РАСПОРЯЖЕНИЕ
УПРАВЛЕНИЕ ИМУЩЕСТВЕННЫХ И ЗЕМЕЛЬНЫХ ОТНОШЕНИЙ АДМИНИСТРАЦИИ БУДЕННОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

03 октября 2023 г. г. Буденновск № 428 р-од

Об утверждении Политики организации и проведения работ по обеспечению безопасности персональных данных в управлении имущественных и земельных отношений администрации Буденновского муниципального округа Ставропольского края

В соответствии со статьей 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в целях организации и проведения работ по обеспечению безопасности персональных данных

1. Утвердить прилагаемую Политику организации и проведения работ по обеспечению безопасности персональных данных в управлении имущественных и земельных отношений администрации Буденновского муниципального округа Ставропольского края.

2. Признать утратившим силу распоряжение управления имущественных и земельных отношений администрации Буденновского муниципального округа Ставропольского края от 01.03.2021 № 112 р-од «Об утверждении Политики управления имущественных и земельных отношений администрации Буденновского муниципального округа Ставропольского края в отношении обработки персональных данных».

3. Контроль за выполнением настоящего распоряжения оставляю за собой.

Начальник управления Ю.Г. Маркарова

УТВЕРЖДЕНА
распоряжением управления
2 имущественных и земельных
отношений администрации
Буденновского муниципального
округа Ставропольского края
от 03 октября 2023 г. № 428 р-од

ПОЛИТИКА
организации и проведения работ по обеспечению безопасности персональных данных

Общие положения

1.1. Настоящий документ (далее – Политика) определяет порядок организации и проведения работ по обеспечению безопасности персональных данных и содержит общие принципы защиты персональных данных (далее – ПДн) в управлении имущественных и земельных отношений администрации Буденновского муниципального округа (далее – Управление).

1.2. Данный документ направлен на достижение следующих целей:

- выполнение требований нормативных документов Российской Федерации, связанных с ПДн;
- защиты прав и свобод граждан Российской Федерации при обработке их ПДн;
- защиты ПДн, обрабатываемых в Управлении, от несанкционированного доступа и от других несанкционированных действий;
- снижение уровня регуляторных рисков в отношении Управления.

1.3. Минимальная периодичность пересмотра Политики – 1 год, максимальная – 3 года.

1.4. Требования настоящей Политики распространяются на все отделы Управления. Настоящий документ обязаны знать и использовать в работе все сотрудники Управления.

1.5. В соответствии с Федеральным законом Российской Федерации от 27 июля 2006г. № 152-ФЗ «О персональных данных» Управление обязано обеспечить защиту обрабатываемых ПДн.

1.6. Настоящая Политика устанавливает требования по защите ПДн в информационных системах ПДн направленные на защиту интересов субъектов ПДн и Управления в области ее непосредственной деятельности.

1.7. Настоящая Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн;
- принятия управленческих решений и разработки практических мер по воплощению и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение вероятности реализации угроз безопасности ПДн;
- координации деятельности отделов Управления при проведении работ по созданию, развитию и эксплуатации информационных систем ПДн с соблюдением требований по обеспечению безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в информационных системах ПДн.

1.8. Предотвращение несанкционированного и нелегитимного доступа к информационным системам, технологиям и информационным ресурсам результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения

комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств защиты информации.

1.9. ПДн являются частью информации ограниченного доступа, не составляющей государственную тайну, обрабатываемой в Управлении.

1.10.Во всех случаях, не урегулированных настоящей Политикой, необходимо руководствоваться действующим законодательством Российской Федерации.

1. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Целью создания системы защиты ПДн является исключение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

2.2. В соответствии с требованиями нормативных документов, для защиты ПДн необходимо обеспечить: конфиденциальность, целостность, доступность, неотказуемость, учетность, аутентичность и адекватность данных.

2.3. Конкретный состав целей защиты ПДн зависит от конкретной информационной системы ПДн и определяется по результатам разработки (актуализации) модели угроз и нарушителя безопасности ПДн.

2.4. К основным задачам в области обеспечения безопасности ПДн относится:

- определение новых информационных систем ПДн;
- инвентаризация и управление изменениями в составе и структуре существующих информационных систем ПДн;
- разработка и актуализация перечня ПДн обрабатываемых в информационных системах ПДн;
- оптимизация информационных и бизнес-процессов обработки ПДн;
- категорирование ПДн;
- определение уровня защищенности информационных систем ПДн;
- разработка (актуализация) модели угроз безопасности ПДн и модели нарушителя;
- разработка (актуализация) нормативной документации на систему защиты ПДн;
- разработка (актуализация) описания системы защиты ПДн;
- выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
- проверка готовности средств защиты к использованию;
- ввод средств защиты в эксплуатацию;
- обеспечение применения для защиты ПДн сертифицированных средств защиты информации;
- эксплуатация системы защиты ПДн в соответствии с документацией на нее;
- контроль уровня защищенности ПДн;
- обучение персонала по вопросам защиты ПДн;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;
- уничтожение ПДн при выводе носителей из эксплуатации;
- обеспечение защищенного документооборота носителей с ПДн;
- учет лиц, допущенных к обработке ПДн;

- учет лиц, доступ к ПДн, обрабатываемым в информационных системах ПДн, необходим для выполнения служебных (трудовых) обязанностей;
- учет лиц, допущенных к работе со средствами криптографической защиты информации;
- определение ответственного пользователя криптосредств;
- определение мест хранения ПДн;
- резервирование ПДн;
- взаимодействие с регулирующими органами по вопросам защиты ПДн;
- актуализация и подача уведомлений в Уполномоченный орган по защите прав субъектов ПДн;
- реагирование на нештатные ситуации, расследование нештатных ситуаций, возникающих при обработке ПДн;
- выполнение лицензионных требований ФСТЭК и ФСБ России в области защиты ПДн;
- контроль лояльности администраторов информационных систем ПДн.

2. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ РЕСУРСОВ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Работы по обеспечению безопасности ПДн при их обработке на ресурсах обработки ПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла ресурсов.

3.2. Работы по обеспечению безопасности ПДн привязаны к жизненному циклу активов, а именно к следующим этапам:

- инициация проекта;
- реализация проекта, в составе:
    - выбор технического решения – концепция реализации;
    - проектирование;
    - производство;
    - передача системы в опытно-промышленную эксплуатацию;
    - опытная эксплуатация.
- эксплуатация;
- модернизация;
- вывод из эксплуатации.

3.3. Работы по защите ПДн с привязкой к этапам жизненного цикла и ответственные за эти работы:

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
1.	**Инициация проекта**			
1.1.	Определение активов как обрабатывающих ПДн	При создании активов или существенном изменении существующих активов определяется необходимость обработки ПДн в них. Если такая необходимость имеется, то активы объявляются как обрабатывающие ПДн	Автоматизированная Неавтоматизированная	Владелец актива
1.2.	Сбор и предоставление данных об активах	Состав собираемых данных, порядок и формы сбора, адресаты определены в разделе 12	Автоматизированная Неавтоматизированная	См. раздел 12
1.3.	Определение предварительной категории ПДн, предполагаемых к обработке на активах	Детализация проводимых работ приведена в разделе 4	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
1.4.	Определение предварительного класса активов информационных систем ПДн	На данном этапе определяется возможный класс данных активов при их классификации как отдельной информационной системы ПДн. Результаты классификации используются при оценке возможности отнесения актива к какой-либо информационной системе ПДн. Детализация проводимых работ приведена в разделе 4	Автоматизированная	Ответственный за обеспечение безопасности ПДн
1.5.	Правовая оценка возможности создания активов	На данном этапе дается правовая оценка возможности создания активов с учетом: – нормативных оснований для обработки состава ПДн предполагаемого к обработке на активе; – нормативных ограничений на допустимые цели и способы обработки и т.п.	Автоматизированная Неавтоматизированная	Ответственный за юридический анализ

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
1.6.	Организационно-техническая оценка возможности создания активов	Организационно-техническая оценка возможности создания активов должна предусматривать: – возможность встраивания системы защиты актива в общую инфраструктуру системы защиты ПДн Учреждения; – необходимые мероприятия по защите ПДн обрабатываемых на актива (переработка нормативных документов, внедрение средств защиты и т.п.); – финансовые затраты необходимые на обеспечение построения системы защиты ПДн актива.	Автоматизированная	Ответственный за обеспечение безопасности ПДн, ответственный за информационные технологии
2.	**Реализация проекта – определение информационных систем ПДн**			
2.1.	Определение информационных систем ПДн к которым принадлежат активы	На данном этапе посредством анализа состава обрабатываемых ПДн, целей обработки ПДн определяется информационная система ПДн, к которой возможно присоединение актива. При отсутствии информационной системы ПДн, к которой допустимо присоединение актива инициируется создание новой информационной системы ПДн.	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
2.2.	Определение класса и уровня защищенности информационной системы ПДн	В случае необходимости создания новой информационной системы ПДн производится выполнение работ приведенных в разделе 4	Автоматизированная	Комиссия по информационной безопасности

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
2.3.	Определение необходимости создания системы защиты ПДн	На данном этапе на основе класса и уровня защищенности информационных систем ПДн, данные о составе ПДн, определяется необходимость создания системы защиты ПДн. Создание системы защиты ПДн не требуется в случае отсутствия ущерба субъекту ПДн по всем свойствам ПДн	Автоматизированная	Ответственный за обеспечение безопасности ПДн
2.4.	Оценивается возможность оптимизации информационных систем ПДн	Детализация проводимых работ приведена в разделе 5	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
2.5.	Определение перечня актуальных угроз безопасности ПДн	Детализация проводимых работ приведена в разделе 6	Автоматизированная	Ответственный за обеспечение безопасности ПДн
3.	**Реализация проекта – выбор технического решения**			
3.1.	Оптимизация архитектуры активов по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн	Детализация выполняемых работ представлена в разделе 5	Автоматизированная	Ответственный за обеспечение безопасности ПДн, владелец актива

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
3.2.	Выбор средств реализации требований к системе защиты ПДн	Выбор средств реализации требований к системе защиты ПДн производится в соответствии с действующими нормативными требованиями и составом актуальных угроз, в том числе рассматривается применение средств: – межсетевого экранирования; – антивирусной защиты; – аутентификации; – контроля доступа; – обнаружения вторжений; – криптографической защиты; – анализа защищенности.	Автоматизированная	Ответственный за обеспечение безопасности ПДн, ответственный за информационные технологии
3.3.	Анализ необходимости изменения документации на информационные системы ПДн в целом, в связи с появление новых активов	На данном этапе производится анализ документации на информационные системы ПДн в целом (модели угроз, описания системы защиты, нормативных документов и т.п.) на предмет соответствия текущей ситуации с учетом появления нового актива. При необходимости инициируются работы по модернизации информационной системы ПДн	Автоматизированная	Ответственный за обеспечение безопасности ПДн
4.	**Реализация проекта – проектирование и поставка средств защиты**			
4.1.	Разработка спецификации на поставку средств защиты	На данном этапе осуществляется разработка детальной спецификации необходимых средств защиты ПДн	Автоматизированный	Ответственный за обеспечение безопасности ПДн
4.2.	Поставка средств защиты	На данном шаге осуществляется поставка выбранных средств защиты ПДн	Автоматизированный	Ответственный за обеспечение безопасности ПДн

