проводимых работ
1.3	Правовая оценка возможности создания ИСПДн	На данном этапе производится оценка соответствия процессов обработки ПДн в рамках ИСПДн принципам и правилам обработки ПДн, указанным в документе «Положение об обработке персональных данных». В частности производится оценка: − целей обработки ПДн; − операций, которые будут выполняться с ПДн; − необходимости и возможности сбора согласий субъектов на обработку ПДн; − степени участия контрагентов Компании в обработке ПДн и необходимых юридических оснований для такой обработки
2	***Проектирование ИСПДн***	
2.1	Определение необходимости корректировки документации Компании	На данном этапе определяется необходимость корректировки следующих документов: − Положение по обработке персональных данных; − Настоящее Положение; − Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных (в состав которой включается новая система, либо в которой производятся существенные изменения); − Акт определения уровня защищенности персональных данных при обработке в информационной системе персональных данных (в состав которой включается новая система, либо в которой производятся существенные изменения); − Уведомление в Роскомнадзор о своем намерении осуществлять обработку ПДн (при необходимости)
2.2	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения безопасности ПДн и определение перечня актуальных угроз безопасности ПДн в конкретных условиях функционирования (разработка модели угроз и нарушителя безопасности ПДн)	Производится на основе уже существующих в Компании методик, описанных в утвержденных моделях угроз

№ п/п	Стадия существования ИСПДн, необходимые мероприятия	Детализация проводимых работ
2.3	Определение уровня защищенности ПДн при обработке в ИСПДн	Уровень защищенности ПДн при обработке в ИСПДн определяется в соответствии с [11.1] и с учетом типов актуальных угроз безопасности персональных данных. Результаты фиксируются в Акте определения уровня защищенности ПДн при обработке в ИСПДн
2.4	Определение требований к защите ПДн при их обработке в ИСПДн	Определяются конкретные требования к организационным и техническим мерам в СЗПДн, которые соответствуют требованиям нормативных документов РФ в области обработки и обеспечения безопасности ПДн и которые позволяют снизить вероятность реализации УБПДн. Форма фиксации требований к СЗПДн определятся Комиссией. Рекомендуемой формой является разработка (доработка) Технического задания на создание СЗПДн
2.5	Разработка проектного решения по защите ПДн в ИСПДн	Выполнение требований к защите ПДн при их обработке в ИСПДн осуществляется путем разработки проектного решения, которое может включать в себя внедрение организационных или технических мер, изменение процессов обработки ПДн и т. п. В случае если было разработано несколько вариантов проектных решений, Комиссия проводит сравнение предложенных вариантов и выбирает окончательный. Форма фиксации проектного решения по реализации СЗПДн определятся Комиссией. Рекомендуемой формой является разработка (доработка) Технического проекта на создание СЗПДн
3	***Реализация ИСПДн***	
3.1	Внедрение комплекса средств обработки и защиты ПДн, а также мер защиты ПДн в соответствии с проектной документацией на ИСПДн и СЗПДн	Производятся монтажные, пуско-наладочные работы средств обработки и средств защиты информации. Производится реализация комплекса организационно-технических мероприятий по защите ПДн
3.2	Проводится инструктаж работников по правилам обработки ПДн	Детализация проводимых работ приведена в документе «Положение по обработке персональных данных»
3.3	Сбор согласий субъектов на обработку ПДн	Проводится в случае необходимости, определенной в п. 1.3 данной таблицы

№ п/п	Стадия существования ИСПДн, необходимые мероприятия	Детализация проводимых работ
3.4	Внесение изменений в Уведомление Роскомнадзора о своем намерении осуществлять обработку ПДн	Проводится в случае необходимости, определенной в п. 2.1 данной таблицы. Порядок подачи Уведомления описан в документе «Положение по обработке персональных данных»
4	***Эксплуатация ИСПДн***	
4.1	Контроль изменений в составе и структуре ИСПДн	Детализация проводимых работ приведена в разделе 5 настоящего Положения
4.2	Поддержание в работоспособном состоянии	Детализация проводимых работ приведена в разделе 7.1 настоящего Положения
4.3	Допуск персонала к работе ПДн	Детализация проводимых работ приведена в разделе 7.2 настоящего Положения
4.4	Регистрация событий безопасности	Детализация проводимых работ приведена в разделе 7.3 настоящего Положения
4.5	Работа с носителям ПДн (учет, хранение и уничтожение)	Детализация проводимых работ приведена в разделе 7.4 настоящего Положения
4.6	Учет средств защиты информации	Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним осуществляется в рамках проектной документации, разрабатываемой на СЗПДн в соответствии с п. 2.5данной таблицы
4.7	Защита от несанкционированного физического доступа к элементам ИСПДн	Детализация проводимых работ приведена в разделе 7.5 настоящего Положения
4.8	Резервирование ПДн в ИСПДн, где необходимо обеспечить целостность или доступность ПДн	Детализация проводимых работ приведена в разделе 7.6 настоящего Положения
4.9	Управление уязвимостями	Детализация проводимых работ приведена в разделе 7.7 настоящего Положения
4.10	Реагирование на инциденты	Детализация проводимых работ приведена в разделе 8 настоящего Положения
4.11	Контроль за обеспечением необходимого уровня защищенности ПДн	Детализация проводимых работ приведена в разделе 9 настоящего Положения
4.12	Взаимодействие с субъектами ПДн по вопросам обработки их ПДн	Детализация проводимых работ приведена в документе «Регламент взаимодействия с субъектами персональных данных»

№ п/п	Стадия существования ИСПДн, необходимые мероприятия	Детализация проводимых работ
5	***Вывод из эксплуатации ИСПДн***	
5.1	Уничтожение ПДн	Детализация проводимых работ приведена в разделе 7.4 настоящего Положения
5.2	Модернизация СЗПДн	Детализация проводимых работ приведена в разделах 6 и 10 настоящего Положения

5. МОНИТОРИНГ И ПЛАНИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Мониторинг СЗПДн осуществляется с целью актуализации существующей СЗПДн в соответствии с текущими процессами обработки ПДн, элементами ИТ- и ИБ-инфраструктуры, и требованиями по безопасности ПДн.

