

Секреты безопасности: комплаенс и информационная безопасность в банковском мире

10.10.23

Александр Мизерин

3

2

1

Немного о себе

Работаю в Отделе ИБ Яндекса:



Немного о себе

Работаю в Отделе ИБ Яндекса:

- Окончил МГТУ «Станкин» в 2019 году, степень магистр



Немного о себе

Работаю в Отделе ИБ Яндекса:

- Окончил МГТУ «Станкин» в 2019 году, степень магистр
- Опыт работы в кредитно-финансовых организациях с 2017 года



Немного о себе

Работаю в Отделе ИБ Яндекса:

- Окончил МГТУ «Станкин» в 2019 году, степень магистр
- Опыт работы в кредитно-финансовых организациях с 2017 года
- Имею соответствующие сертификации в области ИБ (ISO 27001:2022; PCI DSS; ГОСТ 57580 и т.д.)



Немного о себе

Работаю в Отделе ИБ Яндекса:

- Окончил МГТУ «Станкин» в 2019 году, степень магистр
- Опыт работы в кредитно-финансовых организациях с 2017 года
- Имею соответствующие сертификации в области ИБ (ISO 27001:2022; PCI DSS; ГОСТ 57580 и т.д.)
- Занимаюсь комплаенсом ИБ в Финтехе Яндекса уже 1,5 года



Введение

Введение

Информационная безопасность становится все более актуальной для всех видов организаций, особенно для банков.

Введение

Информационная безопасность становится все более актуальной для всех видов организаций, особенно для банков.

Банки обрабатывают невероятное количество конфиденциальных данных, которые должны быть надежно защищены.

Введение

Информационная безопасность становится все более актуальной для всех видов организаций, особенно для банков.

Банки обрабатывают невероятное количество конфиденциальных данных, которые должны быть надежно защищены.

Мы разберем основные аспекты комплаенса, его необходимость для банков и пути его применения.



Опыт Финтеха Яндекса



Опыт Финтеха Яндекса

- Команда Compliance помогает сервисам Финтеха выстраивать процессы, чтобы они соответствовали стандартам информационной безопасности



Опыт Финтеха Яндекса

- Команда Compliance помогает сервисам Финтеха выстраивать процессы, чтобы они соответствовали стандартам информационной безопасности
- В первую очередь мы заботимся о реальной безопасности наших сервисов и снижении рисков



Опыт Финтеха Яндекса

- Команда Compliance помогает сервисам Финтеха выстраивать процессы, чтобы они соответствовали стандартам информационной безопасности
- В первую очередь мы заботимся о реальной безопасности наших сервисов и снижении рисков
- Финтех быстро растет и меняется, стремится использовать передовые технологии, а мы помогаем гибко настроить процессы под развитие бизнеса



Чем выгоден комплаенс ИБ в Банках?

Чем выгоден комплаенс ИБ в Банках?

Применение комплаенса в информационной безопасности может принести множество преимуществ, таких как:

Чем выгоден комплаенс ИБ в Банках?

Применение комплаенса в информационной безопасности может принести множество преимуществ, таких как:

01

Соответствие
требованиям
регуляторов и
законодательству

Чем выгоден комплаенс ИБ в Банках?

Применение комплаенса в информационной безопасности может принести множество преимуществ, таких как:

01

Соответствие
требованиям
регуляторов и
законодательству

02

Драйвер
развития ИБ

Чем выгоден комплаенс ИБ в Банках?

Применение комплаенса в информационной безопасности может принести множество преимуществ, таких как:

01

Соответствие требованиям регуляторов и законодательству

02

Драйвер развития ИБ

03

Создание культуры безопасности

Чем же помогает комплаенс в Банках?

86-ФЗ, 149-ФЗ,
152-ФЗ, 161-ФЗ,
187-ФЗ, 482-ФЗ



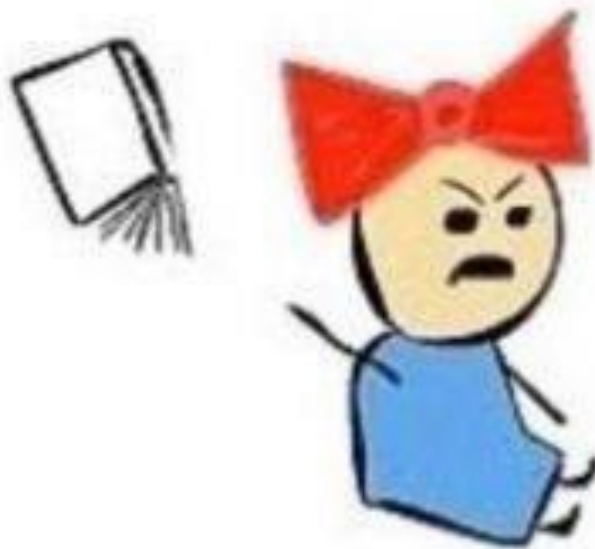
ПП 676, ПП 1119, ПП 127,
683-П, 716-П, 719-П,
802-П, 779-П, 787-П



