Ибрагимова Маргарита Дерениковна

Подписано цифровой подписью: Ибрагимова Маргарита Дерениковна
Дата: 2025.02.13 14:51:56 +03'00'

УТВЕРЖДАЮ

Директора МБОУ ДО ЦРТДЮ

_____М.Д. Ибрагимова

30.12.2021

ПОЛИТИКА
организации и проведения работ по обеспечению безопасности персональных данных

г. Краснодар
2021

Содержание

1. 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 муниципальном бюджетном образовательном учреждении дополнительного образования муниципального образования город Краснодар «Центр развития творчества детей и юношества» (далее – МБОУ ДО ЦРТДЮ).

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 МБОУ ДО ЦРТДЮ, от несанкционированного доступа и от других несанкционированных действий.

1.3. Настоящий документ обязаны знать и использовать в работе все сотрудники МБОУ ДО ЦРТДЮ, участвующие в организации и проведении работ по обеспечению безопасности ПДн.

1.4. В соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» МБОУ ДО ЦРТДЮ обязана обеспечить защиту обрабатываемых ПДн.

1.5. 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;
- создания, развития 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.

1.6. 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.

1.7. ПДн являются частью информации ограниченного доступа, не составляющей государственную тайну, обрабатываемой в МБОУ ДО ЦРТДЮ.

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

2. 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 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 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 сотрудников 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;
- 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;
- контроль лояльности администраторов информационной безопасности.

3. Порядок организации и проведения работ по обеспечению безопасности персональных данных

3.1. Работы по обеспечению безопасности ПДн при их обработке на вычислительных ресурсах обработки ПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла информационного ресурса МБОУ ДО ЦРТДЮ.

3.2. Работы по обеспечению безопасности ПДн привязаны к жизненному циклу информационного ресурса, 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 следующий:

№ 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.	Сбор и предоставление данных	Состав собираемых данных, порядок и формы сбора, адресаты определены в разделе 11	Автоматизированная Неавтоматизированная	См. раздел 11
1.2.	Определение предварительной категории обрабатываемых ПДн и предварительного уровня защищенности информационных систем ПДн	На данном этапе определяется категория и уровень защищенности отдельной информационной системы ПДн. Детализация проводимых работ приведена в разделе 4	Автоматизированная	Ответственный за организацию обработки ПДн
1.3.	Правовая оценка	На данном этапе дается правовая оценка возможности обработки ПДн с учетом: – нормативных оснований для обработки состава ПДн предполагаемого к обработке; – нормативных ограничений на допустимые цели и способы обработки и т.п.	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
1.4.	Организационно-техническая оценка	Организационно-техническая оценка должна предусматривать: – возможность встраивания системы защиты информационной системы ПДн в общую инфраструктуру системы защиты ПДн МБОУ ДО ЦРТДЮ; – необходимые мероприятия по защите ПДн обрабатываемых в информационной системе (переработка нормативных документов, внедрение средств защиты и т.п.); – финансовые затраты необходимые на	Автоматизированная	Ответственный за обеспечение безопасности ПДн Администратор 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
		обеспечение построения системы защиты ПДн.		
2.	**Реализация проекта – определение информационных систем ПДн**			
2.1.	Определение информационных систем ПДн	На данном этапе посредством анализа состава обрабатываемых ПДн, целей обработки ПДн определяется информационная система ПДн.	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
2.2.	Определение 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
2.3.	Определение необходимости создания системы защиты ПДн	На данном этапе на основе 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 организацию обработки ПДн Ответственный за обеспечение безопасности ПДн
2.4.	Оценивается возможность оптимизации информационных систем ПДн	Детализация проводимых работ приведена в разделе 5	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн Ответственный за обеспечение безопасности ПДн Администратор информационной безопасности
2.5.	Определение перечня актуальных угроз безопасности ПДн	Детализация проводимых работ приведена в разделе 6	Автоматизированная	Ответственный за организацию обработки ПДн Ответственный за