В процессе мониторинга СЗПДн решаются задачи по актуализации:

- сведений о процессах обработки ПДн:
  - перечень ПДн, обрабатываемых в Компании;
  - объем обрабатываемых ПДн;
  - категории субъектов, чьи ПДн обрабатываются в Компании;
  - пользователи ПДн (структурные подразделения и отдельные работники) и третьи стороны (контрагенты, аутсорсинговые и обслуживающие организации и т. п.), имеющие доступ к ПДн;
  - структура и состав ИСПДн;
  - мероприятия и технические меры обеспечения безопасности ПДн.
- уровня защищенности ПДн при их обработке в ИСПДн, в т. ч.:
  - вреда, который может быть причинен субъектам ПДн в случае нарушения безопасности ПДн, и соответственно показателя опасности угроз безопасности в отдельных ИСПДн;
  - угроз безопасности ПДн.
- требований к СЗПДн;
- документации на СЗПДн;
- вариантов реализации СЗПДн (в т. ч. проведение дополнительных мероприятий по защите ПДн).

5.2. Принятые решения по результатам мониторинга фиксируются в Плане мероприятий по обеспечению безопасности ПДн. План работ также составляется на основе результатов реагирования на инциденты безопасности и проведения контрольных мероприятий. Планирование работ (в т. ч. назначение ответственных) осуществляется Комиссией не реже одного раза в 3 (три) года.

6. МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В соответствии с утвержденным Планом мероприятий по обеспечению безопасности ПДн проводятся работы по модернизации СЗПДн. Работы могут проводиться как собственными силами Компании, так и с привлечением третьих сторон (подрядчика) – компаний, оказывающих услуги в области ИБ. Обязательным требованием для подрядчиков является наличие лицензии на деятельность по технической защите конфиденциальной информации.

6.2. Комиссия осуществляет контроль работ по модернизации СЗПДн на всех стадиях.

6.3. Все изменения в составе и структуре ИСПДн должны контролироваться. Контролю подлежат следующие изменения:

– внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т. п.);

– изменение мест включения существующих компонент ИСПДн;

– удаление устройств из состава ИСПДн;

– изменение мест установки устройств в составе ИСПДн;

– прокладка новых кабельных линий связи СКС и внешних линий связи или удаление старых кабельных линий связи;

– существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

– создание новых и изменение существующих процессов обработки ПДн.

7. ЭКСПЛУАТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Процесс эксплуатации СЗПДн является непрерывным и постоянно поддерживается Ответственным за обеспечение безопасности ПДн. В процессе эксплуатации СЗПДн осуществляются следующие мероприятия:

- поддержание работоспособности компонентов СЗПДн;
- управление доступом к ПДн;
- регистрация событий безопасности ПДн;
- учет, хранение и уничтожение носителей ПДн;
- контроль использования технологий беспроводного доступа;
- управление информационными потоками;
- защита от несанкционированного физического доступа к элементам ИСПДн;
- резервирование ПДн;
- управление уязвимостями.

7.1. Поддержание работоспособности компонентов системы защиты персональных данных

В процессе эксплуатации в целях поддержания работоспособности компонентов СЗПДн Ответственный за обеспечение безопасности ПДн может в оперативном порядке вносить незначительные изменения в параметры конфигурации компонентов СЗПДн, не влияющие на установленные правила обеспечения безопасности ПДн в Компании.

В случае необходимости оперативного внесения существенных изменений, данный вопрос выносится на рассмотрение Комиссии.

7.2. Управление доступом к персональным данным

7.2.1. Оформление заявок на предоставление, изменение и прекращение прав доступа

Оформление заявки на предоставление, изменение или прекращение прав доступа к ПДн (далее – Заявка) осуществляется одним из следующих способов:

- заявка в бумажном виде (типовая форма Заявки приведена в Приложение А);
- электронная заявка.

Заявка подается Ответственному за обеспечение безопасности ПДн от имени Руководителя структурного подразделения, в котором числится работник. Заявка содержит следующие сведения:

- Ф.И.О. и должность руководителя структурного подразделения, подающего Заявку;
- Ф.И.О. и должность работника, которому необходимо предоставить, изменить или прекратить доступ;

– перечень компонентов ИСПДн, с указанием полномочий в рамках этих систем (например, 1С-Зарплата и управление персоналом чтение, 1С-Бухгалтерия чтение, запись, удаление);

– цели и основание для оформления доступа;

– дополнительные сведения при необходимости.

7.2.2. Предоставление прав доступа

Основанием для предоставления прав доступа к ПДн на постоянной основе является наем нового работника в штат Компании или перевод работника на должность, подразумевающую его участие в процессах обработки ПДн в рамках выполнения своих трудовых обязанностей.

По завершении предоставления доступа работнику, Ответственный за обеспечение безопасности ПДн уведомляет об этом руководителя, оформившего Заявку, электронным письмом или по телефону. Срок исполнения Заявки не превышает 3 рабочих дней.

