УТВЕРЖДАЮ

Генеральный директор
ООО «Легион-ннформ»

_____М.А. Шарипов

УТВЕРЖДАЮ

Директор МАОУ СОШ № 31

_____Е.В. Иванова

ДСП
Экз.№ 1

ЧАСТНОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На защиту информационной системы персональных данных
(СЗ ИСПДн)

Содержание

Обозначения и сокращения

В настоящем документе используются следующие обозначения и их сокращения:

АС	Автоматизированная система
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОИ	Объект информатизации
ПАК	Программно-аппаратный комплекс
ПДн	Персональные данные
ПО	Программное обеспечение
РД	Руководящие документы
СПД	Сети передачи данных
СЗ ПДн	Система защиты персональных данных
СЗИ и ЗКСПД	Система защиты информации и защищенной корпоративной сети передачи данных
СЗИ	Средства защиты информации
СКЗИ	Система криптографической защиты информации
СОВ	Система обнаружения вторжений
СПО	Специальное программное обеспечение
СУБД	Система управления базой данных
ТЗ	Техническое задание
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЧТЗ	Частное техническое задание

1. Общие сведения

СЗИ и ЗКСПД создается в соответствии с требованиями обеспечения безопасности информации с использованием программных и программно-аппаратных средств. Работы производятся в муниципальном автономном общеобразовательном учреждении города Калининграда средней общеобразовательной школы № 31 (далее – МАОУ СОШ № 31) самостоятельно и из собственных финансовых источников.

1.1. Перечень документов, являющихся основанием для работ по созданию СЗИ и ЗКСПД

Все мероприятия по созданию СЗИ и ЗКСПД осуществляются в соответствии с требованиями и рекомендациями следующих документов:

- Федеральный закон от 27 августа 2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
- Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Постановление Правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю России от 18.02.2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности»;
- «Методических рекомендаций по разработке нормативно правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утверждены руководством 8 Центра ФСБ России (№149/7/6-432 от 31.03.2015);
- Приказа ФСБ России от 9 февраля 2005 года № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службы по техническому и экспортному контролю России 15.02.2008г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службы по техническому и экспортному контролю России 14.02.2008г.).

1.2. Порядок оформления результатов создания СЗИ и ЗКСПД

Техническая документация разрабатывается на русском языке.

2. Этапы и перечень работ

Работы по созданию СЗИ и ЗКСПД для МАОУ СОШ № 31 (далее по тексту - Объект), выполняются в соответствии со следующими этапами.

2.1. Первый этап - проводится обследование объектов и анализ исходных данных, необходимых для создания СЗИ и ЗКСПД.

2.2. Второй этап - защита каналов передачи данных и создание системы защиты информации (установка и настройка оборудования и выполнение пуско-наладочных работ).

Второй этап включает в себя следующие виды работ:

2.2.1. Разработка пакета документации, предусмотренной руководящими и нормативно-методическими документами в сфере защиты информации, в том числе и защиты персональных данных. Должна быть выполнена разработка пакета документов, регламентирующих обработку конфиденциальной информации. Пакет документов должен включать следующие категории документов:

- общие документы;
- организационные документы;
- проекты приказов;
- инструкции и положения;
- журналы учета;
- документы по политике информационной безопасности;
- эксплуатационная документация на созданную систему защиты.

2.2.2. Разработка модели (ей) угроз безопасности для информационных систем.

2.2.3. Разработка частного технического задания на систему защиты информации.

2.2.4. Разработка рекомендаций по применению средств защиты информации для информационных систем МАОУ СОШ № 31.

2.2.5. Установка технических средств. Объект на которые устанавливаются средства определяются по мере приобретения средств.

2.2.6. Проведение пуско-наладочных работ технических средств, необходимых для создания системы защиты информации и защищенной корпоративной сети передачи данных.

2.2.7. Проведение опытной эксплуатации СЗИ и ЗКСПД в целях проверки реализации возможности передачи данных между объектами.

2.3. Третий этап - проведение приемо-сдаточных испытаний технических средств по результатам опытной эксплуатации. Проведение сдачи-приемки работ по созданию СЗИ и ЗКСПД.

Третий этап включает в себя следующие виды работ:

2.3.1. Проведение оценки соответствия ИС требованиям безопасности информации, включая следующие мероприятия:

- комплексная проверка ИС на соответствие требованиям по защите передаваемой информации;
- подготовка отчетной документации - заключение по результатам испытаний и декларирование соответствия требованиям безопасности информации.

2.3.2. Ввод в действие системы защиты по требованиям безопасности.

3. Характеристика объектов информатизации

3.1. Центральный узел управления СЗИ и ЗКСПД располагается по адресу: 236040, г. Калининград, ул. Пролетарская, д. 66а.

3.2. Вид информационной системы – ***информационная система, обрабатывающая специальные, иные и общедоступные категории персональных данных сотрудников оператора, иные и общедоступные категории персональных данных, не являющихся сотрудниками оператора.***

Количество обрабатываемых субъектов персональных данных (сотрудников) - ***менее 100 000.***

Количество обрабатываемых субъектов персональных данных (не сотрудников) – **менее *100 000.***

3.3. Установленный уровень защищенности – в соответствии с п.11 (в) и 12 (а, б) Постановления Правительства РФ от 1.11.12 г. № 1119 – 3-й уровень защищенности.

