Практика 11

Цель работы: получение навыков формирования мер и требований к информационной безопасности для обеспечения комплексной безопасности объектов информатизации

Задание выполняется в группах, объекты – те же организации, что и на практике №1 на основе результатов предыдущей работы (практики). При выполнении задания опираться на результаты практик 7-10.

1. На основе нормативных требований (практики 8-10) и модели угроз (практика 7) сформировать общий требований ИБ для рассматриваемой организации. Составить таблицу с колонками:
   1. Источник (конкретный НПА, один или несколько, или МУ). Одинаковые требования из разных источников – объединить.
   2. Формулировка требования
   3. Состояние выполнения требования в организации (выполняется или нет)
2. Разработать план реализации мер информационной безопасности (для не реализованных на данный момент мер) . Составить таблицу вида:
   1. Требование (из таблицы 1)
   2. Планируемый способ выполнения (организационные или технические меры)
   3. Источники требований к средствам / мерам выполнения (сертификация/оценка соответствия, соответствие типовым примерам, соответствие ГОСТ с номером стандарта и т.д.)
   4. Планируемые сроки реализации

Оформить результат в виде:

1. Презентации для рассказа (при необходимости)
2. Файла в формате doc/docx/odt - по одному отдельному файлу на каждый ОКИИ.

|  |  |  |
| --- | --- | --- |
| Источник (НПА) | Формулировка требования | Состояние выполнения требования |
| ФЗ № 149-ФЗ "Об информации, информационных технологиях и о защите информации" | Обязательное включение в реестр КИИ, строгий контроль доступа  Регулярные проверки соответствия требованиям  Минимальные требования, но обязательное соблюдение базовых мер | Выполняется |
| ФЗ № 152 "О персональных данных" (ст. 19) | Шифрование ПДн, строгий контроль доступа, обязательная сертификация ФСТЭК/ФСБ. Авторизация доступа, журналирование, защита от утечек.  Назначение ответственного за обработку персональных данных  Уведомление Роскомнадзора о начале обработки ПДн | Выполняется (шифрование в 1С и CRM)  Выполняется (отдел ИБ + специалист по безопасности данных)  НЕ Выполняется |
| ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» | Обязанность присвоить объектам КИИ категорию значимости и уведомить ФСТЭК/ФСБ. | Выполняется |
| Приказ ФСТЭК России от 11.02.2013 № 17 | Полная изоляция от публичных сетей (при необходимости).  Многофакторная аутентификация.  Обязательное применение сертифицированных СЗИ (средств защиты информации).  Регулярные проверки ФСТЭК.  Контроль целостности данных.  Разграничение прав доступа.  Обязательное ведение журналов событий.  Минимальные меры: антивирус, парольная политика. | Выполняется |
| Приказ ФСТЭК №21 | Использование СКЗИ при передаче ПДн | НЕ Выполняется  (требуется защищенный VPN для 1С и CRM) |
| Приказ ФСТЭК № 31 (требования к антивирусной защите) | Установка сертифицированного антивирусного ПО на все узлы КИИ с ежедневным обновлением баз | Выполняется |
| Приказ ФСТЭК России от 25.12.2020 № 239 | Полная изоляция от интернета (при необходимости).  Внедрение системы фильтрации трафика (межсетевые экраны, IDS/IPS) для объектов КС1 и КС2.  Обязательное применение ГОСТ-сертифицированных средств защиты.  Круглосуточный мониторинг инцидентов.  Защита от DDoS-атак.  Резервное копирование данных. | Выполняется |
| Приказ ФСТЭК № 235 (физическая защита объектов КИИ) | Обеспечение физической охраны серверных помещений (КС1) с видеонаблюдением и контролем доступа | НЕ Выполняется |
| ГОСТ Р 57580.1-2017 | Обязательное применение сертифицированных средств защиты (СЗИ, СКЗИ).  Многофакторная аутентификация (токены).  Шифрование каналов передачи данных (TLS, VPN).  Непрерывный мониторинг и реагирование на инциденты (SIEM-системы).  Физическая защита серверов (ДПЗ, видеонаблюдение).  Обязательное использование межсетевых экранов (МЭ) и антивирусов.  Резервное копирование данных.  Аудит действий пользователей. Ведение журналов учета обращений к ПДн | Частично выполняется |
| Постановление Правительства РФ от 01.11.2012 № 1119 | Обязательное шифрование ПДн.  Физическая охрана серверов.  Контроль доступа на основе ролей.  Регулярные аудиты.  Оценка вреда при утечке ПДн клиентов | Выполняется |
| Постановление Правительства № 1272 (2022) | Назначение заместителя руководителя, ответственного за ИБ, с определением его полномочий | Выполняется |
| Постановление Правительства № 743 (2019) | Обеспечение резервирования каналов связи для объектов КС1 и КС2 | НЕ Выполняется |
| Постановление Правительства № 1478 (2022) | Создание системы мониторинга защищенности объектов КИИ | Выполняется |
| Постановление Правительства № 127 (резервное копирование) | Ежедневное резервное копирование данных КС1 с хранением копий на отдельном защищенном носителе. | Выполняется |
| Приказ ФСБ России от 10.07.2014 № 378 | Обязательное использование сертифицированных СКЗИ (КриптоПро, VipNet).  Рекомендуется шифрование каналов связи. | НЕ Выполняется (требуется КриптоПро 4.0) |
| Приказ Минцифры № 372 (учет и контроль оборудования | Ведение реестра аппаратного и программного обеспечения КИИ с ежегодной инвентаризацией. | НЕ Выполняется |
| Приказ ФСБ № 514 (шифрование данных) | Шифрование каналов передачи данных (VPN, TLS 1.2+) для объектов КС1. | Выполняется |
| Приказ ФСБ № 368 (2018) | Организация обмена информацией о компьютерных инцидента | НЕ Выполняется |
| Приказ ФСБ № 282 (2019) | Информирование ФСБ об инцидентах в течение 1 часа | НЕ Выполняется |
| Приказ ФСБ № 213 (2023) | Проведение мониторинга защищенности информационных ресурсов | Выполняется |

