Защита информационного пространства в образовательных учреждениях

Маргарита Терехова

Эксперт 1С:Инфобезопасность

30.01.2024
–
31.01.2024

Направления «1С:ИнфоБезопасность»

- Защита ПДн
- Защита конфиденциальной информации
- Защита гос.тайны
- Защита объектов КИИ
- Поставка СЗИ
- Проведение пентестов
- Аудит ИБ

- Разработка ИС
- Внедрение системы видеонаблюдения
- Организация защищенного удаленного рабочего места
- Подключение к корпоративному центру мониторинга ГосСОПКА
- Аттестация государственных информационных систем (ГИС)

ИБ в образовании

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации

Цели:

- Защита ПД и информационного пространства от НСД, хищения информации и изменения конфигурации системы со стороны 3-х лиц
- Защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации

Основные понятия

Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Главное условие — по этим данным должно быть возможно однозначно определить, к какому конкретно человеку она относится

Оператор персональных данных – это государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

Основные понятия

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (согласно ФЗ-152)

ГИС – государственными информационными системами являются федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов

Угрозы в ИБ

- Угрозы намеренного характера (воздействие на ИС или ПО)
- Хищение интеллектуальной собственности
- Внешние атаки

Защита персональных данных

Защита персональных данных –

это комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определённому или определяемому на основании такой информации физическому лицу

Меры защиты.
Нормативно-правовые

1. **Постановление Правительства РФ от 01.11.2012 № 1119** «Об утверждении требований к защите ПДН при их обработке в информационных системах персональных данных»
2. **Приказ ФСТЭК России от 29.04.2021 № 77** «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»
3. **Приказ ФСБ России от 10.07.2014 № 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»
4. **Приказ ФСТЭК России от 18.02.2013 № 21** «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Меры защиты.
Административного характера (ОРД)

Система административно-организационных мер строится на базе внутренних регламентов и правил организации, которыми регламентируется порядок обращения с информацией и ее носителями

В том числе должны быть разработаны:

- должностные инструкции
- внутренние методики по ИБ
- перечни не подлежащих передаче данных
- регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Меры защиты. Административного характера (ОРД)

- Техпроцесс обработки и защиты ПДН
- Руководство пользователя
- Руководство пользователя СКЗИ
- Руководство ответственного пользователя СКЗИ
- Руководство ответственного за организацию обработки ПДН
- Руководство администратора безопасности
- Приказ об утверждении матрицы доступа
- Приказ об утверждении контролируемой зоны
- Приказ о создании комиссии
- Приказ о предоставлении доступа к ресурсам ИСПДН
- Приказ о назначении ответственного пользователя СКЗИ
- Приказ о назначении ответственного за обработку ПДН
- Приказ о назначении администратора безопасности
- Приказ о вводе в действие комплекта ОРД
- Правила рассмотрения запросов
- Приказ о вводе ИСПДН в эксплуатацию
- Правила рассмотрения запросов субъектов ПДН
- Правила осуществления внутреннего контроля обработки ПДН
- Правила обработки ПДн
- Положение по использованию СКЗИ
- Инструкция по управлению событиями ИБ
- Инструкция по управлению доступом
- Инструкция по контролю защищенности ПДН
- Инструкция по идентификации и аутентификации
- Инструкция позащите технических средств
- Инструкция по защите машинных носителей информации
- Инструкция по вводу ОРД
- Инструкция по антивирусной защите
- Инструкция о порядке взаимодействия с Роскомнадзор

Меры защиты. Физические

- Пропускная система
- Создание системы контроля доступом
- Сейф
- Решетки на окнах
- Шредер

Меры защиты. Технические

- **Программная защита** от несанкционированного доступа к ИСПДн
- **Организация безопасного межсетевого взаимодействия** при подключении ИСПДн к локальным сетям общего пользования или к сети Интернет
- **Применение систем шифрования** ПДн при необходимости их передачи по открытым каналам связи, например, при обмене информацией между территориально удаленными филиалами или офисами через сеть Интернет
- **Защита ПДн**, обрабатываемых в информационных системах, от вредоносного программного обеспечения, вирусов, троянов и т.д

Проверяющие органы

Роскомнадзор

ФСБ

ФСТЭК

Примеры ИС

- ФРДО
- ГНА
- ФИС ГИА и приема
- РИС ЕГЭ
- ИС «Бухгалтерия и кадры»
- «Электронный дневник», «Моя школа»

Этапы подключения к ИС

Создать систему защиты:

Разработать Организационно-распорядительную документацию

Пройти Оценку соответствия

Получить электронно-цифровую подпись (если необходимо)