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
4.3.	Разработка описания системы защиты ПДн	На данном этапе разрабатывается проект (раздел проекта) на систему защиты ПДн актива(ов). Описание разрабатывается в случае, если текущее описание не учитывает систему защиты активов	Автоматизированная	Ответственный за обеспечение безопасности ПДн
4.4.	Разработка эксплуатационной документации на систему защиты ПДн	Производится разработка (адаптация имеющихся) нормативных документов определяющих порядок защиты ПДн (при необходимости)	Автоматизированный Неавтоматизированный	Ответственные в рамках своей области ответственности
5.	**Реализация проекта – производство**			
5.1.	Проводятся работы по сертификации (подтверждению сертификата) применяемых средств и механизмов защиты ПДн	Согласно описанию СЗПДн проводятся работы по сертификации средств и механизмов защиты на соответствие требуемым функциям и классам средств защиты.	Автоматизированная	Ответственный за обеспечение безопасности ПДн
5.2.	Внедрение комплекса средств и мер защиты ПДн	Производятся монтажные, пуско-наладочные работы средств защиты информации указанных в проекте. Производится реализация комплекса организационно-технических мероприятий по защите ПДн.	Автоматизированная	Ответственный за обеспечение безопасности ПДн, ответственный за информационные технологии
5.3.	Реализация требований по физической защите активов	Производятся монтажные работы средств физической защиты (замков, шкафов, сейфов и т.п.). Детализация проводимых работ приведена в разделе 14	Автоматизированная Неавтоматизированная	Ответственный за физическую безопасность

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
5.4.	Проводится обучение сотрудников по направлению обеспечения безопасности ПДн	На данном этапе определяется наличие пользователей и администраторов ресурса, которые ранее не работали с ПДн. При их наличии проводится обучение. Детализация проводимых работ приведена в разделе 8	Автоматизированная Неавтоматизированная	Руководители структурных подразделений участвующих в процессах обработки и защиты ПДн, ответственный за обеспечение безопасности ПДн
5.5.	Проводится ознакомление сотрудников с нормативными документами в области защиты ПДн	На данном этапе определяется наличие сотрудников, которые не ознакомлены с требованиями к процессам обработки и защиты ПДн. При наличии таких сотрудников производится их ознакомление с нормативными документами	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
5.6.	Проводится проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации	Проверка готовности производится посредством анализа выполнения всех требований к системе защиты предусмотренных: – описанием системы защиты ПДн, – условиями эксплуатации средств защиты. Результатов проверки является заключение, форма которого представлена в Приложении 2.	Автоматизированная	Ответственный за информационные технологии, ответственный пользователь криптосредств, администраторы информационной безопасности в своих областях ответственности

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
5.7.	Производится учет средств защиты информации, эксплуатационной документации к ним используемых для защиты ресурсов	Учет средств криптографической защиты информации, документации, ключевых носителей, действий, выполняемых со средствами криптографической защиты информации, осуществляется в журнале, форма которого должна быть приведена в соответствующей инструкции. Учет других средств защиты осуществляется в соответствии с формой Приложения 3.	Автоматизированная	Ответственный за информационные технологии, ответственный пользователь криптосредств, администраторы информационной безопасности в своих областях ответственности
5.8.	Производится ввод средств защиты в эксплуатацию	На данном этапе, на основе результатов проверки готовности средств защиты информации к использованию готовится приказ на ввод средств в эксплуатацию. Форма приказа представлена в Приложении 4.	Автоматизированная	Ответственный за информационные технологии, ответственный пользователь криптосредств, администраторы информационной безопасности в своих областях ответственности
5.9.	Определение мест хранения ПДн	На данном шаге приказом оформляется перечень помещений, в которых разрешена обработка ПДн, категории ПДн, которые обрабатываются в данных помещениях. Форма приказа представлена в Приложении 5.	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
5.10.	Ввод информационных систем ПДн в эксплуатацию	Ввод информационных систем ПДн в эксплуатацию осуществляется по приказу (форма Приложения 12)	Автоматизированная	Ответственный за обеспечение безопасности ПДн

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
6.	**Эксплуатация**			
6.1.	Допуск персонала к обработке ПДн	Детализация проводимых работ приведена в разделе 10	Автоматизированная Неавтоматизированная	Руководители структурных подразделений участвующих в процессах обработки ПДн
6.2.	Учет лиц, допускаемых к работе с ПДн	Детализация проводимых работ приведена в разделе 10	Автоматизированная Неавтоматизированная	Руководители структурных подразделений участвующих в процессах обработки ПДн
6.3.	Пользователи допускаются к работе со средствами криптографической защиты информации	При появлении пользователей, которым требуется работать со средствами криптографической защиты информации, производится допуск их к работе на основании приказа. Порядок допуска пользователей должен быть регламентирован в соответствующей инструкции	Автоматизированная	Ответственный пользователь криптосредств
6.4.	Учет носителей ПДн	В процессе эксплуатации производится учет съемных и несъемных носителей используемых для хранения ПДн. Детализация проводимых работ приведена в разделе 12	Автоматизированная Неавтоматизированная	Руководители структурных подразделений участвующих в процессах обработки ПДн, владельцы активов

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
6.5.	Учет ключевых носителей	Ключевые носители, используемые в целях криптографической защиты ПДн, подлежат обязательному учету и контролю. Порядок выдачи, учета, обращения ключевых носителей, а также форма журнала учета представлены в соответствующей инструкции	Автоматизированная	Ответственный пользователь криптосредств
6.6.	Учет ключей от спецпомещений органа криптографической защиты	Учет ключей от спецпомещений, выдача ключей производится с обязательной записью в журнале учета. Порядок учета должен быть регламентирован в соответствующей инструкции	Автоматизированная	Ответственный пользователь криптосредств
6.7.	Осуществляется, при необходимости, передача средств криптографической защиты информации между пользователями	Передача средств криптографической защиты информации между пользователями осуществляется на основании внесения соответствующих пометок в журнал. Форма журнала, порядок его ведения должен быть регламентирован в соответствующей инструкции	Автоматизированная	Ответственный пользователь криптосредств
6.8.	Осуществляется отслеживание изменений в составе и структуре активов	Детализация проводимых работ приведена в разделе 12. При определении изменений выполняются работы по модернизации активов в соответствии с требованиями этапа 7 настоящей таблицы	Автоматизированная Неавтоматизированная	Владелец актива, ответственный за информационные технологии, руководители структурных подразделений, участвующих в процессах обработки ПДн