|  |  |  |  |
| --- | --- | --- | --- |
| **Требование (из Таблицы 1)** | **Планируемый способ выполнения** | **Источники требований к средствам / мерам выполнения** | **Планируемые сроки реализации** |
| Уведомление Роскомнадзора о начале обработки ПДн (ФЗ №152) | Организационные меры: подготовить и отправить уведомление | ФЗ №152, Методические рекомендации Роскомнадзора | 2 квартал 2025 |
| Использование СКЗИ при передаче ПДн | Технические меры: внедрение защищенного VPN на базе сертифицированных СКЗИ | Приказ ФСТЭК №21, ГОСТ Р 56939-2016, ФСТЭК реестр СКЗИ | 3 квартал 2025 |
| Физическая охрана серверных помещений (Приказ ФСТЭК №235) | Технические и организационные меры: установка СКУД, видеонаблюдение | Приказ ФСТЭК №235, ГОСТ Р 51558-2014 | 4 квартал 2025 |
| Использование сертифицированных криптосредств (Приказ ФСБ №378) | Технические меры: закупка и внедрение КриптоПро CSP 4.0+ | Приказ ФСБ №378, Реестр ФСБ сертифицированных криптосредств | 3 квартал 2025 |
| Резервирование каналов связи (Постановление №743) | Технические меры: подключение альтернативных каналов связи | Постановление №743, договоры с провайдерами связи | 4 квартал 2025 |
| Ведение реестра оборудования и ПО (Приказ Минцифры №372) | Организационные меры: формирование и ведение актуального реестра | Приказ Минцифры №372, форма учёта оборудования | 2 квартал 2025 |
| Ежегодная инвентаризация (Приказ Минцифры №372) | Организационные меры: составить план-график инвентаризации | Приказ Минцифры №372 | 4 квартал 2025 |
| Информирование ФСБ об инцидентах за 1 час (Приказ ФСБ №282) | Организационные меры: внедрение процедуры быстрого уведомления | Приказ ФСБ №282 | 2 квартал 2025 |
| Организация обмена информацией о киберинцидентах (Приказ ФСБ №368) | Организационные меры: включение в систему обмена с ФСБ | Приказ ФСБ №368 | 3 квартал 2025 |
| Обязательное применение сертифицированных средств защиты (ГОСТ Р 57580.1-2017) | Технические меры: внедрение сертифицированных СЗИ и СКЗИ. | ГОСТ Р 57580.1-2017, Приказ ФСТЭК №17, Приказ ФСБ №378 | 3-4 квартал 2025 |
| Многофакторная аутентификация (ГОСТ Р 57580.1-2017) | Технические меры: внедрение токенов и МФА систем для доступа к критическим ресурсам | ГОСТ Р 57580.1-2017, Приказ ФСТЭК №17 | 3 квартал 2025 |
| Шифрование каналов передачи данных (ГОСТ Р 57580.1-2017) | Технические меры: внедрение TLS и VPN на всех каналах связи | ГОСТ Р 57580.1-2017, Приказ ФСБ №514, Приказ ФСТЭК №21 | 3-4 квартал 2025 |
| Непрерывный мониторинг и реагирование на инциденты (ГОСТ Р 57580.1-2017) | Технические меры: внедрение и настройка SIEM-системы | ГОСТ Р 57580.1-2017, Приказ ФСТЭК №239 | 4 квартал 2025 — 1 квартал 2026 |
| Обязательное использование межсетевых экранов и антивирусов (ГОСТ Р 57580.1-2017) | Технические меры: установка и настройка сертифицированных межсетевых экранов и антивирусов | ГОСТ Р 57580.1-2017, Приказ ФСТЭК №31 | 2-3 квартал 2025 |
| Резервное копирование данных (ГОСТ Р 57580.1-2017) | Технические меры: ежедневное создание резервных копий, хранение на защищенных носителях | ГОСТ Р 57580.1-2017, Постановление №127 | Выполняется / контроль - 2 квартал 2025 |