



ОЦЕНКА СООТВЕТСТВИЯ ПО ГОСТ 57580.1 ГЛАЗАМИ АУДИТОРА

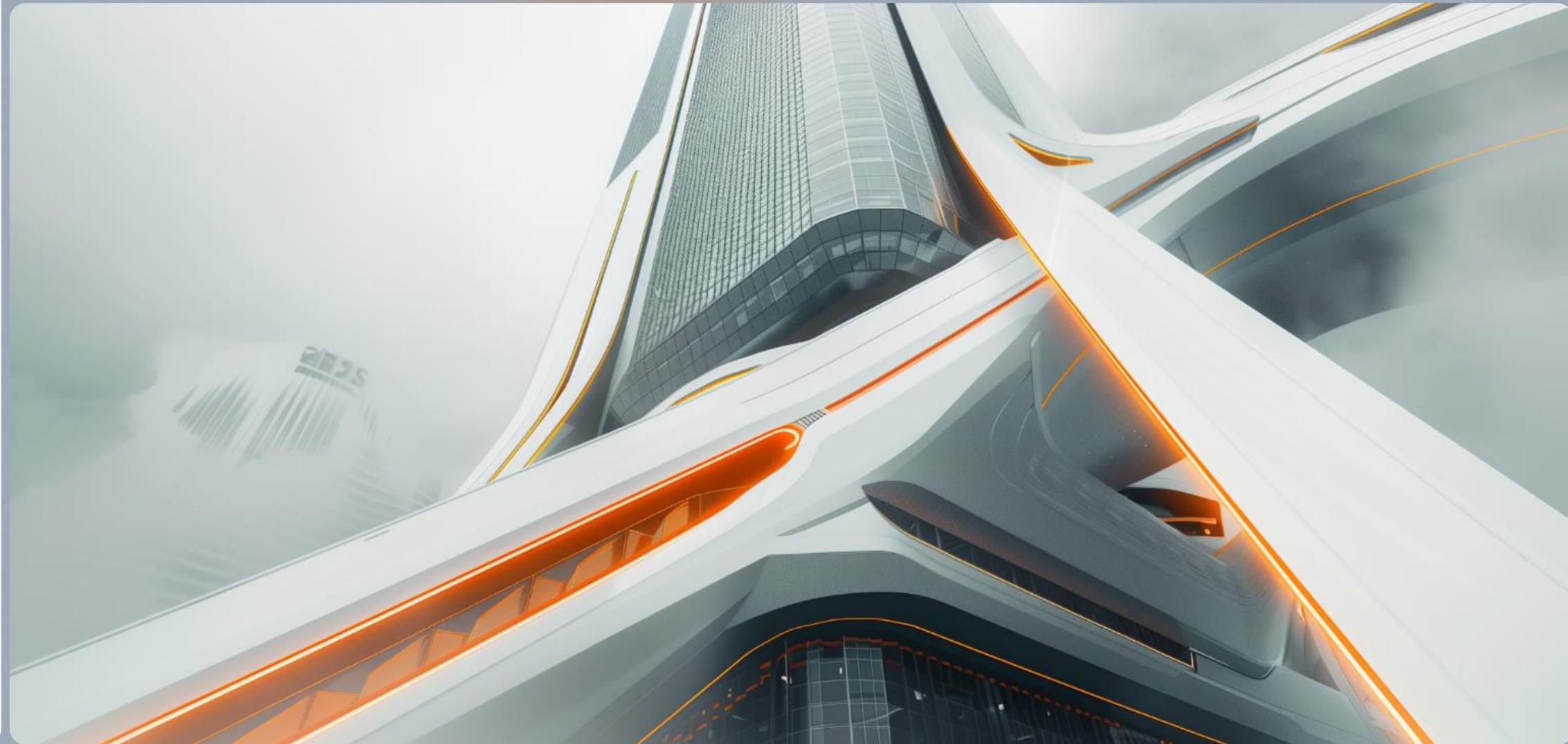
Александр
Хонин

Руководитель отдела
консалтинга и аудита
Angara Security





ОСНОВНЫЕ ТРЕБОВАНИЯ





МЕТОДОЛОГИЧЕСКАЯ ОСНОВА ПРОВЕДЕНИЯ РАБОТ



Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»



Национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018
«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»



УРОВНИ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень 3 – **минимальный**



Уровень 2 – **стандартный**



Уровень 1 – **усиленный**





ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

- Обеспечение защиты информации при управлении доступом
- Обеспечение защиты вычислительных сетей
- Защита среды виртуализации
- Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств
- Контроль целостности и защищенности информационной инфраструктуры
- Защита от вредоносного кода
- Предотвращение утечек информации
- Управление инцидентами защиты информации





ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ





ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

Меры защиты информации
на этапе «Создание
(модернизация) АС»

Меры защиты
информации на этапе
«Ввод в эксплуатацию АС»

Меры защиты
информации на этапе
«Эксплуатация
(сопровождение) АС»

Меры защиты информации
на этапе «Эксплуатация
(сопровождение) и снятие
с эксплуатации АС»





ВЫБОР И ПРИМЕНЕНИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

Выбор мер защиты информации из базового состава (раздел 7 Стандарта)



Адаптация (уточнение) при необходимости выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей безопасности информации и структурно-функциональных характеристик объектов информатизации, в том числе АС, включаемых в область применения стандарта



Исключение из базового состава мер, не связанных с используемыми информационными технологиями



Дополнение при необходимости адаптированного (уточненного) состава и содержания мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации



Применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты информации в соответствии с положениями разделов 8 и 9 настоящего стандарта