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
6.9.	Обеспечивается защита от несанкционированного физического доступа к элементам активов	Детализация проводимых работ приведена в разделе 14	Автоматизированная Неавтоматизированная	Ответственный за физическую безопасность
6.10.	Осуществляется эксплуатация подсистемы антивирусной защиты	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Ответственный за информационные технологии
6.11.	Осуществляется эксплуатация подсистемы межсетевого экранирования	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Ответственный за информационные технологии
6.12.	Осуществляется эксплуатация подсистемы аутентификации и защиты от несанкционированного доступа	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Ответственный за информационные технологии
6.13.	Осуществляется эксплуатация подсистемы обнаружения вторжений	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Администраторы информационной безопасности

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
6.14.	Осуществляется эксплуатация подсистемы криптографической защиты	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Ответственный пользователь криптосредств
6.15.	Осуществляется эксплуатация подсистемы анализа защищенности	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Администраторы информационной безопасности
6.16.	Осуществляется эксплуатация подсистемы контроля утечки	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Администраторы информационной безопасности
6.17.	Выполняются условия использования средств защиты информации	Эксплуатация сертифицированных средств защиты информации производится с выполнением обязательных условий эксплуатации предусмотренных в документации на эти средства.	Автоматизированная	Администраторы информационной безопасности, ответственный пользователь криптосредств, ответственный за информационные технологии в своих областях ответственности

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
6.18.	Осуществляется отслеживание необходимости повторной сертификации (иной оценки соответствия) средств защиты, проведение работ по повторной сертификации	В рамках данной задачи производится периодический анализ имеющихся сертификатов на средств защиты. В случае приближения срока завершения действия сертификата (за 1 год) инициируется проведение работ по повторной сертификации (оценке соответствия)	Автоматизированная	Ответственный за обеспечение безопасности ПДн
6.19.	Осуществляется контроль за обеспечением необходимого уровня защищенности ПДн	Детализация проводимых работ приведена в разделе 16	Автоматизированная	Ответственный за обеспечение безопасности ПДн
6.20.	Производится реагирование на нештатные ситуации	Детализация проводимых работ приведена в разделе 17	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
6.21.	Производится контроль лояльности персонала	Детализация проводимых работ приведена в разделе 18	Автоматизированная	Ответственный за обеспечение безопасности ПДн
6.22.	Проводится обучение персонала правилам обеспечения безопасности ПДн	Данная задача заключается в обучении новых пользователей по мере их появления. Детализация проводимых работ приведена в разделе 8	Автоматизированная	Ответственный за обеспечение безопасности ПДн, руководители структурных подразделений участвующих в процессах обработки и защиты ПДн

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
6.23.	Проводится ознакомление сотрудников с нормативными документами в области защиты ПДн	Данная задача заключается в ознакомлении новых пользователей ресурса с корпоративными нормативными документами по мере их появления.	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
6.24.	Опечатывание или опломбирование криптосредств	Производится оборудование средствами контроля за вскрытием (печатями, пломбами) аппаратных средств, с которыми осуществляется штатное функционирование криптосредств, а также аппаратных и аппаратно-программных криптосредств	Автоматизированная	Владелец актива, пользователи криптосредств
6.25.	Осуществляется резервирование ПДн	Детализация проводимых работ приведена в разделе 15	Автоматизированный	Ответственный за ИТ
6.26.	Осуществляется взаимодействие с регуляторными органами по вопросам защиты ПДн		Автоматизированный Неавтоматизированный	Ответственный за обеспечение безопасности ПДн
7.	**Модернизация**			
7.1.	По планируемым изменениям производится сбор и предоставление данных об активах	Состав собираемых данных, порядок и формы сбора, адресаты определены в разделе 12	Автоматизированная Неавтоматизированная	Владелец актива

№ п/п	Этап, последователь-ность работ по защите ПДн	Детализация проводимых работ по защите ПДн, ссылки на разделы, в которых детализирован состав работ	На какие виды обработки распространяется	Ответственный исполнитель
7.2.	Производится оценка существенности предполагаемой модернизации активов	Проводится анализ: – возможности изменения класса и уровня защищенности информационных систем ПДн, актуальных угроз, требований к системе защиты ПДн вследствие изменения ресурса; – необходимости корректировки документации на систему защиты ПДн; – необходимости проведения дополнительных мероприятий по защите ПДн; – возможности изменения принадлежности ресурса к информационным системам ПДн	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
7.3.	Инициируются работы по модернизации	В случае необходимости корректировок инициируется выполнение необходимого работ указанных в этапах 1-6 данной таблицы	Автоматизированная Неавтоматизированная	Владелец актива
8.	**Вывод из эксплуатации**			
8.1.	Производится передача ПДн в архив	В процессе вывода актива из эксплуатации производится передача ПДн в архив (при необходимости)	Автоматизированная Неавтоматизированная	Владелец актива
8.2.	Производится уничтожение ПДн обрабатываемых на активах	Детализация проводимых работ приведена в разделе 11	Автоматизированная	Владелец актива (при наличии технической возможности), ответственный за информационные технологии
8.3.	Актив выводится из эксплуатации	Вывод ресурса из эксплуатации осуществляется на основании приказа	Автоматизированная	Владелец актива

3. КАТЕГОРИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Категорирование ПДн и определение уровня защищенности информационных систем ПДн должно проводиться для информационных систем с автоматизированной обработкой ПДн.

4.2. Определение уровня защищенности информационных систем ПДн и категорирование ПДн проводятся в соответствии с Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.3. Процесс категорирования ПДн и определения уровня защищённости информационных систем ПДн является основой для определения требований к уровню защиты ПДн.