№ 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
				обеспечение безопасности ПДн Администратор информационной безопасности
3.	**Реализация проекта – выбор технического решения**			
3.1.	Оптимизация архитектуры 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
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	Автоматизированная	Ответственный за организацию обработки ПДн Администратор информационной безопасности
3.3.	Анализ необходимости изменения документации на информационные системы ПДн в целом, в связи с появление новых информационных систем	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 новой информационной системы. При необходимости инициируются работы по модернизации информационной системы ПДн	Автоматизированная	Ответственный за организацию 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
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
4.3.	Разработка описания системы защиты ПДн	На данном этапе разрабатывается проект (раздел проекта) на систему защиты ПДн. Описание разрабатывается в случае, если текущее описание не учитывает систему защиты ПДн	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	Ответственный за обеспечение безопасности ПДн
5.	**Реализация проекта – производство**			
5.1.	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 Администратор информационной безопасности
5.2.	Реализация требований по физической защите	Производятся монтажные работы средств физической защиты (замков, шкафов, сейфов и т.п.). Детализация проводимых работ приведена в разделе 13	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн 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
5.3.	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	Ответственный за организацию обработки ПДн
5.4.	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 организацию обработки ПДн
5.5.	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 обеспечение безопасности ПДн Администратор информационной безопасности
5.6.	Производится учет средств защиты информации, эксплуатационной документации к ним используемых для защиты ресурсов	Учет средств защиты осуществляется в соответствии с формой Приложения 3.	Автоматизированная	Ответственный за обеспечение безопасности ПДн Администратор информационной безопасности
5.7.	Производится ввод средств защиты в эксплуатацию	На данном этапе, на основе результатов проверки готовности средств защиты информации к использованию готовится приказ	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
		на ввод средств в эксплуатацию. Форма приказа представлена в Приложении 4.		Администратор информационной безопасности
5.8.	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 организацию обработки ПДн Ответственный за обеспечение безопасности ПДн
5.9.	Ввод информационных систем ПДн в эксплуатацию	Ввод информационных систем ПДн в эксплуатацию осуществляется по приказу (форма Приложения 6)	Автоматизированная	Ответственный за организацию обработки ПДн
6.	**Эксплуатация**			
6.1.	Допуск персонала к обработке ПДн	Детализация проводимых работ приведена в разделе 9	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
6.2.	Учет лиц, допускаемых к работе с ПДн	Детализация проводимых работ приведена в разделе 9	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
6.3.	Учет носителей ПДн	В процессе эксплуатации производится учет съемных и несъемных носителей используемых для хранения ПДн. Детализация проводимых работ приведена в разделе 11	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
6.4.	Осуществляется отслеживание изменений в составе и структуре информационной	Детализация проводимых работ приведена в разделе 11	Автоматизированная	Ответственный за организацию 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
	системы			
6.5.	Обеспечивается защита от несанкционированного физического доступа к носителям ПДн	Детализация проводимых работ приведена в разделе 13	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
6.6.	Осуществляется эксплуатация подсистем защиты	Эксплуатация подсистемы осуществляется в соответствии с проектной и эксплуатационной документацией.	Автоматизированная	Администратор информационной безопасности
6.7.	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
6.8.	Осуществляется контроль за обеспечением необходимого уровня защищенности ПДн	Детализация проводимых работ приведена в разделе 15	Автоматизированная	Ответственный за организацию обработки ПДн
6.9.	Производится реагирование на нештатные ситуации	Детализация проводимых работ приведена в разделе 16	Автоматизированная Неавтоматизированная	Ответственный за обеспечение безопасности ПДн
6.10.	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 организацию обработки ПДн Ответственный за обеспечение безопасности ПДн
6.11.	Проводится ознакомление	Данная задача заключается в ознакомлении новых пользователей ресурса с корпоративными	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки

№ 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
	сотрудников с нормативными документами в области защиты ПДн	нормативными документами по мере их появления.		ПДн Ответственный за обеспечение безопасности ПДн
6.12.	Осуществляется резервирование ПДн	Детализация проводимых работ приведена в разделе 14	Автоматизированный	Администратор информационной безопасности
6.13.	Осуществляется взаимодействие с регуляторными органами по вопросам защиты ПДн	Производится взаимодействие с регуляторами по вопросам защиты ПДн в случае проверок или запросов со стороны регулирующих органов	Автоматизированный Неавтоматизированный	Ответственный за организацию обработки ПДн
7.	**Модернизация**			
7.1.	По планируемым изменениям производится сбор и предоставление данных	Состав собираемых данных, порядок и формы сбора, адресаты определены в разделе 11	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
7.2.	Производится оценка существенности предполагаемой модернизации информационных систем	Проводится анализ: – возможности изменения 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 организацию обработки ПДн 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
7.3.	Инициируются работы по модернизации	В случае необходимости корректировок инициируется выполнение необходимого работ указанных в этапах 1-6 данной таблицы	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн Ответственный за обеспечение безопасности ПДн
8.	**Вывод из эксплуатации**			
8.1.	Производится передача ПДн в архив	В процессе вывода носителя ПДн из эксплуатации производится передача ПДн в архив (при необходимости)	Автоматизированная Неавтоматизированная	Ответственный за организацию обработки ПДн
8.2.	Производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 10	Автоматизированная	Ответственный за организацию обработки ПДн

4. 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 7.

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.

5. Оценка возможности оптимизации ресурсов и информационных систем персональных данных

5.1. Оценка возможности оптимизации 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;
- 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. 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.

5.2.3. 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.

6. 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;
- банк данных угроз безопасности информации ФСТЭК России, приведенного на сайте http://www.bdu.fstec.ru/.