4 Требования к составу и компонентам СЗИ и ЗКСПД

4. 1. Состав СЗИ и ЗКСПД в целом

В состав системы должны входить следующие основные подсистемы:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;

- ограничений программной среды;
- защиты машинных носителей информации;
- регистрации событий безопасности;
- антивирусной защиты;
- обнаружения (предотвращение) вторжений;
- контроля (анализа) защищенности информации;
- целостности информационной системы и информации;
- доступности информации;
- защиты среды виртуализации;
- защиты технических средств;
- защиты информационной системы, ее средств, систем связи и передачи данных
- выявление инцидентов и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

4.2. Требования к компонентам СЗИ и ЗКСПД

4.2.1. Подсистема идентификации и аутентификации субъектов доступа и объектов доступа

Должна обеспечивать идентификацию и аутентификацию пользователей (как работников оператора, так и внешних пользователей), устройств, в том числе стационарных, мобильных и портативных. Должен быть определен порядок и правила управления идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Должна быть обеспечена защита обратной связи при вводе аутентификационной информации.

В подсистеме должна осуществляться блокировка сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.

Подсистема должна осуществлять разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

4.2.2. Подсистема управления доступом субъектов доступа к объектам доступа

Должна осуществлять управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа осуществляется исходя из положения Политики информационной безопасности.

Подсистема должна производить управление (фильтрацию, маршрутизацию, контроль соединений и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

Должно выполняться разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

Устанавливается ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе), блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

Для удаленных пользователей системы необходима реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно - телекоммуникационные сети.

Должен быть обеспечен регламент и контроль использования в информационной системе технологий беспроводного доступа, мобильных технических средств

Подсистема должна обеспечивать управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

4.2.3. Подсистема ограничений программной среды

К подсистеме ограничения программной среды особые требования не предъявляются.

4.2.4. Подсистема защиты машинных носителей информации.

В подсистеме должен быть определен порядок учета машинных носителей информации, управления доступом к машинным носителям информации, правила уничтожения (стирания) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также систему контроля за уничтожением (стиранием) информации.

Должен быть определен порядок уничтожения (стирания) или обезличивания персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания информации.

4.2.5. Подсистема регистрации событий безопасности.

В соответствии с Политикой информационной безопасности, должны быть определены события безопасности, состав и содержание информации о событиях безопасности, подлежащие регистрации, и сроки их хранения.

Подсистема должна обеспечивать сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения, реагировать на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

Все события безопасности должны быть защищены от несанкционированных действий пользователей.

4.2.6. Подсистема антивирусной защиты.

В информационной системе должна быть обеспечена антивирусная защита. Антивирусная защита должна быть подключена к системе обновления базы данных признаков вредоносных компьютерных программ (вирусов).

4.2.7. Подсистема обнаружения (предотвращения) вторжений.

К подсистеме обнаружения вторжений особые требования не предъявляются.

4.2.8. Подсистема контроля (анализа) защищенности информации.

Должен быть определен порядок и правила контроля за установкой обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, работоспособность и параметры настройки, правильности функционирования программного обеспечения и средств защиты информации.

Подсистема должна содержать средства выявления, анализа уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. Должен осуществляться контроль работоспособности и состава средств защиты информации, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

4.2.9. Подсистема целостности информационной системы и информации.

В системе должны быть обеспечены возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций. Время и порядок восстановления должны быть определены соответствующими регламентирующими документами.

4.2.10. Подсистема доступности информации.

К подсистеме обеспечения доступности информации особые требования не предъявляются.

4.2.11. Подсистема защиты среды виртуализации.

Средства виртуализации в ИС не применяются.

4.2.12.Подсистема защиты технических средств.

На территории МАОУ СОШ № 31 должна быть обеспечена организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

Должен осуществляться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Необходимо исключить несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, помещения и сооружения, в которых они установлены.

Размещение устройств вывода (отображения) информации должно исключать ее несанкционированный просмотр.

4.2.13.Подсистема защиты информационной системы, ее средств, систем связи и передачи данных.

Подсистема должна обеспечивать защиту информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Подсистема должна обеспечивать защиту беспроводных соединений и мобильных технических средств, применяемых в информационной системе.

Подсистема должна обеспечивать защиту беспроводных соединений, применяемых в информационной системе.

4.2.14. Подсистема выявление инцидентов и реагирование на них.

К подсистеме выявления инцидентов и реагирование на них особые требования не предъявляются. Подсистема может быть реализована исходя из Политики информационной безопасности в МАОУ СОШ № 31.

4.2.15. Подсистема управления конфигурацией информационной системы и системы защиты персональных данных.

В МАОУ СОШ № 31 должен быть определен перечень лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных. Должны быть определены правила внесения изменений в конфигурацию. Перед внесением изменений должен проводиться анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных.

5. Требования к результатам проведения работ:

5.1. Требования к составу разработанной документации

В результате работ в МАОУ СОШ № 31 разрабатываются следующие документы:

- Приказ о назначении должностного лица, ответственного за организацию обработки персональных данных.
- Акт определения уровня защищенности.
- Акт классификации.
- Перечень ИСПДн.
- Частная модель угроз безопасности информации.
- Перечень целей и задач, решаемых информационной системой (перечень персональных данных).
- Рекомендации по организационно - техническим мероприятиям, направленным на блокирование (нейтрализацию) отдельных угроз безопасности информации.
- Политика обработки и защиты персональных данных (Положение об обработке и защите персональных данных).
- Проектная документация (частное техническое задание) на систему защиты информации информационной системы).
- Эксплуатационная документация на СЗИ (при закупке средств защиты информации).
- Правила (инструкции) доступа к управлению (администрированию) системы защиты информации.
- Правила осуществления внутреннего контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе.
- Методика проведения проверок полноты и детальности организационно-распорядительных документов по защите информации, действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации.

- Инструкции по действиям должностных лиц, ответственных за реализацию мер защиты информации.

- Правила оценки возможного вреда субъектам персональных данных и принятия мер по их предотвращению.

- Документы по оценке соответствия информационной системы требованиям по защите информации.