Предоставление доступа к ПДн работнику, должность которого, не предполагает его участие в процессах обработки ПДн в рамках выполнения своих трудовых обязанностей, возможно только в случае необходимости разового временного доступа. Основанием для предоставления такого доступа является выполнение служебного задания, в рамках которого работнику требуется доступ к ПДн. Заявка на оформление разового временного доступа оформляется в соответствии с п. 7.2.1 настоящего Положения с дополнительным указанием служебного задания и времени, на которое предоставляется доступ. Заявка на предоставление разового доступа согласовывается с Ответственным за обеспечение безопасности ПДн. Срок рассмотрения Заявки на предоставление доступа может быть сокращен, если это связано с условиями выполнения служебного задания.

7.2.3. Пересмотр, изменение или прекращение прав доступа

Основаниями для пересмотра прав доступа являются:

– увольнение или перевод работника на должность, предусматривающую расширение, сокращение или прекращение прав доступа к ПДн;

– достижение заявленных целей, для которых предоставлялся разовый временный доступ к ПДн;

– проведение в отношении работника служебного расследования, в рамках которого работнику ограничиваются права доступа к ПДн.

Руководитель структурного подразделения, к которому относится работник, в течение одного рабочего дня с момента возникновения основания пересматривает права доступа к ПДн и принимает решение о целесообразности их изменения.

В случае принятия решения об изменении прав доступа к ПДн, Руководитель структурного подразделения оформляет заявку в соответствии с п. 7.2.1. Срок рассмотрения Заявки не превышает 3 рабочих дней.

7.2.4. Управление средствами аутентификации

Ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации является Ответственный за обеспечение безопасности ПДн.

Механизмы аутентификации должны быть реализованы с использованием защищенных протоколов аутентификации.

В случае использования в информационной системе механизмов аутентификации на основе пароля или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

– длина пароля не менее восьми символов;

– алфавит пароля не менее 70 символов;

– использование специальных символов, цифр, символов в верхнем регистре;

– обязательная смена пароля пользователем при первичной аутентификации;

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток;

– блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут;

– смена паролей не более чем через 90 дней.

Конфиденциальность паролей при хранении и передаче, должна обеспечиваться шифрованием или хешированием с применением стойких криптографических алгоритмов.

Должна обеспечиваться возможность назначения первичного пароля администратором ИСПДн и обязательной смены пароля пользователем при первичной аутентификации в ИСПДн.

Должно обеспечиваться явное ограничение или запрет на действия пользователя в ИСПДн до прохождения процедур идентификации и аутентификации. В частности, пользователю не должна выдаваться информация о типе и версии ИС или ее компонентов до успешного завершения процедур аутентификации.

7.3. Регистрация событий безопасности персональных данных

В Компании подлежит регистрации информация о следующих событиях безопасности в ИСПДн:

– вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (отключение) операционной системы;

– подключение машинных носителей информации и вывод информации на носители информации;

– запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

– попытки доступа программных средств к, определяемым оператором, защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

– попытки удаленного доступа.

События безопасности, подлежащие регистрации в ИСПДн, сроки их хранения, а также состав и содержание информации о событиях безопасности, приведены в Приложении Ж к настоящему Положению.

7.4. Порядок работы с носителями персональных данных

7.4.1. Общие правила использования машинных носителей персональных данных

Обработку ПДн на отчуждаемых машинных носителях (внешние жесткие диски, гибкие диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее)) разрешается осуществлять только в случае невозможности использования каналов связи корпоративной сети или внутренних защищенных мест хранения.

В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся Ответственному за обеспечение безопасности ПДн.

Передача машинного носителя ПДн третьим сторонам производится в порядке обмена носителями ПДн, закрепленном в договоре между Компанией и третьим лицом. В случае отсутствия в договоре порядка обмена носителями ПДн, порядок согласовывается с Ответственными за организацию обработки ПДн.

При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны Компании запрещается без соответствующего разрешения Ответственного за обеспечение безопасности ПДн.

7.4.2. Учет машинных носителей персональных данных

Учету подлежат следующие типы машинных носителей ПДн:

– отчуждаемые носители ПДн (внешние жесткие диски, гибкие диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее));

– неотчуждаемые носители ПДн (жесткие диски).

Машинные носители ПДн обязательно регистрируются и учитываются в Журнале учета носителей ПДн (типовая форма журнала приведена в ПриложениеБ). Регистрация и учет машинных носителей ПДн осуществляется в момент выдачи их Пользователям ПДн. Машинные носители ПДн выдаются для выполнения конкретных трудовых обязанностей и подлежат возврату по завершении работы с ними.

Для учета машинных носителей ПДн используются их серийные (заводские) номера, а при отсутствии такового – учетный номер. Учетный номер наносится на корпус носителя, его упаковку или на корпус СВТ, в котором он установлен. При маркировке корпуса СВТ должны быть реализованы меры по своевременному обнаружению вскрытия корпуса (например, учетный номер наносится на специальный стикер, который наклеивается на стык крышки и корпуса СВТ).

Неотчуждаемые носители ПДн закрепляются за работником, ответственным за СВТ, в котором они установлены.

7.4.3. Хранение машинных носителей персональных данных

Хранение машинных носителей ПДн осуществляется в условиях, исключающих возможность хищения, нарушения целостности или уничтожения содержащейся на них информации.

Отчуждаемые съемные носители после окончания работы с ними должны убираться в шкаф или ящик, запираемые на ключ.

Не допускается оставлять без присмотра на рабочем столе или в СВТ отчуждаемые машинные носители ПДн.

Персональную ответственность за сохранность полученных машинных носителей ПДн и предотвращение несанкционированного доступа к записанным на них ПДн несет Пользователь ПДн, за которым закреплен носитель.

7.4.4. Уничтожение персональных данных с машинного носителя

Основанием для уничтожения записей или части записей ПДн с машинного носителя являются следующие случаи:

– возврат носителя работником;

– передача носителя в ремонт;

– списание носителя.