ОСНОВНЫЕ НЕДОСТАТКИ, ВЫЯВЛЯЕМЫЕ НА ДАННОМ ЭТАПЕ



Отсутствует модель угроз и нарушителей
безопасности информации



Отсутствует выбранный состав мер
защиты информации





ОЦЕНКА СООТВЕТСТВИЯ





ОСНОВНЫЕ ЭТАПЫ ПРОВЕДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ

Сбор исходных
данных



Проведение
обследования



Оценка
соответствия



Подготовка
отчета



СБОР ИСХОДНЫХ ДАННЫХ

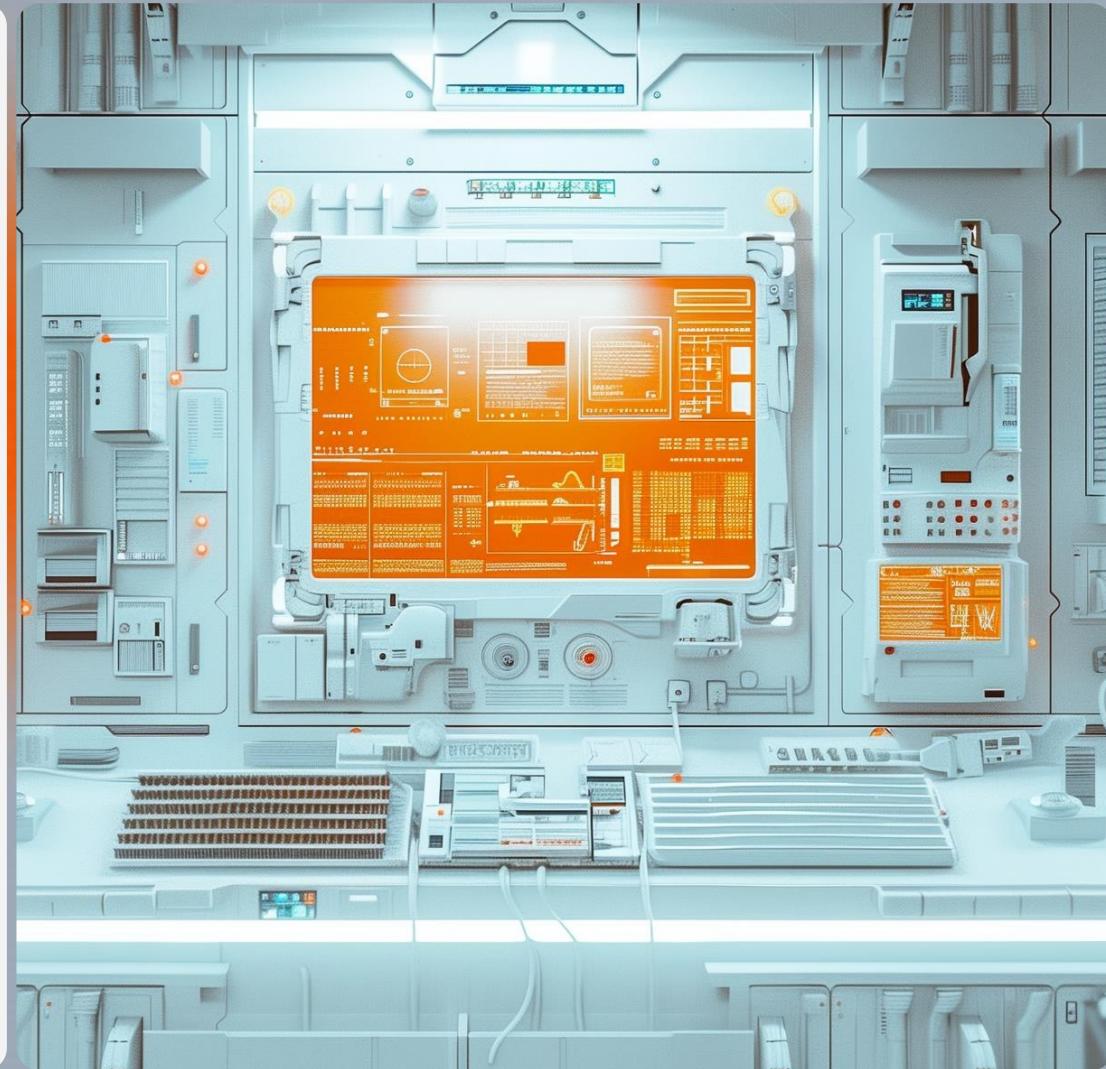
- Сведения о Банке
- Сведения о площадках Банка, входящих в область проекта
- Сведения о подразделениях Банка, задействованных в осуществлении переводов денежных средств и платежных операциях
- Предварительный статус работ
- Сведения об участии в платежных системах и реализации отдельных требований Положений ЦБ РФ
- Сведения об ИТ-инфраструктуре
- Сведения о персонале
- Общие вопросы по обеспечению информационной безопасности в Банке
- Сведения о документировании процессов информационной безопасности
- Схема информационной инфраструктуры Банка