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.

7. Разработка описания на систему защиты персональных данных

7.1. Описание на систему защиты ПДн должно включать:

- ведомость проекта;
- пояснительную записку, описывающую состав и структуру комплекса технических средств защиты;
- схему комплекса технических средств;
- ведомость покупных изделий.

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

8. 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 на обучение осуществляется ответственным за организацию обработки ПДн.

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.

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;
- администраторов информационной безопасности.

8.5. 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.

8.6. Внутренние семинары, инструктажи проводятся ответственным за организацию обработки ПДн, приглашенными специалистами, а также другими подготовленными лицами.

8.7. Учения проводятся для закрепления практических навыков реагирования на возникающие угрозы и могут проводиться как для отдельных сотрудников МБОУ ДО ЦРТДЮ, так и для МБОУ ДО ЦРТДЮ в целом.

8.8. 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.

8.9. Факт проведения инструктажа должен фиксироваться в журнале учета, форма Приложения 8.

9. Допуск персонала к обработке персональных данных

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

9.2. Включение в «Список лиц» конкретных сотрудников осуществляется на основании приказа. Форма приказа на включение в «Список лиц» представлена в Приложении 9.

9.3. Перечни составляются и ведутся ответственным за организацию обработки ПДн, на основании данных о лицах, допущенных к ПДн.

Перечень может вестись в электронном виде.

9.4. 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

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

10.2. Уничтожение ПДн осуществляет комиссией по информационной безопасности, а стирание ПДн с электронных носителей (в том числе съёмных) – администратором информационной безопасности.

10.3. Факт уничтожения ПДн должен подтверждаться соответствующей записью.

10.4. 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

11.1. Все изменения в составе и структуре информационных системах ПДн должны контролироваться.

11.2. К сведениям, которые влияют на требования в области защиты 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, сетевое и телекоммуникационное оборудование);
- программное обеспечение;
- каналы связи;
- помещения, в которых осуществляется обработка ПДн и т.п.

11.3. 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.

11.4. В указанных целях производится сбор и предоставление информации:

11.4.1. Ответственному за организацию обработки ПДн о следующих изменениях:

- вводе и выводе из эксплуатации информационных систем, модернизации информационных систем, обрабатывающие ПДн;
- изменении состава обрабатываемых ПДн, изменение категории (клиенты, сотрудники 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 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;
- внесении новых ключевых устройств в состав обрабатывающих ПДн (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 (состава используемых ПДн, способов обработки ПДн, целей и оснований для обработки);

- появлении новых потоков ПДн к другим информационным системам;
- 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 носителей ПДн, используемых для обработки ПДн.

11.4.2. 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 (появления новых) потоков ПДн (состава ПДн и категорий лиц, данные которых передаются) к другим ресурсам обработки ПДн;
- изменении в составе системного и прикладного программного обеспечения, участвующего в обработке ПДн;
- изменении состава помещений, в которых размещаются ключевые компоненты информационных систем (сервера, системы хранения, сетевое и телекоммуникационное оборудование).

11.4.3. Администратору информационной безопасности 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.

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

12. Организация работы с носителями персональных данных

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

12.2. Работы по организации работы с носителями включают:

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

12.3. Порядок организации официального документооборота, связанного с ПДн в МБОУ ДО ЦРТДЮ соответствует единому порядку организации конфиденциального делопроизводства.

12.4. 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.

12.5. Учет, обращение, хранение, подготовка носителей, содержащих ПДн производится ответственным за организацию обработки ПДн.

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

- ответственный за организацию обработки ПДн заводит «Журнал учета носителей персональных данных» (далее – Журнал ПДн). Журнал ПДн может вестись в электронном виде (форма Приложения 10);
- 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 ответственным за организацию обработки ПДн.

13. Защита от несанкционированного физического доступа к компонентам информационных систем персональных данных

13.1. 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 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.

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

13.3. В помещениях, в которых осуществляется обработка ПДн, должен быть установлены надежно запираемые двери.

13.4. 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 шкафы и/или сейфы для хранения носителей ПДн.

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

14. Резервирование персональных данных

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

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

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

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

15. Контроль за обеспечением необходимого уровня защищенности персональных данных

15.1. 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.

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

15.3. 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 требований корпоративных нормативных документов по защите ПДн;
- соответствие системы защиты ПДн требованиям, предъявляемым к ней.

15.4. Выявленные несоответствия процессов защиты ПДн обязательны к устранению.

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

16. Реагирование на нештатные ситуации

16.1. Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн в МБОУ ДО ЦРТДЮ, 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.

16.2. В МБОУ ДО ЦРТДЮ должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

16.3. 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.

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

17. Ответственность за нарушение норм, регулирующих обработку персональных данных

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

17.2. 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.

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

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