Уничтожение ПДн с машинных носителей осуществляется с использованием средств гарантированного уничтожения Ответственным за обеспечение безопасности ПДн. По результатам уничтожения ПДн с носителя подготавливается Акт об уничтожении записей с носителя ПДн, Форма которого представлена в ПриложениеГ.

7.4.5. Хранение бумажных носителей персональных данных

Бумажные носители ПДн хранятся в шкафах или ящиках, запираемых на ключ. Главным условием хранения бумажных носителей ПДн является невозможность получения доступа к таким документам со стороны лиц, которым такой доступ не предоставлен.

Запрещается совместное хранение носителей ПДн с другими документами, не содержащими ПДн, кроме случаев, когда носители ПДн являются приложениями к другим документам или наоборот.

Во время работы на столе должны находиться только те носители, непосредственно с которыми ведется работа.

Носители ПДн должны быть убраны в шкаф или ящик, запираемые на ключ, в следующих случаях:

– когда с носителем ПДн не ведется работа;
– когда работник покидает рабочее место;
– по окончании рабочего дня.

Ответственность за соблюдение норм, описанных в данном разделе, возлагается на всех Пользователей ПДн, а контроль их выполнения возлагается на соответствующих Руководителей структурных подразделений.

7.4.6. Уничтожение бумажных носителей персональных данных в рабочем порядке

Основаниями для уничтожения носителей ПДн являются:

– достижение целей обработки ПДн;
– отсутствие необходимости использования носителя (при этом ПДн могут сохраняться в базах данных ИСПДн);
– отзыв согласия субъекта ПДн на обработку его ПДн;
– выявление неправомерной обработки ПДн.

Уничтожение бумажных носителей ПДн производится с помощью специальных бумагорезательных технических средств (шредеров).

Ответственность за своевременное уничтожение бумажных носителей ПДн возлагается на Пользователей ПДн, а контроль за исполнением этого требования – на Руководителей структурных подразделений.

7.4.7. Централизованное уничтожение бумажных носителей персональных данных

Централизованному уничтожению подлежат массивы бумажных носителей ПДн – архивы, библиотеки и т. п. Централизованное уничтожение осуществляется по решению Комиссии и под ее контролем.

При централизованном уничтожении бумажных носителей ПДн проводится их экспертиза за соответствующий период времени. Цель проведения экспертизы – определить возможность уничтожения носителей либо дальнейшие сроки их хранения. По результатам экспертизы Комиссией составляется список подлежащих уничтожению носителей ПДн.

Уничтожение бумажных носителей ПДн производится с помощью специальных бумагорезательных технических средств (шредеров) или путем сжигания.

К централизованному уничтожению бумажных носителей ПДн могут привлекаться третьи стороны (подрядчики).

После уничтожения носителей ПДн Комиссией составляется Акт об уничтожении носителей ПДн (типовая форма акта приведена в Приложение).

7.5. Контроль использования технологий беспроводного доступа

Мероприятия по защите и контролю беспроводных соединений включают в себя:

– ограничение на использование в информационной системе беспроводных соединений (в частности, 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) информационной системы, для решения которых такие соединения необходимы;

– ограничение на использование технологий беспроводного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администратору ИСПДн или Ответственному за обеспечение безопасности ПДн;

– обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);

– регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

7.6. Управление информационными потоками

Управление информационными потоками должно обеспечивать разрешенный Компанией маршрут прохождения информации между пользователями, устройствами,

сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

7.7. Защита от несанкционированного физического доступа к элементам информационных систем персональных данных

7.7.1. Мероприятия по физическому контролю доступа включают:

- контроль доступа на территорию;
- контроль доступа в помещения с оборудованием ИСПДн;
- контроль доступа к техническим средствам ИСПДн;
- контроль перемещений физических компонентов ИСПДн.

7.7.2. Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории Компании.

7.7.3. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными замками или приспособлениями для опечатывания. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода работников.

7.7.4. Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие работники), должно производиться только в присутствии работников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями ИСПДн.

7.7.5. При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т. п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

7.7.6. Конкретный состав мероприятий для отдельных ИСПДн определяется по результатам разработки модели угроз и нарушителя.

7.8. Резервирование персональных данных

7.8.1. В целях восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, в ИСПДн, в которых (согласно модели угроз) необходимо обеспечить целостность и доступность ПДн, должно проводиться резервное копирование ПДн.

7.8.2. Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

7.8.3. Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

7.8.4. Восстановление информации производится в случае ее частичной или полной утраты путем переноса данных с резервных копий на основные носители в соответствии с эксплуатационной документацией на используемую систему восстановления данных. По завершению восстановления осуществляется проверка работоспособности и целостности данных.

7.8.5. Ответственным за резервирование необходимых массивов ПДн является Ответственный за обеспечение безопасности ПДн.

7.9. Управление уязвимостями

7.9.1. Управление уязвимостями является обязательной составной частью процесса обеспечения безопасности ПДн от несанкционированного доступа.

7.9.2. Результаты управления уязвимостями позволяют объективно оценить уровень защищенности ИСПДн и принять необходимые меры для его приведения в соответствие установленным требованиям.

7.9.3. Мониторинг уязвимостей в Компании производится не реже одного раза в месяц путем сканирования объектов СЗПДн Компании (системного и прикладного ПО серверов, рабочих станций, коммуникационного оборудования).

7.9.4. В ходе сканирования выполняется идентификация сетевых служб, используемых на объекте сканирования (сервер, рабочая станция, коммуникационное оборудование), проверка своевременного обновления системного и прикладного ПО, возможно моделирование несанкционированных действий злоумышленника по получению доступа к обрабатываемым и хранимым на объекте ПДн.