4.4. Классификация информационных систем ПДн и определение уровня защищенности информационных систем ПДн проводятся путем:

- приведения исходных характеристик, влияющих на уровень защищенности информационных систем и категорию ПДн;
- указания предположений, влияющих на категорию ПДн и определение уровня защищенности информационных систем ПДн;
- логического обоснования предполагаемых категорий ПДн и уровня защищенности информационных систем ПДн.

4.5. Выводы об уровне защищенности той или иной информационной системы ПДн и категории ПДн приводятся в «Акте определения уровня защищенности информационных систем персональных данных». Форма акта приведена в Приложении 6.

4.6. Оценка необходимости пересмотра уровня защищенности информационных систем ПДн должна осуществляться каждый раз, когда изменились характеристики, учитываемые при утверждении уровня защищенности информационных систем ПДн.

4. ОЦЕНКА ВОЗМОЖНОСТИ ОПТИМИЗАЦИИ РЕСУРСОВ И ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оценка возможности оптимизации активов и информационных систем ПДн имеет своей целью такую реструктуризацию, выполнение требований по защите ПДн, в которых может быть обеспечено с минимальным уровнем затрат на создание и эксплуатацию системы защиты ПДн.

5.2. При проведении оптимизации должна оцениваться возможность:

- исключения обработки ПДн;
- снижения категории обрабатываемых ПДн;
- обезличивания ПДн;
- придания ПДн статуса общедоступных;
- изменения структуры и состава технических и программных средств информационной системы ПДн, технологических процессов обработки ПДн.

5.2.1. Снижение категории ПДн, в общем случае, позволяет снизить уровень защищенности информационных систем ПДн и, соответственно, уровень требований к защите.

5.2.2. Обезличивание ПДн и отнесение ПДн к общедоступным – это эффективный способ обеспечения их безопасности, так как для обезличенных и общедоступных ПДн не требуется обеспечение их конфиденциальности. Отсутствие необходимости защиты конфиденциальности ПДн не снимает необходимости защиты других характеристик безопасности (целостности, доступности и т.п.).

Среди мероприятий по обезличиванию ПДн, можно выделить следующие:

- разделение ПДн, позволяющих идентифицировать субъекта ПДн, и остальной информации по разным активам, базам или массивам данных;
- удаление ПДн, позволяющих идентифицировать субъекта ПДн, в технологических процессах, в которых не требуется однозначного определения физического лица.

5.2.3. Придание ПДн статуса общедоступных возможно в следующих случаях:

- при наличии федерального закона, определяющего, что этот состав ПДн является общедоступным;
- при наличии возможности сбора согласий на общедоступность их ПДн с субъектов ПДн.

5.2.4. Изменение структуры и состава технических и программных средств ресурсов и информационных систем ПДн, технологических процессов обработки ПДн может проводиться, в том числе, с целью:

- уменьшения количества компонентов информационных систем ПДн, на которые потребуется установка средств защиты;
- изменения возможности, степени опасности угроз для ИСПДн и, соответственно, уменьшения перечня актуальных угроз;

- изменения требований к характеристикам средств защиты информации, в результате которого возможно использование более оптимальных по стоимости средств и т.п.

5.3. Результаты оценки оформляются в виде соответствующего отчета, включающего, как минимум:

- варианты оптимизации;
- технический анализ вариантов оптимизации;
- стоимостной анализ вариантов оптимизации;
- выводы об оптимальном варианте оптимизации.

5. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Система защиты ПДн внедряется для нейтрализации актуальных угроз безопасности ПДн.

6.2. Оценка актуальности угроз производится посредством разработки «Модели угроз безопасности персональных данных и модели нарушителя» (далее – «Модель угроз безопасности ПДн»).

6.3. «Модель угроз безопасности ПДн» может быть разработана на несколько информационных систем ПДн сразу или на какую-либо конкретную информационную систему ПДн.

6.4. Методической базой для разработки «Модели угроз безопасности ПДн» является:

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 года;
- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 года;
- методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432.

6.5. Результатом разработки «Модели угроз безопасности ПДн» должен являться:

- перечень актуальных угроз;
- вывод об уровне защищенности информационных систем ПДн;
- вывод о типе нарушителя, существующем в информационных системах ПДн и требуемом классе средств криптографической защиты информации.

6.6. «Модель угроз безопасности ПДн» должна содержать:

- описание структуры и состава информационных систем ПДн (состав обрабатываемых ПДн, состав технических средств и программного обеспечения, существующие процессы обработки ПДн и т.п.);
- обоснование характеристик безопасности ПДн (конфиденциальность, целостность, доступность и т.п.), нарушение которых ведет к ущербу для субъектов ПДн;
- модель угроз (перечень угроз, оценку вероятностей угроз, показатели опасности угроз для конкретной информационной системы ПДн, оценки возможностей реализации угроз, выводы об актуальности угроз);
- модель нарушителя (объекты атак, возможные типы нарушителей, предположения о возможностях нарушителей, предположения об

ограничениях на эти возможности, предположения о каналах атак и средствах атак, выводы о типе нарушителя).

6.7. «Модель угроз безопасности ПДн» должна пересматриваться каждый раз, когда изменяются характеристики, влияющие на актуальность угроз, класс и уровень защищенности информационных систем ПДн, тип нарушителя.

6. РАЗРАБОТКА ОПИСАНИЯ НА СИСТЕМУ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Описание на систему защиты ПДн должно включать:

- пояснительную записку, описывающую состав и структуру комплекса технических средств защиты;
- схему комплекса технических средств.

7.2. Допустимо делать описание на систему защиты в виде эскизного (технического) проекта.

7.2.1. Эскизный проект (описание) на систему защиты ПДн в части применения средств криптографической защиты информации, в том числе, должен включать:

- индексы, условные наименования и регистрационные номера используемых криптосредств;
- подтверждение соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;
- подтверждение соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, требованиям к ним, с описанием основных средств защиты;
- подтверждение выполнения требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем ПДн (при их наличии).

7. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Должно проводиться обучение всех сотрудников, участвующих в процессах защиты ПДн.