Приказ ФСТЭК: 17, 21, 31, 55,
75, 76, 235, 236, 239; Приказ
ФСБ: 66, 196, 281, 282, 366,
ГОСТ 57580.х, 15408, 56939,
50922



... буду художницей



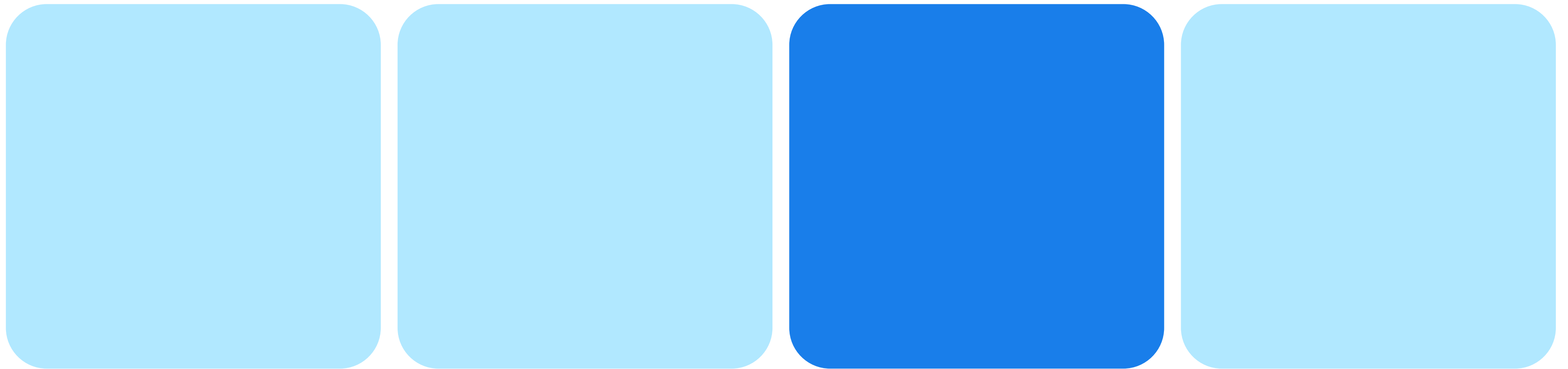
Соответствовать
законодательству
и регулятивным
положениям

Контролировать выполнение требований

Защищать данные и
конфиденциальную
информацию

Улучшать
репутацию и
доверие со
СТОРОНЫ КЛИЕНТОВ

Что делать, если нет возможности нанять специалиста в штат?



Что делать, если нет возможности нанять специалиста в штат?

Пользоваться
услугами
аутсорсинга

Что делать, если нет возможности нанять специалиста в штат?

Пользоваться
услугами
аутсорсинга

Инвестировать
в обучение
текущего
персонала

Что делать, если нет возможности нанять специалиста в штат?

Пользоваться
услугами
аутсорсинга

Инвестировать
в обучение
текущего
персонала

Использовать
автоматизацию

Что делать, если нет возможности нанять специалиста в штат?

Пользоваться
услугами
аутсорсинга

Инвестировать
в обучение
текущего
персонала

**Использовать
автоматизацию**

Соответствовать
актуальным
тенденциям
безопасности

А что же у нас?

А что же у нас?

Команда Безопасности Финтеха постоянно растет и включает такие команды, как:

А что же у нас?

Команда Безопасности Финтеха постоянно растет и включает такие команды, как:

01

Отдел инженеров
безопасности

А что же у нас?

Команда Безопасности Финтеха постоянно растет и включает такие команды, как:

01

Отдел инженеров
безопасности

02

Отдел
методологии и
аудита

А что же у нас?

Команда Безопасности Финтеха постоянно растет и включает такие команды, как:

01

Отдел инженеров
безопасности

02

Отдел
методологии и
аудита

03

Отдел
мониторинга и
реагирования на
инциденты

А что же у нас?