7.9.5. Сканирование объектов СЗПДн Компании проводится Ответственным за обеспечение безопасности ПДн с рабочего места, оборудованного системой обнаружения уязвимостей. Сканирование объектов СЗПДн Компании также может проводиться администраторами ИСПДн, по согласованию с Ответственным за обеспечение безопасности ПДн.

7.9.6. Перед началом проверки Ответственный за обеспечение безопасности ПДн определяет область проверки, производит соответствующие настройки в системе обнаружения уязвимостей и согласовывает время проведения сканирования с администраторами ИСПДн, ответственными за администрирование вошедших в область проверки компонентов СЗПДн Компании.

7.9.7. При проведении сканирования администраторы ИСПДн осуществляют мониторинг работоспособности сканируемых объектов СЗПДн Компании. В случае возникновения сбоев в их работе администраторы ИСПДн незамедлительно ставят в известность Ответственного за обеспечение безопасности ПДн, выполняющего сканирование. При возникновении сбоев, существенно влияющих на выполнение критичных процессов Компании, сканирование немедленно прекращается до устранения причин сбоя.

7.9.8. Для снижения возможного отрицательного воздействия процедуры сканирования на объекты СЗПДн Компании, задействованные в выполнении критичных процессов, сканирование объектов СЗПДн целесообразно проводить в заранее определенные технологические окна, согласованные с администраторами ИСПДн.

7.9.9. По завершении процедуры сканирования Ответственный за обеспечение безопасности ПДн отражает результаты проведенного сканирования в отчете по результатам выявления (поиска) уязвимостей. В отчете должна быть отражена следующая информация:

– число проведенных сканирований в разрезе имеющихся IP-сетей за отчетный период;

– перечень объектов СЗПДн Компании (АРМ, серверы, коммуникационное оборудование), на которых обнаружены уязвимости, связанные с несвоевременным исполнением требований к обновлению системного и прикладного ПО, а также с нарушениями в настройках механизмов безопасности сканируемых объектов;

– описание выявленных уязвимостей;

– рекомендации по устранению обнаруженных уязвимостей (план мероприятий по их устранению).

7.9.10. Подготовленный отчет о сканировании передается администраторам ИСПДн для проведения соответствующих работ по устранению выявленных уязвимостей.

7.9.11. Администраторы ИСПДн устраняет выявленные уязвимости, в том числе путем установки обновлений ПО средств защиты информации, общесистемного и прикладного ПО и микропрограммного обеспечения технических средств.

7.9.12. По итогам устранения выявленных уязвимостей подразделение ИТ информирует Ответственного за обеспечение безопасности ПДн о их результатах.

8. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Типы инцидентов безопасности

8.1.1. К инцидентам безопасности ПДн (далее – Инциденты) относятся:

– нарушение конфиденциальности, целостности или доступности ПДн;

– отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;

– несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);

– заражение программных компонентов ИСПДн вредоносным программным обеспечением.

8.1.2. К Инцидентам также относятся попытки и факты получения НСД к ИСПДн:

– сеансы работы в ИСПДн незарегистрированных пользователей;

– сеансы работы Пользователей ПДн с нарушением установленного времени доступа;

– сеансы работы Пользователей ПДн, срок действия полномочий которых истек, либо в состав полномочий которых не входят выявленные действия с ПДн;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т. п.) без ведома владельца учетной записи;

– совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др.;

– несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки или защиты, входящих в состав ИСПДн.

8.1.3. Кроме того, к Инцидентам относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

8.2. Оповещение об инциденте информационной безопасности

В случае выявления Инцидента устанавливается следующая последовательность действий Пользователей ПДн и их непосредственных руководителей:

1) Прекратить работу с ресурсом, в котором выявлен Инцидент.

2) Оповестить своего непосредственного руководителя о факте выявления инцидента безопасности ПДн.

3) Непосредственный руководитель работника должен оповестить Ответственного за обеспечение безопасности ПДн о факте выявления инцидента безопасности ПДн.

4) После извещения указанного должностного лица по его требованию необходимо предоставить всю необходимую информацию.

Ответственный за обеспечение безопасности ПДн проводит краткий анализ произошедшего Инцидента и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший Инцидент, его последствия и оценка необходимости проведения расследования Инцидента. Справка передается Ответственному за организацию обработки ПДн для принятия решения о необходимости проведении расследования Инцидента. Порядок проведения расследования Инцидента описан в разделе 8.3.

Если по результатам краткого анализа Инцидента установлено, что последствия Инцидента незначительны, то справка может не передаваться Ответственному за организацию обработки ПДн, и разбирательство проводится самостоятельно Ответственным за обеспечение безопасности ПДн. К незначительным последствиям Инцидента относятся следующие случаи:

– последствия для субъектов ПДн незаметны либо мало ощутимы;

– отсутствует измеримый финансовый, репутационный, моральный ущерб для субъектов ПДн;

– репутация субъектов ПДн, его материальное благополучие, жизнь и здоровье не затронуты;

– основные интересы и права субъекта ПДн, закрепленные Конституцией РФ, не затронуты;

– отсутствуют финансовые и (или) репутационные потери для Компании.

8.3. Расследование инцидентов безопасности персональных данных

Целями проведения расследования Инцидента являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования проводится по решению Ответственного за организацию обработки ПДн. С целью проведения расследования в обязательном порядке формируется комиссия по расследованию инцидента, в состав которой также входит Ответственный за обеспечение безопасности ПДн. При необходимости, к работе комиссии привлекаются руководители структурных подразделений, в которых зафиксировано нарушение, и иные должностные лица.

Комиссия по расследованию инцидента должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления Инцидента.