Получить доступ

Сбор и анализ данных

Установка СЗИ

Мероприятия по выстраиванию системы защиты

- Сбор и анализ исходных данных
- Формирование требований к защите информации
- Разработка системы защиты ИС
- Внедрение системы защиты ИС
- Оценка соответствия информационной системы по требованиям защиты информации
- Обеспечение защиты информации в ходе эксплуатации аттестованной ИС
- Обеспечение защиты информации при выводе из эксплуатации ИС

Меры по оценке соответствия

Существует **две формы проведения мероприятий** по оценке соответствия системы защиты ПДн требованиям по защите информации:

Оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн

Аттестация ИСПДн на соответствие требованиям по защите информации

Талица №1. Отличия мер оценки соответствия системы защиты ПДн

Критерии сопоставления	Оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн	Аттестация ИСПДн на соответствие требованиям по защите информации
Разрабатываемые итоговые документы подтверждающие соответствие ИСПДн требованиям защиты информации (далее – Итоговые документы)	– «Протокол проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных»; – «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных».	– «Протокол проведения аттестационных испытаний информационной системы персональных данных»; – «Заключение по результатам аттестационных испытаний информационной системы персональных данных»; – «Аттестат соответствия информационной системы персональных данных требованиям по защите информации»
Срок действия итоговых документов при неизменности архитектуры ИСПДн	До 3 (трех) лет	В течение всего срока эксплуатации ИСПДн
Периодичность проведения периодического контроля уровня защиты ПДн, при их обработке в ИСПДн	Только при изменении инфраструктуры ИСПДн	Не реже 1 (одного) раза в 2 (два) года
Предоставление Заказчиком протоколов контроля уровня защищенности ПДн, при их обработке в ИСПДн, во ФСТЭК России	Не требуется	Обязательное условие. В случае невыполнения, действие Итоговых документов приостанавливается

Итог всех этих этапов

1. **Реализованы** организационные и технические меры по защите информации
2. **Функционирует** система защиты
3. **Разработаны** организационно-распорядительные документы

Пример: проведения работ по защите ИС «Бухгалтерия и Кадры» на 1 АРМ

Сбор и анализ исходных данных:

Результатом сбора и анализа исходных данных является документация, разрабатываемая Исполнителем, а именно:

- Акт обследования информационной системы персональных данных
- Модель угроз безопасности персональных данных
- Проект Акта определения уровня защищенности персональных данных
- Техническое задание на создание системы защиты персональных данных
- Программа и методики оценки эффективности реализованных мер по обеспечению безопасности персональных данных
- Комплект шаблонов организационно-распорядительной документации

Пример: проведения работ по защите ИС «Бухгалтерия и Кадры» на 1 АРМ

Поставка средств защиты информации, включает:

1. **Право на использование комплекта** «Постоянная защита» (СЗИ НСД, МЭ). Средства защиты информации Secret Net Studio 8
2. **Право на использование модуля** антивируса для ПО Secret Net Studio 8 (Срок использования 1 год)
3. **Внедрение поставляемых СЗИ** и разработка документации:
   - «Проект Технического паспорта ИСПДн»
4. **Проведение мероприятий** по оценке эффективности реализованных мер по обеспечению безопасности ПДн. Результатом мероприятий по оценке эффективности реализованных мер по обеспечению безопасности ПДн является разработанная Исполнителем документация:
   - «Протокол проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн»
   - «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности ПДн». Срок действия «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности ПДн»: 3 года при условии, что Заказчик обеспечивает соответствие ИСПДн, выданному заключению

Комплекс мер

- Проведение аттестационных работ и выдача аттестата соответствия
- Подбор и поставка СЗИ и СКЗИ
- Услуги по установке и настройке СЗИ и СКЗИ
- Проведение пентестов и аудитов

ASTRAL VIDEO SYSTEM

Отечественное решение для систем видеонаблюдения, предназначенное для визуального контроля объектов любого масштаба

Комплексный подход при построении систем видеонаблюдения

- Поставка оборудования
- Монтаж СКС и оборудования
- Настройка оборудования и ПО
- Интеграция с внедренными системами
- Тестирование системы и ввод в эксплуатацию
- Техническое сопровождение

Функционал текущей версии

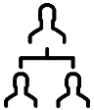
Трансляция Передает аудио и видео данные на внешний сервер или портал по открытым и защищенным каналам связи

Запись Ведет видеозапись с одновременным контролем целостности записываемых файлов и свободного пространства на диске

Контроль Реализует управление видеокамерами через систему мониторинга, с разграничением прав доступа пользователей

Масштабирование Позволяет увеличить количество объектов видеонаблюдения и видеокамер без необходимости кратного наращивания мощностей в ЦОД