8.2. Контроль прохождения обучения, отправка сотрудников, участвующих в процессах обработки и защиты ПДн на обучение, осуществляется начальником Управления. В общем случае, для различных категорий сотрудников форматы обучения должны отличаться.

8.3. Определены следующие форматы обучения:

- полные курсы (длительностью 5 дней и более);
- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи;
- учения (по необходимости).

8.4. Полные и кратковременные курсы, конференции, внешние семинары проводятся по необходимости во внешних специализированных организациях для сотрудников, выполняющих роли:

- ответственного за организацию обработки ПДн;
- ответственного за обеспечение безопасности ПДн;
- ответственного за физическую безопасность;
- ответственного за информационные технологии;
- ответственного пользователя криптосредств;
- администраторов информационной безопасности.

8.5. Для начальников отделов, участвующих в процессах обработки и защиты ПДн могут проводиться кратковременные курсы во внешних специализированных организациях.

8.6. Для обучения остальных категорий персонала, участвующих в процессах обработки ПДн, проводятся:

- кратковременные инструктажи при первичном допуске к работе с ПДн;
- внутренние семинары (не обязательно).

8.7. При проведении кратковременных инструктажей должны быть освещены следующие вопросы:

- состав корпоративных нормативных документов, регулирующих вопросы защиты ПДн, основные положения этих документов;
- основные требования в части защиты ПДн к работе сотрудников;
- ответственность за нарушение требований по защите ПДн.

8.8. Внутренние семинары, инструктажи проводятся ответственным за обеспечение безопасности ПДн, приглашенными специалистами, а также другими подготовленными лицами.

8.9. Учения проводятся для закрепления практических навыков реагирования на возникающие угрозы и могут проводиться как для отделов Управления, так и для Управления в целом.

8.10. Рекомендуется, чтобы инструкторы учебных групп в первый год, а в дальнейшем не реже 1 раза в 3 года проходили подготовку в специализированных учебно-методических центрах по вопросам защиты ПДн.

8.11. Начальник Управления обязан оказывать организационную, техническую и методическую помощь инструкторам учебных групп и осуществлять постоянный контроль за подготовкой и проведением занятий.

8.12. Факт проведения инструктажа должен фиксироваться в журнале учета, форма Приложения 7.

8. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ И ОТВЕТСТВЕННЫХ ПОЛЬЗОВАТЕЛЕЙ КРИПТОСРЕДСТВ

9.1. Подразделение или лицо, на которое возложены функции ответственного пользователя криптосредств выполняет следующие функции:

- заводит и ведет на каждого пользователя криптосредств лицевой счет, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы;
- получает неиспользованные или выведенные из действия ключевые документы или дают указание на их уничтожение на месте;
- осуществляют текущий контроль за организацией и обеспечением функционирования криптосредств;
- хранит ключевые документы, эксплуатационную и техническую документацию, инсталлирующие носители криптосредств;
- санкционирует передачу криптосредств между пользователями;
- выполняет другие функции, предусмотренные требованиями ФСБ России к эксплуатации средств криптографической защиты информации.

9.2. Пользователи криптосредств выполняют следующие функции:

- уведомляют ответственного пользователя криптосредств об уничтожении ключевых документов (телефонограммой, устным сообщением по телефону и т.п.) для списания уничтоженных документов с их лицевых счетов;
- сообщают о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно уведомляют оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых ПДн;
- сдают криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;
- уведомляют ответственного пользователя криптосредств о нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием ПДн.

9.3. Конкретные процедуры управления средствами криптографической защиты информации должны быть регламентированы в соответствующей инструкции.

9. ДОПУСК ПЕРСОНАЛА К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Доступ к ПДн предоставляется только лицам, указанным в «Списке лиц, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных в Управлении, необходим для выполнения служебных (трудовых) обязанностей» (далее – Список лиц).

10.2. Включение в «Список лиц» конкретных сотрудников осуществляется на основании приказа. Форма приказа на включение в «Список лиц» представлена в Приложении 8.

10.3. Перечни составляются и ведутся начальниками отделов, на основании данных о лицах, допущенных к ПДн.

Перечень может вестись в электронном виде.

10.4. Доступ лиц к конкретным ПДн осуществляется на основании соответствующих заявок. Форма, порядок подачи и согласования которых должны быть регламентированы в соответствующей инструкции.

10. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1.При выводе ресурсов, информационных систем ПДн из эксплуатации, со всех носителей содержащих ПДн и не предназначенных для архивного хранения должна быть проведена операция гарантированного уничтожения ПД.

11.2.Уничтожение ПДн осуществляют администраторы информационной безопасности.

11.3.Факт уничтожения ПДн должен подтверждаться соответствующей записью.

11.4.Конкретные процедуры уничтожения должны быть регламентированы в соответствующей инструкции.

11. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ И СТРУКТУРЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕСУРСОВ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1.Все изменения в составе и структуре информационных системах ПДн и активов обрабатывающих ПДн должны контролироваться.

12.2.К активам, которые влияют на требования в области ПДн, в том числе, относятся:

- сотрудники, контрагенты, участвующие в обработке ПДн;
- сотрудники, контрагенты задействованные в процессах поддержки и обеспечения безопасности информационных систем;
- автоматизированные информационные массивы (базы данных, файлы и файловые каталоги);
- неавтоматизированные информационные массивы (бумажные документы, журналы и т.п.);
- технические средства (АРМ, серверы, сетевое и телекоммуникационное оборудование);
- виртуальные сервера;
- программное обеспечение;
- каналы связи;
- помещения, в которых осуществляется обработка ПДн и т.п.

12.3.Изменения контролируются в целях:

- актуализации документации на существующую систему защиты ПДн;
- разработки новых документов на систему защиты ПДн;
- сопровождения, изменения конфигурации существующих средств и мер защиты ПДн;
- внедрения новых средств и мер защиты.