Общая продолжительность внутреннего расследования не должна превышать один месяц.

В рамках проведения расследования инцидента безопасности ПДн комиссия по расследованию инцидента уполномочена:

– проводить опрос работников, по вине которых предположительно произошел Инцидент, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента безопасности ПДн;

– проводить осмотр объектов и предметов, которые могут иметь отношение к Инциденту;

– привлекать (с уведомлением непосредственного руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования.

По решению Ответственного за организацию обработки ПДн на комиссию по расследованию инцидента могут быть возложены дополнительные обязанности и права.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с решением о проведении расследования.

Все действия членов комиссии по расследованию инцидента и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки, отчеты и т. п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами комиссии по расследованию инцидента в виде протокола.

В целях исключения возможности какого-либо воздействия на процесс расследования члены комиссии по расследованию инцидента обязаны соблюдать конфиденциальность расследования до принятия по нему решения руководством Компании.

Одновременно с проведением внутреннего расследования Ответственный за организацию обработки ПДн может поручить комиссии по расследованию инцидента определить ущерб для Компании и (или) для субъекта ПДн от произошедшего инцидента безопасности ПДн. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

По окончании внутреннего расследования комиссия по расследованию инцидента представляет Ответственному за организацию обработки ПДн Отчет по результатам расследования, в котором излагаются:

– основания и время проведения расследования;

– проделанная работа (кратко);

– время, место и обстоятельства факта нарушения;

– причины и условия совершения нарушения;

– виновные лица и степень их вины;

– наличие умысла в действиях виновных лиц;

– предложения по возмещению ущерба;

– предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;

– рекомендации по исключению подобных нарушений;

– другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

К отчету прилагаются:

– письменные объяснения лиц, которых опрашивали члены комиссии по расследованию инцидента;

– акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;

– другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

Отчет должен быть подписан всеми членами комиссии по расследованию инцидента. При несогласии с выводами или содержанием отдельных положений член комиссии по расследованию инцидента, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под подпись с отчетом по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях работника признаков административного правонарушения или уголовного преступления Компании обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

Отчет со всеми прилагаемыми материалами (в т. ч. приказы) подлежит хранению в отдельном деле.

8.4. Мероприятия при наступлении инцидента информационной безопасности, ставшего причиной негативных последствий для субъекта персональных данных

В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов персональных данных, персональные данные этих субъектов необходимо немедленно блокировать. Решение о блокировании персональных данных принимает Ответственный за организацию обработки персональных данных.

Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ и его последствий.

Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Ответственный за организацию обработки персональных данных обеспечивает уничтожение персональных данных в срок, не превышающий десяти рабочих дней.

В случае отсутствия возможности уничтожения персональных данных в течение дести рабочих дней, осуществляется блокирование таких персональных данных и обеспечивается уничтожение персональных данных в срок не более чем шесть месяцев.

9. ВНУТРЕННИЕ КОНТРОЛЬНЫЕ МЕРОПРИЯТИЯ

В целях контроля соответствия процессов обработки ПДн законодательству РФ в области обработки и защиты ПДн, требованиям к защите ПДн, политике Компании в отношении обработки персональных данных и локальным актам Компании проводятся внутренние контрольные мероприятия.

Состав внутренних контрольных мероприятий определяется Комиссией. Контрольные мероприятия включается в План мероприятий по обеспечению безопасности ПДн. Типовой перечень контрольных мероприятий в отдельных подсистемах СЗПДн приведен в к настоящему Положению. Кроме того, в ходе контрольных мероприятий обязательно производятся выборочные проверки работников на предмет знания и соблюдения ими требований локальных актов Компании в сфере ПДн.

Непосредственно перед началом проведения контрольных мероприятий, за 3 рабочих дня Комиссией направляются уведомления Руководителям структурных подразделений, в которых планируется проведение проверки.

По итогам проведения внутренних контрольных мероприятий формируется отчет, включающий в себя описательную часть и таблицу соблюдения установленных правил обеспечения безопасности ПДн (типовая форма отчета приведена в Приложение).

10. КОРРЕКТИРУЮЩИЕ ДЕЙСТВИЯ

Корректирующие действия направлены на устранение выявленных (в результате проведенных контрольных мероприятий или расследований инцидентов) отклонений от правил обработки и обеспечения безопасности ПДн.

На данном этапе необходимо оценить степень критичности выявленных отклонений и провести работы по их устранению.

10.1. Оценка степени критичности выявленных отклонений

При оценке степени критичности каждого выявленного отклонения Комиссия руководствуется следующими критериями:

– отклонение можно исправить в оперативном порядке (например, смена разглашенного пользователем пароля доступа, незначительное изменение правил фильтрации на межсетевом экране и т. п.);

– отклонение невозможно исправить в оперативном порядке и требуется внесение изменений в СЗПДн, компоненты ИСПДн или процессы обработки ПДн.

10.2. Устранение выявленных отклонений

В зависимости от критичности выявленных отклонений Комиссия либо выдает задание на оперативное устранение и назначает ответственных за данную работу, либо работы по устранению отклонений вносятся в План мероприятий по обеспечению безопасности ПДн.

11. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем Положении использованы ссылки на следующие нормативные правовые документы:

11.1. Постановление Правительства Российской Федерации от 01.11.20__2 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

12. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

Таблица 2.

