|  |  |  |
| --- | --- | --- |
| Источник (НПА) | Формулировка требования | **Состояние выполнения для классов защищенности информационной системы** |
| 1 класс |
| Федеральный закон от 27.07.2006 № 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. |  |
| 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 России от 25.12.2020 № 239 | Полная изоляция от интернета (при необходимости).  Обязательное применение ГОСТ-сертифицированных средств защиты.  Круглосуточный мониторинг инцидентов.  Защита от DDoS-атак.  Резервное копирование данных. |  |
| ГОСТ Р 56939-2016 | Не содержит требований |  |
| 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.  Контроль доступа на основе ролей (RBAC).  Резервное копирование данных.  Аудит действий пользователей. | **50/50 тк этот гост для финансовых организаций** |
| Постановление Правительства РФ от 01.11.2012 № 1119 | Обязательное шифрование ПДн.  Физическая охрана серверов.  Контроль доступа на основе ролей.  Регулярные аудиты. |  |
| Приказ ФСБ России от 10.07.2014 № 378 | Обязательное использование сертифицированных СКЗИ (КриптоПро, VipNet).  Рекомендуется шифрование каналов связи. |  |

Таблица 1

| Требование (из таблицы 1) | Планируемый способ выполнения | Источники требований |
| --- | --- | --- |
| Шифрование ПДн, журналирование (ФЗ № 152) | Внедрение SIEM-системы для журналирования. Обновление политик шифрования. | ГОСТ Р 57580.1-2017, Приказ ФСТЭК № 17 |
| Защита от DDoS-атак, мониторинг (Приказ ФСТЭК № 239) | Установка DDoS-протекции и внедрение системы мониторинга. | Рекомендации ФСТЭК, ГОСТ Р 57580.1-2017 |
| Сертификация VipNet (Приказ ФСБ № 378) | Приобретение и внедрение сертифицированного ПО VipNet. | Требования ФСБ к СКЗИ (Приказ № 378) |
| Внедрение SIEM-системы (ГОСТ Р 57580.1-2017) | Закупка SIEM-решения (например, Splunk) для непрерывного мониторинга. | ГОСТ Р 57580.1-2017, Приказ ФСТЭК № 239 |
| Физическая защита серверов (ГОСТ Р 57580.1-2017) | Установка СКУД и видеонаблюдения в серверной | ГОСТ Р 57580.1-2017, Постановление № 1119. |
| Шифрование каналов связи (Приказ ФСБ № 378) | Внедрение VPN на базе VipNet. | Приказ ФСБ № 378 (п. 7), ГОСТ Р 57580.1-2017 |

Таблица 2