12.4.В указанных целях производится сбор и предоставление информации:

12.4.1. Владельцами активов ответственному за обеспечение безопасности ПДн, о следующих изменениях:

- вводе и выводе из эксплуатации активов, модернизации активов,
- изменении состава обрабатываемых ПДн, изменение категории (клиенты, сотрудники, посетители и т.п.) лиц, данные которых обрабатываются,
- изменении целей обработки ПДн;
- изменении объема обрабатываемых ПДн по сравнению с объемом, указанным в акте определения уровня защищенности информационных систем ПДн;
- изменении владельца актива;
- изменении состава третьих сторон, других операторов ПДн, которым ПДн передаются или от которых получаются;
- изменении состава ПДн предоставляемых пользователям, третьим лицам, другим операторам ПДн;

- изменении объема ПДн предоставляемых третьим лицам, другим операторам ПДн;
- изменении состава стран, в которые осуществляется передача ПДн (расхождения с данными, указанными в акте определения уровня защищенности информационных систем ПДн);
- внесении новых ключевых устройств в состав обрабатывающих ПДн (серверов, систем хранения, сетевого и телекоммуникационного оборудования), замена и удаление таких устройств;
- изменении состава потоков ПДн (состава ПДн и категорий лиц данные которых передаются) к другим ресурсам обработки ПДн;
- изменении процессов обработки ПДн на активах (состава используемых ПДн, способов обработки ПДн, целей и оснований для обработки);
- появлении новых потоков ПДн к другим активам;
- изменении состава офисов, в которых используются активы;
- изменении логических и физических сегментов, в которых расположены компоненты ресурсов;
- изменении состава системного и прикладного программного обеспечения, участвующего в обработке ПДн;
- изменении режима разграничения прав доступа (разные или равные права) пользователей к обрабатываемым ПДн (наличие расхождение с актом определения уровня защищенности информационных систем ПДн);
- изменении состава помещений, в которых осуществляется неавтоматизированная обработка ПДн;
- изменении состава администраторов ресурсов обработки ПДн;
- изменении состава неавтоматизированных активов, используемых для обработки ПДн.

12.4.2. Ответственному за информационные технологии, ответственному за обеспечение безопасности ПДн, о следующих изменениях:

- внесении новых ключевых устройств в состав обрабатывающих ПДн (серверов, систем хранения, сетевого и телекоммуникационного оборудования), замена и удаление таких устройств;
- изменении состава потоков ПДн (состава ПДн и категорий лиц, данные которых передаются) к другим ресурсам обработки ПДн;
- появлении новых потоков ПДн к другим активам;
- изменении состава системного и прикладного программного обеспечения, участвующего в обработке ПДн;
- изменении состава помещений, в которых размещаются ключевые компоненты информационной системы ПДн (сервера, системы хранения, сетевое и телекоммуникационное оборудование);
- прокладке новых кабельных линий связи, которые будут проходить за пределами контролируемой зоны и внешних линий связи или удалении старых кабельных линий связи, проходящих за пределами контролируемой зоны, которые используются для передачи ПДн.

12.4.3. Руководителями структурных подразделений, участвующих в процессах обработки ПДн, ответственному за обеспечение безопасности ПДн, о следующих изменениях:

- внесении новых пользователей в состав информационных систем ПДн, исключении сотрудников из числа пользователей этих систем;
- изменении процессов обработки ПДн (состава используемых ПДн, способов обработки ПДн, целей и оснований для обработки);
- изменении состава помещений, в которых установлены автоматизированные рабочие места информационных систем ПДн.

12.5. Каждое определенное выше изменение должно анализироваться на предмет соответствия требованиям по защите ПДн. При необходимости должна производиться модернизация системы защиты ПДн.

12.6. Для сбора указанных данных должны использоваться формы сбора данных представленные в Приложении 9. В случае использования системы автоматизации выполнения требований в области ПДн, указанные данные должны вноситься непосредственно в данную систему.

12. ОРГАНИЗАЦИЯ РАБОТЫ С НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Учет носителей ПДн осуществляется в том случае, если такая необходимость определена требованиями к информационным системам ПДн соответствующего уровня защищенности.

13.2. Работы по организации работы с носителями включают:

- работы по обеспечению конфиденциального официального документооборота;
- работы по обеспечению конфиденциального обращения других носителей, содержащих ПДн.

13.3. Порядок организации официального документооборота, связанного с ПДн в Управлении, соответствует единому порядку организации конфиденциального делопроизводства.

13.4. Работы по обеспечению конфиденциального обращения других носителей, содержащих ПДн включают:

- учет носителей;
- обращение с носителями;
- хранение носителей;
- подготовка носителей данные для передачи их в архив.

13.5. Учет, обращение, хранение, подготовка носителей, содержащих ПДн производится в структурных подразделениях, участвующих в процессах обработки ПДн.

13.6. Организацию учета, хранения и т.п. носителей содержащих ПДн осуществляют руководители данных структурных подразделений и владельцы активов.

13.7. Обеспечение конфиденциального обращения других носителей, содержащих ПДн, производится с соблюдением следующих требований:

- руководители структурных подразделений и владельцы активов заводят «Журнал учета носителей персональных данных» (далее – Журнал ПДн). Журнал учета ведется в электронном виде (форма Приложения 10);
- Журнал ПДн должен иметь актуальную резервную копию на случай повреждения носителя, где он хранится;
- Журнал ПДн предоставляется руководителями структурных подразделений и владельцами активов по запросу ответственного за обеспечение безопасности ПДн;
- учет используемых несъемных носителей ПДн автоматизированного рабочего места (жестких дисков) и съемных носителей (CD/DVD диски, Flash накопители, дискеты и т.п.), на которых обрабатываются ПДн, осуществляется руководителями структурных подразделений;
- учет несъемных носителей ПДн серверов и хранилищ осуществляется владельцами этих активов.

13. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К КОМПОНЕНТАМ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Мероприятия по защите от несанкционированного физического доступа к компонентам информационных систем ПДн включают:

- мероприятия по защите от несанкционированного физического доступа на территорию, на которой находятся компоненты информационных систем ПДн;
- мероприятия по защите от несанкционированного физического доступа в помещения с компонентами информационных систем ПДн;
- мероприятия по защите от несанкционированного физического доступа в спецпомещения;
- мероприятия по защите от несанкционированного физического доступа к кабельным коммуникациям, участвующим в процессах обработки ПДн;
- мероприятия по защите от несанкционированного физического доступа к носителям ПДн;
- мероприятия по контролю перемещений физических компонентов информационных систем ПДн.

14.2. Конкретный состав мероприятий и требований по контролю физического доступа в помещения, порядок их реализации, ответственные должны быть определены в соответствующей инструкции.

14.3. В помещениях, в которых осуществляется обработка ПДн, должен быть принят следующий комплекс мер защиты:

- установка надежных запираемых дверей на входе в помещения,
- установка приспособлений для опечатывания помещений, либо установка системы охранной сигнализации.

14.3.1. В случае если помещение находится на первом этаже здания, либо окна помещения легкодоступны для лиц, не допущенных к обработке ПДн:

- на окнах должны быть установлены решетки,
- либо установлена система охранной сигнализации,
- либо организована круглосуточная охрана.

14.4. В помещениях, в которых осуществляется неавтоматизированная обработка ПДн и в которых возможно неконтролируемое пребывание лиц, не допущенных ко всем обрабатываемым ПДн, дополнительно, должны быть установлены запираемые металлические шкафы и/или сейфы для хранения носителей ПДн.

14.5. Носители ПДн, в случае возможности неконтролируемого пребывания лиц, не допущенных ко всем обрабатываемым ПДн, должны помещаться в запираемые металлические шкафы и/или сейфы.

14. РЕЗЕРВИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. Резервирование ПДн должно обеспечить возможность восстановления ПДн обрабатываемых в информационных системах ПДн при нарушении целостности основных хранилищ данных.

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

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

15.4. Конкретные процедуры резервирования должны быть регламентированы в соответствующей инструкции.

15. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

16.1. Для повышения эффективности процесса защиты ПДн проводится:

- контроль за соблюдением требований по обработке и защите ПДн;
- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- контроль эффективности средств защиты ПДн.

16.2. Для контроля эффективности системы защиты ПДн должны использоваться средства выявления уязвимостей.

16.3. При проведении контроля эффективности в общем случае должно проверяться:

- наличие установленных средств защиты информации;
- корректность настроек средств защиты информации;
- выполнение пользователями информационных систем ПДн и администраторами активов требований корпоративных нормативных документов по защите ПДн;
- соответствие системы защиты ПДн требованиям, предъявляемым к ней.

16.4. Выявленные несоответствия процессов защиты ПДн обязательны к устранению.

16.5. Конкретные процедуры контроля должны быть разработаны в соответствующей инструкции.

16. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

17.1. Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Управлении должны быть регламентированы следующие вопросы:

- порядок определения нештатной ситуации;
- порядок оповещения сотрудников при возникновении различных нештатных ситуаций;
- порядок действий по нейтрализации нештатных ситуаций, сведения их негативных последствий к минимуму.

17.2. В Управлении должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

17.3. В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью ПДн;
- ликвидация последствий инцидентов, связанных с безопасностью ПДн;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

17.4. Конкретные процедуры управления нештатными ситуациями должны быть разработаны в соответствующей инструкции.

17. КОНТРОЛЬ ЛОЯЛЬНОСТИ ПЕРСОНАЛА

18.1. В Управлении должен проводиться комплекс мероприятий, направленных на исключение присутствия злоумышленника, а также возможность сговора двух и более злоумышленников.

18.2. Комплекс мероприятий должен включать, в том числе:

18.2.1. проверки пользователей при первоначальном допуске к ПДн, в том числе:

- изучение личного дела сотрудника;
- проверка правильности данных, указанных в документах, предоставляемых сотрудником при приеме на работу;
- детальное тестирование квалификации сотрудников, с использованием тестов;
- проверка отсутствия судимостей у сотрудника;

18.2.2. проверки администраторов активов при назначении на соответствующую должность, в том числе:

- изучение личного дела сотрудника;
- проверка правильности данных, указанных в документах, предоставляемых сотрудником при приеме на работу;
- получение (проверка) отзывов о работе данного сотрудника на предыдущих местах работы;
- проверка личных и профессиональных характеристик, посредством общения с руководителями с прошлых мест работы (по возможности);
- детальное тестирование квалификации сотрудников, с использованием тестов;
- проверка отсутствия судимостей у сотрудника;

18.2.3. периодический мониторинг действий пользователей и администраторов (для администраторов не реже 1 раза в 2 года), в том числе:

- проверки выполняемых действий и обрабатываемой информации на автоматизированных рабочих местах;
- проверки содержания отправляемых сообщений (службы мгновенных сообщений, электронной почты);
- проведение личного собеседования с сотрудником и с руководителем его структурного подразделения.

18.3. Для администраторов желательны проверки на лояльность на детекторе лжи (полиграфе).

18.4. Проверки могут выполняться как в скрытом, так и в явном режиме.

18.5. Факт и результаты проведения проверки администраторов ресурса фиксируются в заключении о проверке (форма Приложения 11). Наличие отрицательных результатов по каким-либо проведенным проверкам должны являться основанием для отстранения от выполнения функций администратора.

18. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

19.1. Лица, виновные в нарушении требований по обработке персональных данных несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

19.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн сотрудника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой ответственности в порядке, установленном федеральными законами.

19.3. В случае выявления нарушения порядка обработки ПДн, должно проводиться служебное расследование в соответствии с инструкцией.

19.4. При выявлении в ходе служебного расследования нарушителей к ним могут применяться меры дисциплинарного воздействия.

19. ИСТОРИЯ ВЕРСИЙ ДОКУМЕНТА

№ п/п	Дата создания версии	Должность ответственного за разработку	ФИО ответственного за разработку	Краткое описание изменений документа
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				