Перечень приложений

№ п/п	Наименование приложения
А	Форма служебной записки на предоставление доступа к ПДн
Б	Форма журнала учета носителей ПДн
В	Акт об уничтожении носителей ПДн
Г	Акт об уничтожении записей с носителей ПДн
Д	Типовой перечень внутренних контрольных проверок в отдельных подсистемах системы защиты персональных данных
Е	Форма отчета по итогам проведения внутренних контрольных мероприятий
Ж	События безопасности, подлежащие регистрации, и сроки их хранения

Приложение А Форма служебной записки на предоставление доступа к ПДн

Служебная записка

Прошу предоставить работнику _____(структурное подразделение, Фамилия И.О.) с целью выполнения трудовых обязанностей доступ к работе к следующим компонентам ИСПДн: _____ (наименование ресурса) с предоставлением следующих полномочий: _____ (чтение, запись, изменение, удаление).

<должность непосредственного руководителя работника> _____

(подпись)

Заявка исполнена

Дополнительная информация:

присвоено сетевое имя:

<должность Ответственного за обеспечение безопасности ПДн>_____

(подпись)

О порядке смены пароля при первом входе в систему работник проинструктирован:

<должность работника> _____

(подпись)

Приложение Б Форма журнала учета носителей ПДн

Журнал начат «____» _____ 20__ __ г. Журнал завершен «____»

_____ 20__ __ г.

Должность Должность

_____ / Ф.И.О. должностного лица / _____ / Ф.И.О.

должностного лица/

На _____ листах

Учетный номер носителя	Дата регистрации	Вид носителя	Наименование или назначение носителя	Количество листов	Фамилия лица, получившего носитель	Подпись за получение и дата	Подпись за возврат и дата	Отметка об уничтожении носителя или переводе его на учет документов выделенного хранения

Приложение В Акт об уничтожении носителей ПДн

УТВЕРЖДАЮ

<должность Ответственного

за обеспечение безопасности ПДн>

_____

(Ф.И.О., подпись)

Настоящим актом подтверждается уничтожение носителя персональных данных №_____(учетный номер носителя), _____ (дата), закрепленного за _____ (должность, Ф И.О. сотрудника) путем _____ (разрезание, сжигание, механическое уничтожение).

Председатель комиссии _____

(подпись)

Член комиссии _____

(подпись)

Приложение Г Акт об уничтожении записей с носителей ПДн

УТВЕРЖДАЮ

<должность Ответственного

за обеспечение безопасности ПДн>

_____

(Ф.И.О., подпись)

Настоящим актом подтверждается уничтожение (стирание) записей с носителя персональных данных №_____(учетный номер носителя), _____ (дата), закрепленного за _____ (должность, Ф И.О. сотрудника) программным средством _____ (наименование программного средства).

Председатель комиссии _____

(подпись)

Член комиссии _____

(подпись)

Приложение А Приложение Д. Типовой перечень внутренних контрольных проверок в отдельных подсистемах системы защиты персональных данных

Таблица 3. Типовой перечень внутренних контрольных проверок

№ п/п	Контрольные проверки и объекты проверок
1	***Подсистема управления доступом***
1.1	соответствие установленных прав доступа (в прикладных системах, базах данных и т. п.) полномочиям в рамках трудовых обязанностей работника
1.2	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
1.3	процесс идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам ИСПДн)
1.4	механизмы блокирования доступа средствами защиты от НСД при выполнении устанавливаемого числа неудачных попыток ввода пароля
1.5	система смены пароля принудительным образом (по истечению срока действия пароля)
1.6	выполнение требований по стойкости пароля к попыткам компрометации
2	***Подсистема регистрации и учета***
2.1	наличие в системных журналах зарегистрированных попыток НСД (в т. ч. имитация попыток НСД к системе)
2.2	соответствие настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации
2.3	способы защиты системного журнала регистрации от уничтожения или модификации нарушителем
2.4	места хранения носителей ПДн, сейфы и металлические шкафы, надежность их замков
2.5	выполнение установленного порядка учета и хранения носителей ПДн
2.6	фактическое наличие всех носителей ПДн, в том числе учетных журналов, дел, документов (поступивших, изданных, переведенных на выделенное хранение)
2.7	фактическое наличие всех носителей ПДн, переданных на архивное хранение
2.8	номенклатура дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение
2.9	правильность проставления регистрационных данных носителей, документов, дел и учетных журналов
2.10	правильность проставления в журнале учета носителей ПДн отметок о движении носителей
3	***Подсистема обеспечения целостности***
3.1	механизмы контроля целостности пакетов обновлений программного обеспечения СЗИ с использованием контрольных сумм
3.2	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
3.3	целостность используемого ПО, путем вычисления контрольных сумм
3.4	наличие экземпляров резервных копий ПДн, предусмотренных в соответствии с локальными актами
3.5	целостность созданных резервных копий ПДн путем восстановления данных

№ п/п	Контрольные проверки и объекты проверок
3.6	функционирование процедур резервного копирования и восстановления (имитация в специально отведенной тестовой зоне выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы)
4	***Подсистема антивирусной защиты***
4.1	наличие установленных программных средств антивирусной защиты на рабочих станциях и серверах
4.2	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
4.3	процесс своевременного обновления программных средств антивирусной защиты (в т. ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях
4.4	процесс полного сканирования системы в режиме реального времени антивирусным средством
4.5	процесс автоматической проверки антивирусным средством используемых отчуждаемых носителей
4.6	процесс принудительной проверки используемых отчуждаемых носителей
4.7	процессы защиты от заражения вредоносным ПО (имитация в специально отведенной изолированной тестовой зоне попыток заражения вредоносным ПО серверных и рабочих станций)
4.8	наличие зафиксированных случаев заражения вредоносным ПО в системных журналах и отчетах
5	***Подсистема обеспечения безопасного межсетевого взаимодействия***
5.1	соответствие установленных межсетевых экранов уровню защищенности не ниже, чем это регламентировано руководящими документами ФСТЭК России
5.2	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
5.3	функционирование системы сегментации сети (имитация в специально отведенной тестовой зоне или в нерабочее время попыток проникновения в «закрытый» сегмент сети из «открытого», в том числе с применением специального ПО)
5.4	наличие зафиксированных попыток обращения к «закрытым» ресурсам в системных журналах
6	***Подсистема анализа защищенности***
6.1	выполнение своевременного обновления ПО, используемого для анализа защищенности, в т. ч. баз данных уязвимостей
6.2	соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации
6.3	наличие зафиксированных попыток НСД (имитация попыток преодоления системы защиты в специально отведенной тестовой зоне или в нерабочее время) в системных журналах
7	***Подсистема обнаружения и предотвращения вторжений***
7.1	настройки системы обнаружения и предотвращения вторжений в соответствии с эксплуатационной и технической документацией к ней
7.2	информация о срабатывании сигналов тревоги
7.3	ложные срабатывания системы
7.4	соблюдение условий использования системы обнаружения и предотвращения вторжений, предусмотренных эксплуатационной и технической документацией