Возможности текущей версии



Централизованное управление и разграничение прав доступа пользователей

Мониторинг модулей ПО, основных технических средств и состояния каналов связи

Автоматическая балансировка нагрузки гибкая настройка серверной части

Навигация по видеоархивам многомесячной глубины, экспорт файлов

Дистанционная установка, тех. поддержка и обновление до актуальных версий

Возможности текущей версии

Двухуровневая архитектура ПО – реализует мониторинг объектов видеонаблюдения и построение распределенной системы с единым центром управления

Отечественное решение – производительное видео-ядро собственной разработки, функционирующее в среде свободных ОС семейства Linux

Возможность разработки дополнительного функционала для специализированных задач; внедрения сторонних модулей видео аналитики

Видеотрансляция и видеозапись с неограниченного количества камер

Интеграция с федеральными порталами и закрытыми платформами: СМОТРИЕГЭ, ЕИМТС, ЕСПД, VPN-сети РЦОИ

СФЕРА 2.0
Блокиратор радиосигналов

Где применяется:

- Аудитории проведения ЕГЭ
- Медицинские учреждения
- Переговорные комнаты

Устройство блокирует работу сотовых телефонов и цифровых устройств передачи данных, расположенных в радиусе до 15 метров от устройства

Нормативные документы

- Во исполнение писем Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) за № 02-598 от 05.08.2014г. и №02-608 от 12.08.2014г
- **Решение ГКРЧ от 10.03.2017 №17-40-10 дсп**

  «О выделении полос радиочастот 463-467,5 МГц, 791-820 МГц, 925-960 МГц, 1805-1880 МГц, 2110-2170 МГц, 2400-2483,5 МГц, 2570-2620 МГц, 2620-2690 МГц, 5150-5350 МГц для применения блокираторов радиосигналов». О ходе выполнения требований решения ГКРЧ от 10.03.2017 № 17-40-10 дсп по возможности дальнейшего применения блокираторов радиосигналов в местах размещения пунктов проведения экзаменов при проведении единого государственного экзамена (для служебного пользования)

Методические рекомендации по подготовке и проведению ЕГЭ в пунктах проведения экзаменов в 2023 г

- По решению ОИВ ППЭ также могут быть оборудованы системами подавления сигналов подвижной связи. Иные помещение ППЭ (за исключением аудитории и Штаба ППЭ) оборудуются средства видеонаблюдения по решению ОИВ

Описание устройства

Современный дизайн

Работа от сети 220V

Неограниченное время работы

Бесшумная система охлаждения

Гарантия 1 год, срок службы 5 лет, производство - Россия

Интуитивно понятная индикация на корпусе прибора

Использование в федеральных проектах повышающих качество образования

Описание устройства

CDMA-450	CDMA-800	GSM-900	GSM-1800
463 – 467,5	791 – 820	925 – 960	1805 – 1880

3G	4G	Wi-Fi	Bluetooth
2110 – 2170	2570 – 2690	2400 – 2483,5	2400 – 2483,5

Преимущества

Незаметность и тишина Действия прибора незаметно для посетителей и не мешает работе аппаратов мобильной связи, расположенных вне рабочей зоны. Так как вместо кулеров используются радиаторы, работа устройства происходит в полной тишине

Влияние на другие устройства Отсутствие влияния на любые другие радиоэлектронные устройства, кроме диапазона принимаемых сотовым телефоном и цифровым передатчиком данных частот

Бесконечное количество каналов Блокировка одновременно любого количества каналов и всех операторов связи в рабочем диапазоне

Безопасно для здоровья Блокираторы СФЕРА 2.0 абсолютно безопасны для всех и не несут никакого негативного влияния на здоровье. Подавители сотовой связи работают на тех же частотах и той же мощности что и мобильные телефоны или цифровые передатчики данных, поэтому их действие не повлияет даже на эмоциональное состояние человека. Подтверждено СЕРТИФИКАТОМ СанПиН

Проекты для системы образования

- Разработка ведомственных ИС при необходимости
- Аттестация ГИС
- Реализация проектов по защите ИСПДн под ключ
- Подключение к ГНА в Вузах
- Оборудование ППЭ системами подавления сотовой связи
- Подключение к корпоративной сети ФЦТ в Сузах и Вузах
- Оборудование ППЭ системой онлайн видеонаблюдения
- Доработка имеющейся системы защиты ИСПДн
- Развёртывание и техническое обслуживание ситуационного центра видеонаблюдения для проведением ЕГЭ

СПАСИБО ЗА ВНИМАНИЕ!

infosec@1c.ru: