ТКБ ИНВЕСТМЕНТ ПАРТНЕРС

Что делать? Управляющая компания и требования Положения № 757-П Банка России

Илья Смирнов

Ноябрь 2021

17 апреля 2019г…

- Товарищ командир, мы окружены…
- Отлично, сержант! Можем действовать в любом направлении!!!

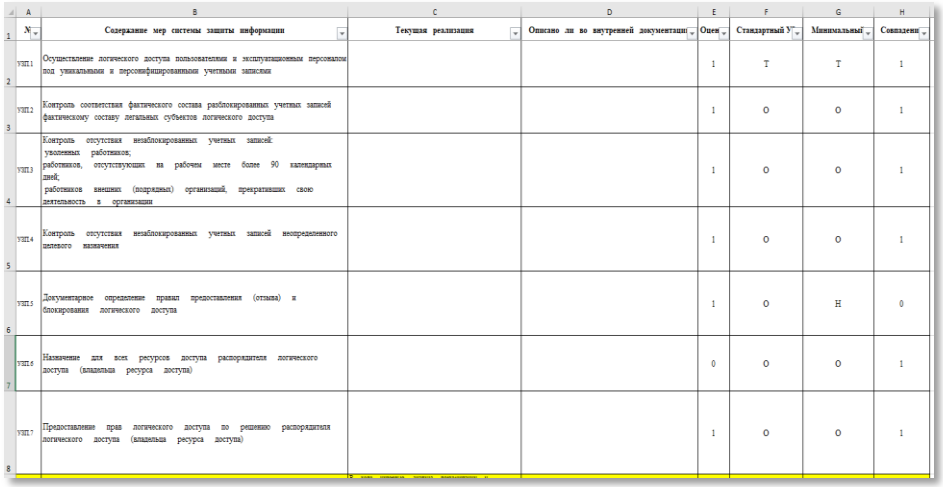
Положение Банка России №684-П

- ГОСТ Р 57580.1-2017
- Требования к ПО взаимодействия с клиентами
- Требования к электронному обмену
- Требования к обработке защищаемой информации
- Требования к управлению инцидентами ИБ.

Положение Банка России от 20.04.2021г. №757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Оценка применимости, состояния, соответствия

- Соответствие какому уровню ЗИ обеспечивать?
  - На текущий момент
  - Через 2-3 года
- Вопросы трактовки положений НПА
  - «Лучше тихо спросить у инструктора, чем громко выстрелить себе в ногу»
  - Банк России
  - Комитет по экономической и информационной безопасности НАУФОР
  - Коллеги и сообщества
  - Правильные вопросы
- Самооценка
  - Excel-файл с формулами
  - Взаимодействие с подразделениями
- Внешний аудит
  - Репетиция аудита «на оценку» (проверки)
  - Накопленный опыт по различным секторам и стандартам.



№	Содержание мер системы защиты информации	Текущая реализация	Описано ли во внутренней документации	Оцен	Стандартный У	Минимальный	Совпадени
УПД.1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями			1	Т	Т	1
УПД.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа			1	О	О	1
УПД.3	Контроль отсутствия незаблокированных учетных записей: уволенных работников; работников, отсутствующих на рабочем месте более 90 календарных дней; работников внешних (подрядных) организаций, прекративших свою деятельность в организации			1	О	О	1
УПД.4	Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения			1	О	О	1
УПД.5	Документарное определение правил предоставления (отзыва) и блокирования логического доступа			1	О	Н	0
УПД.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа)			0	О	О	1
УПД.7	Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа)			1	О	О	1

Стратегия и планирование

- Совместная работа с бизнес-подразделениями и руководством
- Принцип Парето
  - Результаты оценки соответствия
  - Реальные угрозы и векторы атак
- Бюджет
  - Соответствие статей затрат и мер из ГОСТ, 757-П
- Персонал ИБ
  - Security champions
  - Дистанционная работа
  - Фиксация времени
- Внутренняя разработка ПО и ОУД4
  - Больше требований, по сравнению с 684-П
  - Отдельный большой участок работы
- Дорожная карта
  - Учет реалий конкретной УК
  - Наглядность и отслеживание результата

Тактика реализации требований

- Коммуникация и взаимодействие
  - Цели и задачи
  - Идеальный результат
  - Ближайшие шаги
- Инвентаризация активов
  - Что есть?
  - Зачем это?
  - Кто ответственный?
- Принцип Парето (для мер и процессов ИБ)
  - Критические точки
- Итерационное, продуманное выстраивание процессов
- Внедренное техническое СЗИ => время на поддержку
- Внедренный процесс => время на поддержку
- Доработка существующих документов (ЛНА) для смежных областей и НПА под требования 757-П
- Доработка работающих процессов под требования 757-П
- Работа с руководством и ключевыми сотрудниками
- Настройка имеющихся СЗИ.

Вопросы