№ п/п	Контрольные проверки и объекты проверок
8	***Подсистема защиты от утечек по техническим каналам***
8.1	установленные на окнах жалюзи, шторы и т. п. в помещениях, где ведется обработка ПДн
8.2	размещение дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т. п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей ПДн
9	***Контрольные проверки в подсистеме физической защиты***
9.1	электронные журналы СКУД на предмет попыток НСД в защищаемые помещения лиц, не имеющих права доступа в данные помещения
9.2	наличие ключей (в том числе и электронных пропусков) от защищаемых помещений, а также проверка сохранности вторых экземпляров ключей от защищаемых помещений
9.3	заявления об утерянных ключах (в том числе и электронных пропусках), по которым можно получить доступ в защищаемые помещения, а так же принятых мер (блокирование электронного пропуска, смена замка)
9.4	надежность замков, установленных в защищаемых помещениях
10	***Подсистема криптографической защиты***
10.1	соответствие настроек и условий эксплуатации СКЗИ требованиям, указанным в эксплуатационной документации
10.2	сохранность эксплуатационной и технической документации и ключевых документов на СКЗИ
10.3	журналы учета СКЗИ, эксплуатационная и техническая документации к ним, а также используемые криптографические ключи на правильность их учета и хранения
10.4	функционирование СКЗИ путем имитации процессов шифрования и дешифрования информации

Приложение А Приложение Е. Форма отчета по итогам проведения внутренних контрольных мероприятий и пример его заполнения

Таблица 4. Отчет по итогам проведения внутренних контрольных мероприятий

№ п/п	Дата проведения мероприятия	Проверка	Заключение о степени выполнения установленных правил	Степень выполнения
1	_____	Соответствие установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей Пользователей ПДн	Установленные правила доступа соответствуют полномочиям в рамках трудовых обязанностей Пользователей ПДн	*Выполняется полностью*
2	_____	Соответствие настроек и условий эксплуатации СЗИ требованиям, указанным в эксплуатационной документации к ним	Нарушены условия эксплуатации SecretDisk (копирование ключа шифрования на незащищенный носитель)	*Выявлено нарушение*
3	_____	Система регистрации попыток НСД должна регистрировать попытки НСД в системном журнале	По результатам имитации НСД к серверу 1С. Бухгалтерия система регистрации НСД не зарегистрировала данные попытки в системном журнале в связи с отсутствием соответствующего функционала	*Выявлены отклонения от установленных правил*

Приложение Б Приложение Ж. События безопасности, подлежащие регистрации, и сроки их хранения

Таблица 5. События безопасности, подлежащие регистрации, и сроки их хранения

№ п/п	Наименование события безопасности	Состав и содержание информации о событии безопасности	Срок хранения
Общие требования к регистрации событий безопасности			
1	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	• дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) операционной системы; • идентификатор субъекта доступа, предъявленный при попытке доступа; • результат попытки входа (успешный, неуспешный); • результат попытки загрузки (останова) операционной системы (успешный, неуспешный)	180 дней
2	Подключение машинных носителей информации и вывод информации на носители информации	• дата и время подключения машинных носителей информации и вывода информации на носители информации; • логическое имя (номер) подключаемого машинного носителя информации; • идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации	180 дней
3	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	• дата и время запуска; • имя (идентификатор) программы (процесса, задания); • идентификатор субъекта доступа, запросившего программу (процесс, задание); • результат запуска (успешный, неуспешный)	180 дней
4	Попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа	• дата и время попытки доступа к защищаемому объекту; • идентификатор субъекта доступа; • спецификация защищаемого объекта (логическое имя, тип); • результат попытки доступа (успешный, неуспешный)	180 дней
5	Попытки удаленного доступа	• дата и время попытки удаленного доступа; • идентификатор субъекта доступа, используемый протокол доступа; • используемый интерфейс доступа; • результат попытки удаленного доступа (успешная, неуспешная)	180 дней
Дополнительные требования к регистрации событий безопасности в виртуальной инфраструктуре			
6	Запуск (завершение) работы компонентов виртуальной инфраструктуры	• дата и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах; • идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры; • езультат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешный, неуспешный)	180 дней
7	Доступ субъектов доступа к компонентам виртуальной инфраструктуры	• дата и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе; р • идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры; • результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешный, неуспешный)	180 дней
8	Изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения	• дата и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании;	180 дней

№ п/п	Наименование события безопасности	Состав и содержание информации о событии безопасности	Срок хранения
		• идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры; • результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешный, неуспешный)	
9	Изменения правил разграничения доступа к компонентам виртуальной инфраструктуры	• дата и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе; • идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры; • результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешный, неуспешный)	180 дней