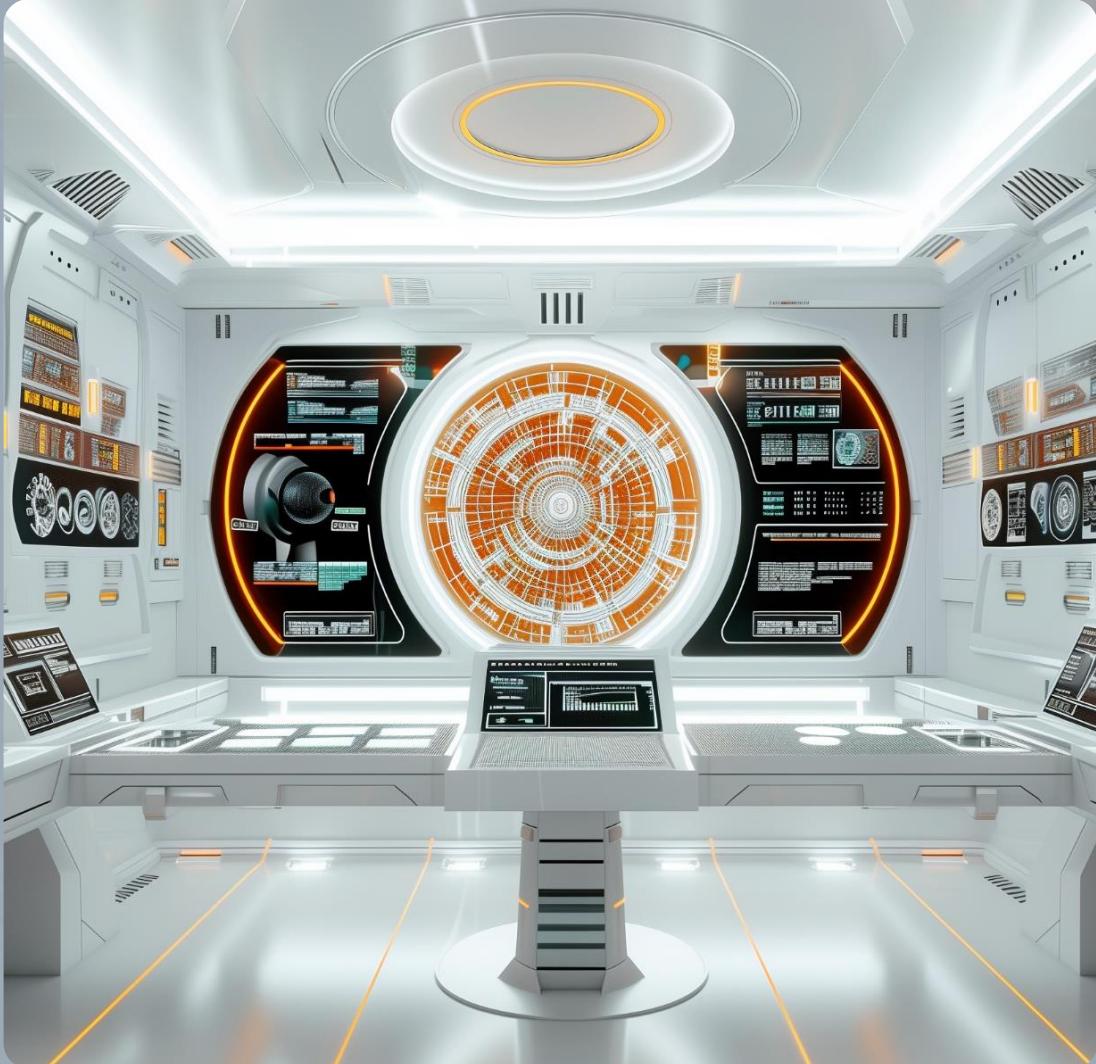


ОСНОВНЫЕ СЛОЖНОСТИ

- Выделение ресурса со стороны проверяемой организации для сбора исходных данных
- Заполнение анкеты по сбору исходных данных
- Длительность предоставления исходных данных



ПРОВЕДЕНИЕ ОБСЛЕДОВАНИЯ



- Подготовка плана интервьюирования
- Проведение интервью
- Подготовка протоколов интервьюирования
- Фиксация выявленных нарушений
- Сбор свидетельств

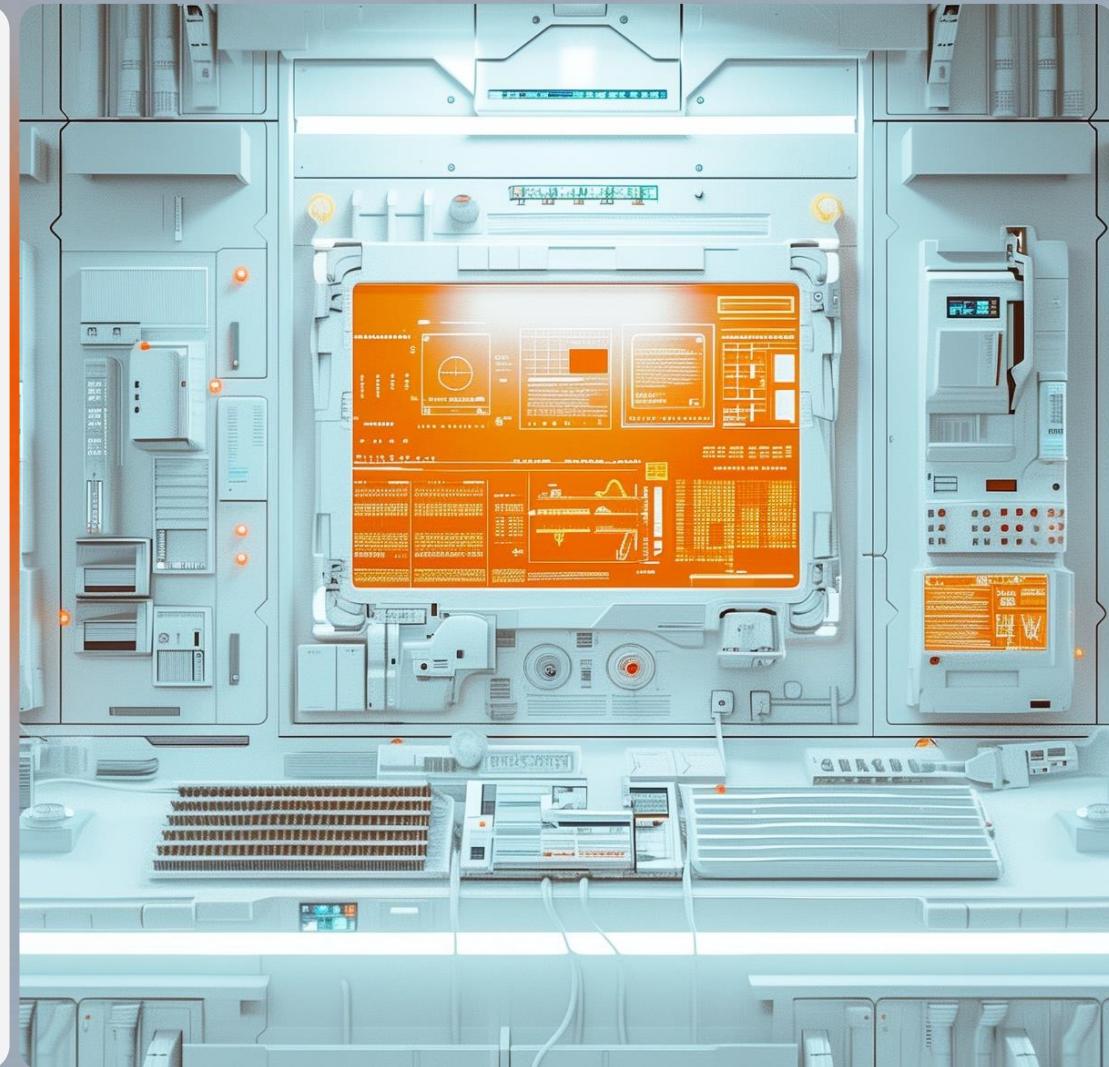


ПЛАН ИНТЕРВЬЮИРОВАНИЯ

| № | Тема встречи | Перечень основных тем | Длительность, часы | Подразделение / сотрудник со стороны Банка | ФИО респондента <i>(указать)</i> | Дата и время <i>(указать)</i> | Контактная информация респондента <i>(указать)</i> | Статус | Комментарии |
|---|---|--|--------------------|---|-------------------------------------|----------------------------------|---|--------|-------------|
| 1 | Вводная встреча по проекту | - Уточнение области аудита (перечня АС/подразделений, входящих в область аудита) - Порядок работы | 1 | - Ответственный за проект со стороны Банка - Руководитель Департамента ИБ - Руководитель (ответственный сотрудник) подразделения ИТ - Ответственный за физическую безопасность - Руководители (ответственные сотрудники) подразделений, задействованных в переводах денежных средств (оциально) | | | | | |
| Архитектура и функционирование автоматизированных систем | | | | | | | | | |
| 2 | Архитектура и функционирование АС **** | 1. Архитектура и состав АС, включая: а) перечень технических средств АС и их роли; б) используемые ОС, СУБД и ППО; | 1 | - Подразделение ИТ (ответственные сотрудники - владелец АС, ответственный за сопровождение и тех.обслуживание АС) - Ответственный сотрудник ДИБ | | | | | |
| 15 | Архитектура и функционирование объектов и ресурсов Банка, предназначенных для взаимодействия с *** | в) физическое расположение технических средств АС; г) пользователи АС, механизмы взаимодействия пользователей с АС; е) ответственность за сопровождение и техническое обслуживание АС. | 0,5 | | | | | | |
| 16 | Архитектура и функционирование объектов и ресурсов Банка, предназначенных для взаимодействия с платежной системой "Мир" | 2. Встроенные меры защиты информации АС: - Механизмы контроля логического доступа к АС; - Регистрация событий безопасности; - Резервное копирование и восстановление данных АС. | 0,5 | | | | | | |
| 17 | Архитектура и функционирование приложения **** | | 0,5 | | | | | | |
| Вопросы обеспечения информационной безопасности | | | | | | | | | |
| 24 | | | | | Управление доступом | | | | |
| 24.1 | управление правами доступа и назначение ролей сотрудникам | - Предоставление, изменение и отзыв прав доступа пользователей (внутренних и внешних) - Правила создания и управления учетными записями пользователей - Определение ролей доступа - Периодический пересмотр прав доступа - Управление удаленным доступом | 1 | - Ответственный сотрудник ДИБ - Сотрудники подразделения ИТ, ответственные за предоставление доступа | | | | | |

ОСНОВНЫЕ СЛОЖНОСТИ

- Выделение ресурса со стороны проверяемой организации для сопровождения интервью и сбора свидетельств
- Выделение ресурсов для проведения интервью
- Сбор свидетельств



ОЦЕНКА СООТВЕТСТВИЯ

- Анализ собранных данных и запрос дополнительной информации при необходимости
- Анализ выполнения мер защиты информации
- Фиксация выявленных нарушений





КОМПЕНСИРУЮЩИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

| ID | Мера реализации | Требование | Компенсирующие мероприятия |
|--|-----------------|---|----------------------------|
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | | | |
| УЗП.1 | Т | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями | |



БАЗОВЫЙ ПЕРЕЧЕНЬ НАРУШЕНИЙ ЗИ



- Осуществление логического доступа под учетными записями неопределенного целевого назначения
- Осуществление логического доступа под коллективными неперсонифицированными учетными записями
- Наличие незаблокированных учетных записей уволенных работников
- Отсутствие разграничения логического доступа
- Несанкционированное предоставление пользователям административных прав
- Несанкционированное предоставление пользователям прав логического доступа
- Хранение паролей субъектов доступа в открытом виде
- Передача аутентификационных данных в открытом виде по каналам и линиям связи



- Отсутствие регистрации персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации
- Отсутствие разграничения физического доступа в помещения, в которых расположены объекты доступа
- Несанкционированный физический доступ посторонних лиц в помещения, в которых расположены объекты доступа
- Отсутствие логической сетевой изоляции внутренних вычислительных сетей финансовой организации и сети Интернет и/или беспроводных сетей
- Передача информации конфиденциального характера с использованием сети Интернет, телекоммуникационных каналов и/или линий связи, не контролируемых финансовой организацией, в открытом виде

БАЗОВЫЙ ПЕРЕЧЕНЬ НАРУШЕНИЙ ЗИ

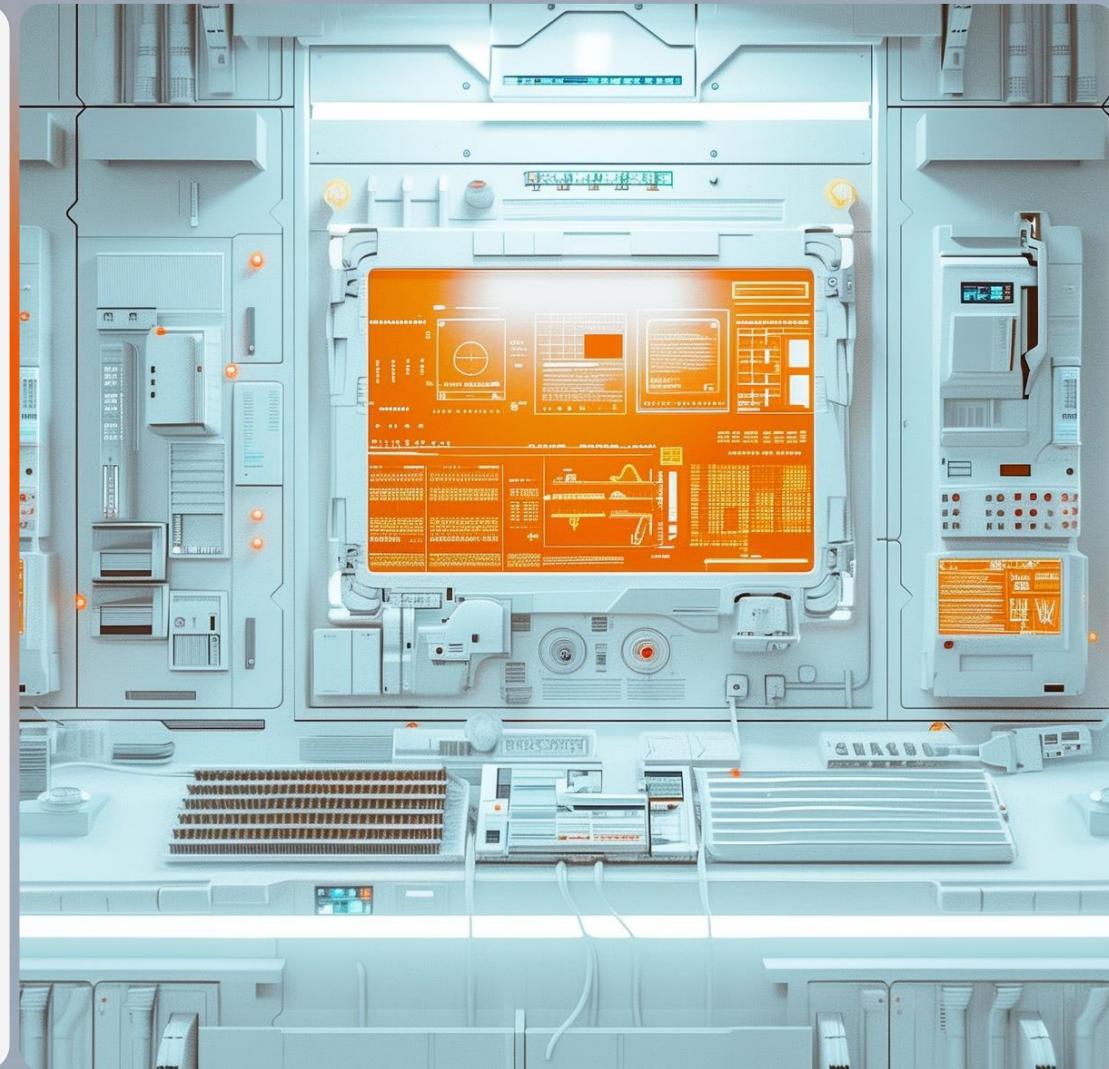
- Наличие в контролируемой зоне финансовой организации незарегистрированных точек беспроводного доступа, имеющих подключение к локальной вычислительной сети финансовой организации
- Использование нелицензионного ПО
- Отсутствие применения средств защиты от воздействия вредоносного кода
- Обработка информации конфиденциального характера с использованием неучтенных МНИ
- Отсутствие гарантированного стирания информации конфиденциального характера с МНИ при осуществлении их вывода из эксплуатации или вывода из эксплуатации СВТ, в состав которого входят указанные МНИ, а также при необходимости их передачи в сторонние организации
- Отсутствие реагирования на инциденты ЗИ





ОСНОВНЫЕ СЛОЖНОСТИ

- Сбор свидетельств





ПОДГОТОВКА ОТЧЕТА

- «Отчет по результатам оценки соответствия требованиям Стандарта ГОСТ Р 57580.1-2017»
- «Калькулятор с результатами оценки соответствия»
- «Архив со свидетельствами»
- «Заполненная форма по ОКУД 0409071»

СТРУКТУРА ОТЧЕТА

| | |
|---|----|
| Термины и определения | 8 |
| Принятые сокращения и условные обозначения | 12 |
| Заявление о конфиденциальности | 15 |
| 1 Общие сведения | 16 |
| 1.1 Цель и задачи проведения работ | 16 |
| 1.2 Сведения о проверяемой организации | 16 |
| 1.3 Сведения о проверяющей организациии | 17 |
| 1.4 Состав проверяющей группы | 17 |
| 1.5 Сроки проведения оценки соответствия | 17 |
| 1.6 Методологическая основа проведения работ | 17 |
| 1.7 Краткое изложение процесса оценки соответствия | 18 |
| 1.8 Область проведения оценки и способы сбора информации | 19 |
| 1.9 Перечень предоставленных свидетельств | 21 |
| 2 Статус Банка в платежных системах | 25 |
| 2.1 Перечень платежных систем | 25 |
| 2.2 Статус Банка в платежной системе Банка России | 25 |
| 3 Описание автоматизированных систем, входящих в область проведения оценки | 31 |
| 3.1 Общие сведения об автоматизированных системах, входящих в область оценки соответствия | 31 |
| 3.2 АБС «****» | 32 |
| 3.2.1 Назначение системы | 32 |
| 3.2.2 Пользователи системы | 32 |
| 3.2.3 Архитектура системы | 33 |
| 3.2.4 Встроенные меры защиты информации | 33 |
| 3.3 АБС «***» | 33 |
| 3.3.1 Назначение системы | 33 |
| 3.3.2 Пользователи АС | 34 |
| 3.3.3 Архитектура АС | 34 |
| 3.3.4 Встроенные меры защиты информации | 34 |
| 3.17 Контур безопасности в соответствии с требованиями нормативно-правовых актов Банка России по ГОСТ Р 57580.1 | 47 |
| 4 Применимые способы и меры обеспечения ИБ | 49 |
| 4.1 Организационные меры обеспечения ИБ | 49 |
| 4.2 Технические меры обеспечения ИБ | 50 |
| 5 Методика проведения оценки соответствия | 52 |
| 6 Результаты оценки соответствия | 54 |
| 6.1 Исключения из области оценки | 54 |
| 6.2 Обоснование применения компенсирующих мер | 55 |
| 6.3 Неразрешенные разногласия между проверяющей группой и проверяемой организацией | 55 |
| 6.4 Результаты оценки соответствия | 56 |



СТРУКТУРА ОТЧЕТА

| | |
|--|-----|
| 7 Заключение | 58 |
| Приложение 1. Сводные результаты оценки соответствия | 59 |
| Процесс 1 «Обеспечение защиты информации при управлении доступом»..... | 59 |
| Подпроцесс «Управление учетными записями и правами субъектов логического доступа» | 59 |
| Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» | 66 |
| Подпроцесс «Защита информации при осуществлении физического доступа»..... | 75 |
| Подпроцесс «Идентификация и учет ресурсов и объектов доступа» | 78 |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | 80 |
| Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей».... | 80 |
| Подпроцесс «Выявление вторжений и сетевых атак» | 86 |
| Подпроцесс «Защита информации, передаваемой по вычислительным сетям» | 89 |
| Подпроцесс «Защита беспроводных сетей» | 90 |
| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | 93 |
| Процесс 4 «Защита от вредоносного кода» | 103 |
| Процесс 5 «Предотвращение утечек информации» | 108 |
| Процесс 6 «Управление инцидентами защиты информации» | 114 |
| Подпроцесс «Мониторинг и анализ событий защиты информации»..... | 114 |
| Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них» | 117 |
| Процесс 7 «Защита среды виртуализации» | 123 |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | 132 |
| Организация и управление системой защиты информации..... | 137 |
| Защита информации на этапах жизненного цикла автоматизированных систем и приложений | 158 |
| Приложение 2. Заполненные листы сбора свидетельств оценки соответствия..... | 169 |
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | 170 |
| Подпроцесс «Управление учетными записями и правами субъектов логического доступа» | 170 |
| Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» | 178 |
| Подпроцесс «Защита информации при осуществлении физического доступа» | 187 |
| Подпроцесс «Идентификация и учет ресурсов и объектов доступа» | 190 |
| Организация и управление защитой информации (Процесс 1) | 192 |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | 203 |
| Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей».... | 203 |
| Подпроцесс «Выявление вторжений и сетевых атак» | 207 |
| Подпроцесс «Защита информации, передаваемой по вычислительным сетям» | 209 |
| Организация и управление защитой информации (Процесс 2) | 211 |
| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | 221 |
| Организация и управление защитой информации (Процесс 3) | 231 |
| Процесс 4 «Защита от вредоносного кода» | 240 |
| Организация и управление защищенной информацией (Процесс 4) | 245 |
| Процесс 5 «Предотвращение утечек информации» | 255 |
| Организация и управление защищенной информацией (Процесс 5) | 260 |
| Процесс 6 «Управление инцидентами защиты информации» | 270 |
| Подпроцесс «Мониторинг и анализ событий защиты информации»..... | 270 |
| Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них» | 273 |
| Организация и управление защищенной информацией (Процесс 6) | 277 |
| Процесс 7 «Защита среды виртуализации» | 288 |
| Организация и управление защищенной информацией (Процесс 7) | 293 |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | 303 |
| Организация и управление защищенной информацией (Процесс 8) | 306 |
| Защита информации на этапах жизненного цикла автоматизированных систем и приложений | 316 |
| Приложение 3. Перечень выявленных нарушений | 326 |
| Приложение 4. Перечень оценок, характеризующих выбор финансовой организацией мер защиты информации | 327 |
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | 327 |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | 334 |
| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | 339 |
| Процесс 4 «Защита от вредоносного кода» | 342 |
| Процесс 5 «Предотвращение утечек информации» | 344 |
| Процесс 6 «Управление инцидентами защиты информации» | 347 |
| Процесс 7 «Защита среды виртуализации» | 350 |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | 355 |
| Защита информации на этапах жизненного цикла автоматизированных систем и приложений | 357 |
| Направление 1 «Планирование процесса системы защиты информации» | 360 |
| Направление 2 «Реализация процесса системы защиты информации» | 362 |
| Направление 3 «Контроль процесса системы защиты информации» | 365 |
| Направление 4 «Совершенствование процесса системы защиты информации» | 367 |
| Приложение 5. Рекомендации по устранению несоответствий | 370 |
| Приложение 6. Описи документов и машинных носителей информации | 376 |
| Контактная информация | 377 |



Результаты оценки соответствия

| Уровень защиты информации для оцениваемого контура безопасности (заполняется вручную для автогенерации применимых требований) | | | | | | | 2 |
|--|--|----------------------------------|--------------------------------|------------------------------|---------------------------------------|---|---|
| Результаты итоговой оценки соответствия требованиям ГОСТ Р 57580.1 | | | | | | | |
| Наименование процесса системы ЗИ, направления ЗИ | Оценка, характеризующая выбор организационных и технических мер системы ЗИ | Планирование процесса системы ЗИ | Реализация процесса системы ЗИ | Контроль процесса системы ЗИ | Совершенствование процесса системы ЗИ | Качественная оценка уровня соответствия процесса системы ЗИ | Числовое значение оценки соответствия процесса системы ЗИ |
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | 0,93 | 0,50 | 0,82 | 1,00 | 1,00 | Четвертый | 0,88 |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | 1,00 | 0,60 | 0,95 | 1,00 | 1,00 | Пятый | 0,95 |
| Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры» | 0,78 | 0,60 | 0,95 | 1,00 | 1,00 | Третий | 0,84 |
| Процесс 4 «Защита от вредоносного кода» | 0,96 | 0,60 | 0,95 | 1,00 | 1,00 | Пятый | 0,93 |
| Процесс 5 «Предотвращение утечек информации» | 0,79 | 0,60 | 0,91 | 1,00 | 1,00 | Третий | 0,83 |
| Процесс 6 «Управление инцидентами защиты информации» | 0,89 | 0,50 | 0,82 | 1,00 | 1,00 | Четвертый | 0,86 |
| Процесс 7 «Защита среди аиртуализации» | 0,87 | 0,50 | 0,82 | 1,00 | 1,00 | Третий | 0,85 |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | 0,83 | 0,60 | 0,86 | 1,00 | 1,00 | Третий | 0,85 |
| Применение организационных и технических мер ЗИ на этапах жизненного цикла АС | | | | | | | 0,93 |
| Количество нарушений ЗИ, выявленных в результате оценки соответствия ЗИ | | | | | | | 0 |
| Итоговая оценка соответствия ЗИ | | | | | | | 0,88 |
| Уровень соответствия | | | | | | | Четвертый |

| ID | Требование | Реализация | Оценка | Способ реализации |
|-------|--|------------|--------|-------------------|
| УЗП.1 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями | | 0 | Т |
| УЗП.2 | Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа | | 1 | О |
| УЗП.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 |

Сводные результаты оценки соответствия



ЗАПОЛНЕННЫЕ ЛИСТЫ СБОРА СВИДЕТЕЛЬСТВ

Приложение 2. Заполненные листы сбора свидетельств оценки соответствия

| № п/п | Должность | Фамилия, инициалы | Процессы | Подпись | Дата |
|---|-----------|----------------------|----------|---------|------|
| Сотрудники проверяемой организации, предоставившие свидетельства оценки соответствия ЗИ | | | | | |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |



Рекомендации по устранению несоответствий

| Цвет | Степень (уровень) сложности устранения | Описание |
|-----------|--|---|
| Зеленый | Первый уровень | Несоответствие может быть устранено путем минимального изменения (внедрения) организационных или технических мер |
| Оранжевый | Второй уровень | Несоответствие может быть устранено путем существенного изменения (внедрения) организационных или технических мер |

| № п/п | Выявленное несоответствие | Мера ГОСТ 57580.1 | Рекомендации по устранению выявленных несоответствий |
|---|---|-------------------|--|
| Реализация процессов защиты информации | | | |
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | | | |
| Подпроцесс «Управление учетными записями и правами субъектов логического доступа» | | | |
| Первый уровень | | | |
| 1. | Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа осуществляется сотрудниками ДИБ в рамках проведения аудитов в АС в течение года. На постоянной основе контроль не осуществляется | уэП.9 | |
| Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа» | | | |
| Первый уровень | | | |

| № | Наименование | Файлы | Хэш-функция ³¹ |
|--------------------|--------------|------------------------|--|
| 1 | Диск DVD-R | Свидетельства_ГОСТ.zip | 858852D304C2E4C5E4856E5697C0F1F 01D76A83996853D3C6EB618753C674 B0C2BD091DCF44CDA2E64951D220C 3E3DF00E35019E9ECDBF558850566F |
| Всего носителей: 1 | | | |

Опись машинных
носителей
информации



ФОРМА ОКУД 0409071

Сведения
об оценке выполнения кредитными организациями
требований к обеспечению защиты информации

по состоянию на "**.**.2023" г.

Полное или сокращенное фирменное наименование кредитной организации: Акционерное
общество «***»

Адрес (местонахождения) кредитной организации: Российская Федерация, ***

Код формы по ОКУД 0409071

На нерегулярной основе

Раздел 1. Сведения об оценке соответствия защиты информации в рамках направления
«Технологические меры»

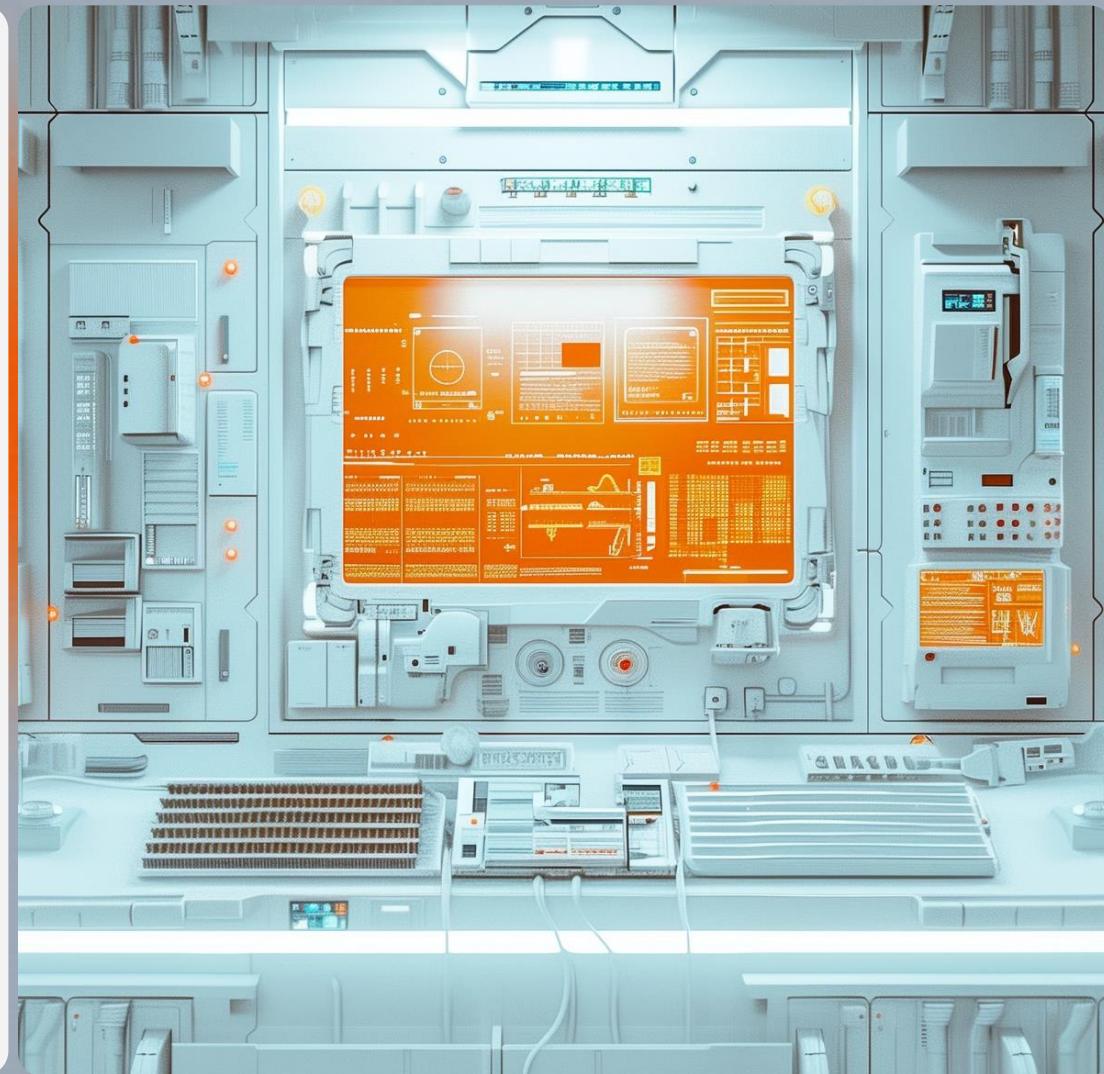
| Номер строки | Направление деятельности | Вид деятельности | Вид оценки | Значение оценки |
|--------------|--------------------------|------------------|------------|-----------------|
| 1 | 2 | 3 | 4 | 5 |
| 1. | N 683-П | Банк | Етмп | 0,98 |
| 2. | N 683-П | Банк | Етмр | 0,92 |
| 3. | N 683-П | Банк | Етмк | 1,00 |
| 4. | N 683-П | Банк | Етмс | 1,00 |
| 5. | N 683-П | Банк | Етм | 0,97 |
| 6. | N 719-П | ОПДС | Етмп | 0,86 |
| 7. | N 719-П | ОПДС | Етмр | 1,00 |

| Номер строки | Направление деятельности | Вид деятельности | Процесс системы защиты информации | Направление защиты информации | Значение оценки |
|--|--------------------------|------------------|-----------------------------------|-------------------------------|-----------------|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 56. | N 683-П | Банк | 8 | Уровень соответствия | Третий |
| 57. | N 683-П | Банк | - | Еас | 0,93 |
| Итоговая оценка соответствия с учетом выявленных нарушений защиты информации | | | | | |
| Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z | | | | | 0 |
| Итоговая оценка соответствия, R | | | | | 0,88 |
| 58. | N 719-П | ОПДС | 1 | Етмз | 0,93 |
| 59. | N 719-П | ОПДС | 1 | Ел | 0,50 |
| 60. | N 719-П | ОПДС | 1 | Ер | 0,82 |



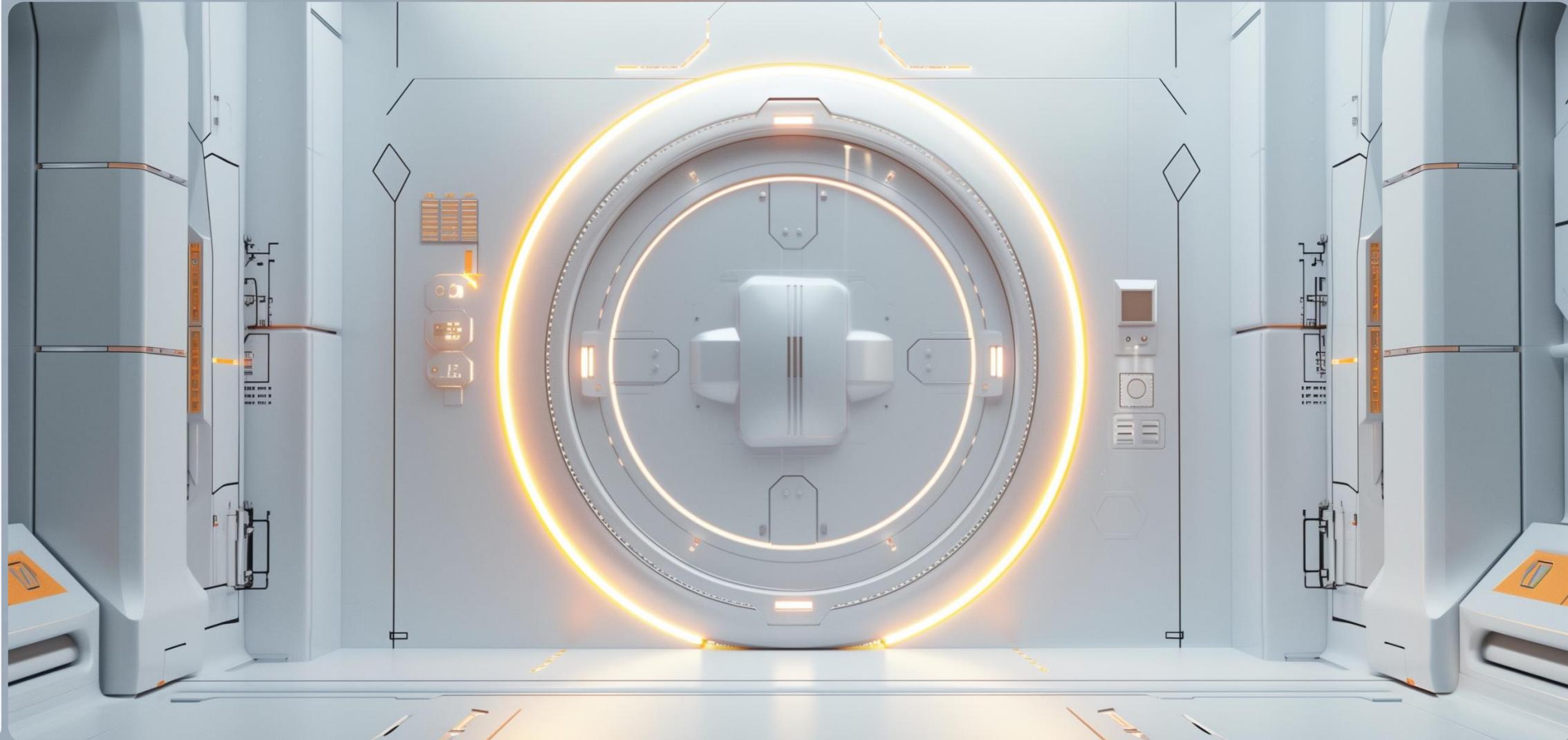
ОСНОВНЫЕ СЛОЖНОСТИ

- Согласование отчета
- Подписание отчета
- Отправка результатов оценки соответствия в ЦБ





КАК ТРАКТОВАТЬ ОТДЕЛЬНЫЕ ТРЕБОВАНИЯ ГОСТ



ANGARA SECURITY

СПАСИБО ЗА ВНИМАНИЕ!



www.angarasecurity.ru

+7 (495) 269-26-06

121096, г. Москва, ул. Василисы
Кожиной, д.1, к.1 БЦ «Парк Победы»