Команда Безопасности Финтеха постоянно растет и включает такие команды, как:

01

Отдел инженеров
безопасности

02

Отдел
методологии и
аудита

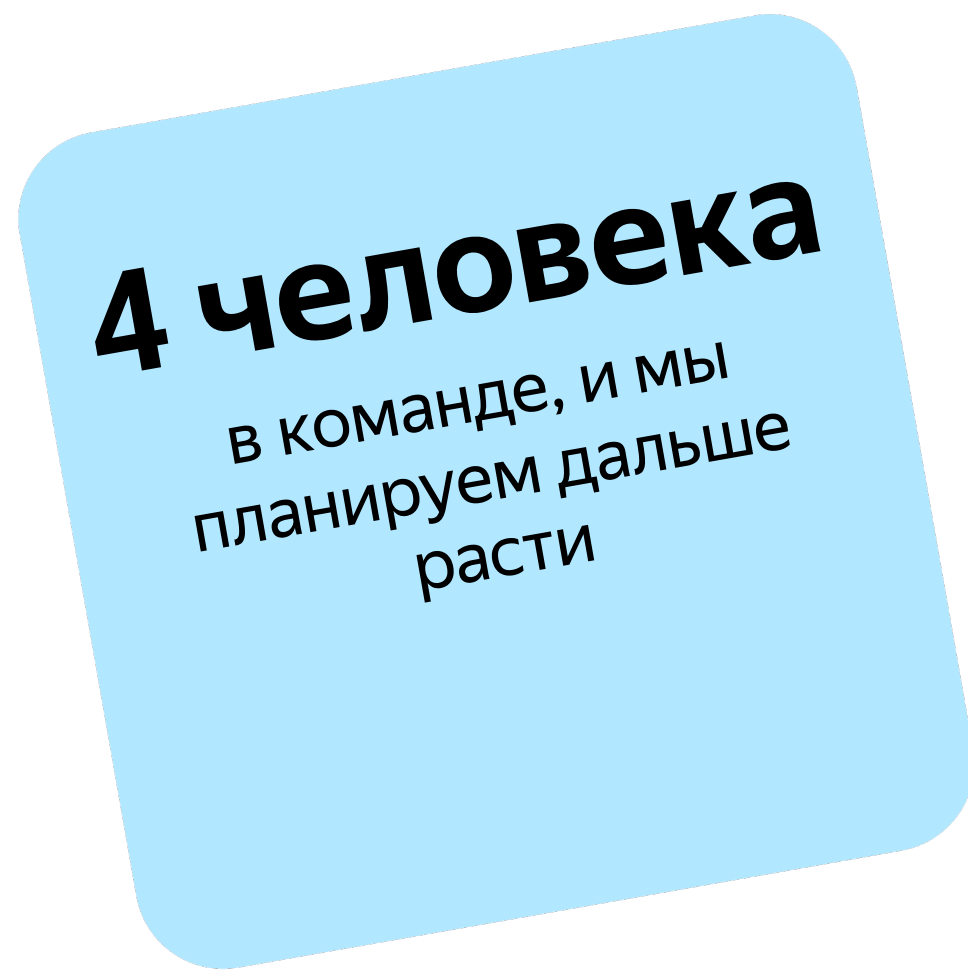
03

Отдел
мониторинга и
реагирования на
инциденты

04

Отдел ИБ

Комплаенс Финтеху Яндекса



Комплаенс Финтеху Яндекса

4 человека

в команде, и мы
планируем дальше
расти

~12

**аудитов в
ГОД**

Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеха Яндекса

4 человека

в команде, и мы
планируем дальше
расти

~12

**аудитов в
год**

Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеха Яндекса включает себя направления работы:

- Методология

Комплаенс Финтеху Яндекса

4 человека

в команде, и мы
планируем дальше
расти

~12

**аудитов в
год**

Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеху Яндекса включает себя направления работы:

- Методология
- Управление рисками ИБ

Комплаенс Финтеху Яндекса

4 человека

в команде, и мы
планируем дальше
расти

**~12
аудитов в
год**

Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеху Яндекса включает себя направления работы:

- Методология
- Управление рисками ИБ
- Контроль соблюдения нормативных требований

Комплаенс Финтеху Яндекса

4 человека

в команде, и мы
планируем дальше
расти

**~12
аудитов в
год**

Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеху Яндекса включает себя направления работы:

- Методология
- Управление рисками ИБ
- Контроль соблюдения нормативных требований
- Обучение и осведомленность

Комплаенс Финтеху Яндекса

4 человека

в команде, и мы
планируем дальше
расти

**~12
аудитов в
год**

Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеху Яндекса включает себя направления работы:

- Методология
- Управление рисками ИБ
- Контроль соблюдения нормативных требований
- Обучение и осведомленность
- Взаимодействие с внешними сторонами

Комплаенс Финтеха Яндекса

4 человека

в команде, и мы
планируем дальше
расти

**~12
аудитов в
год**

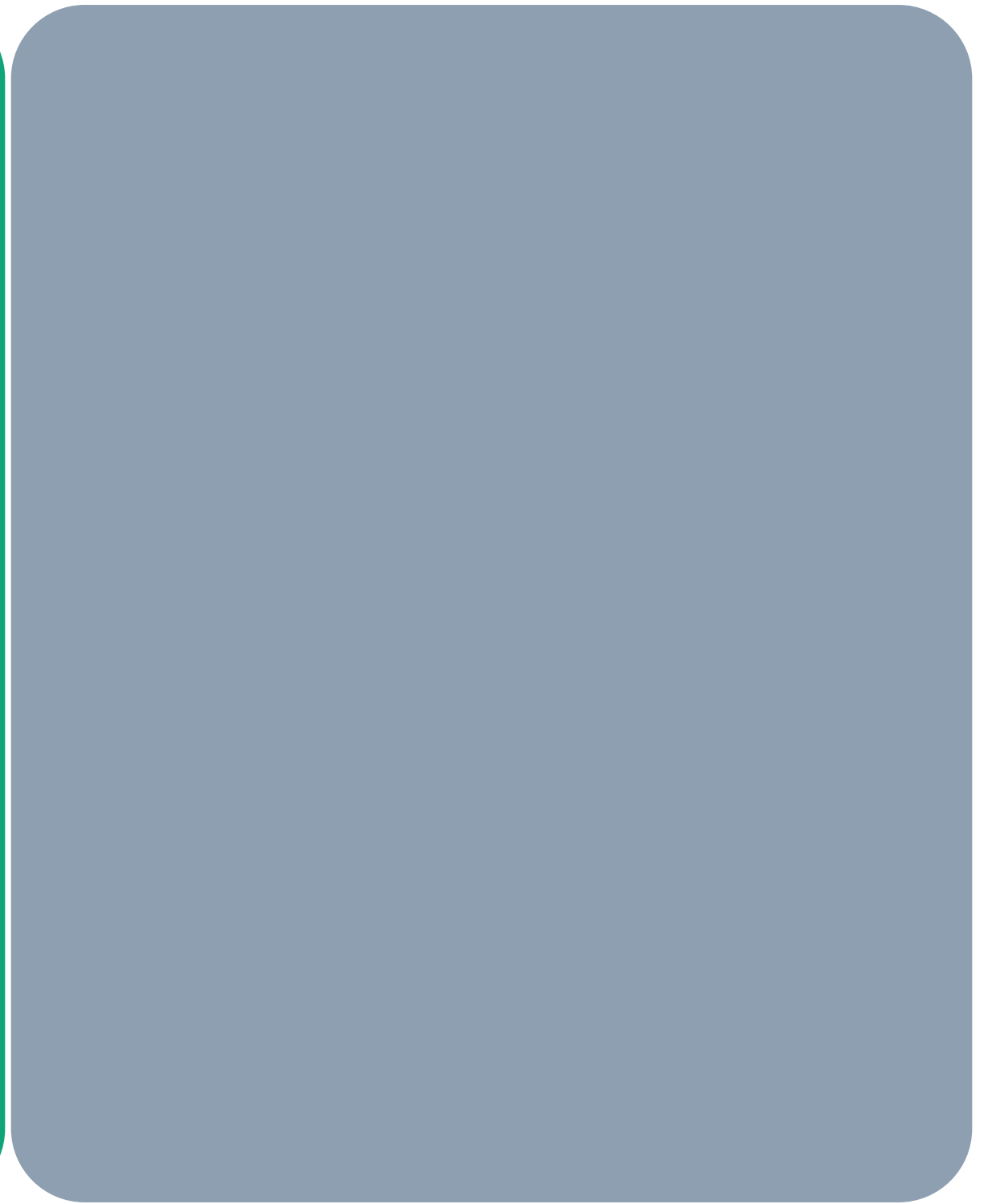
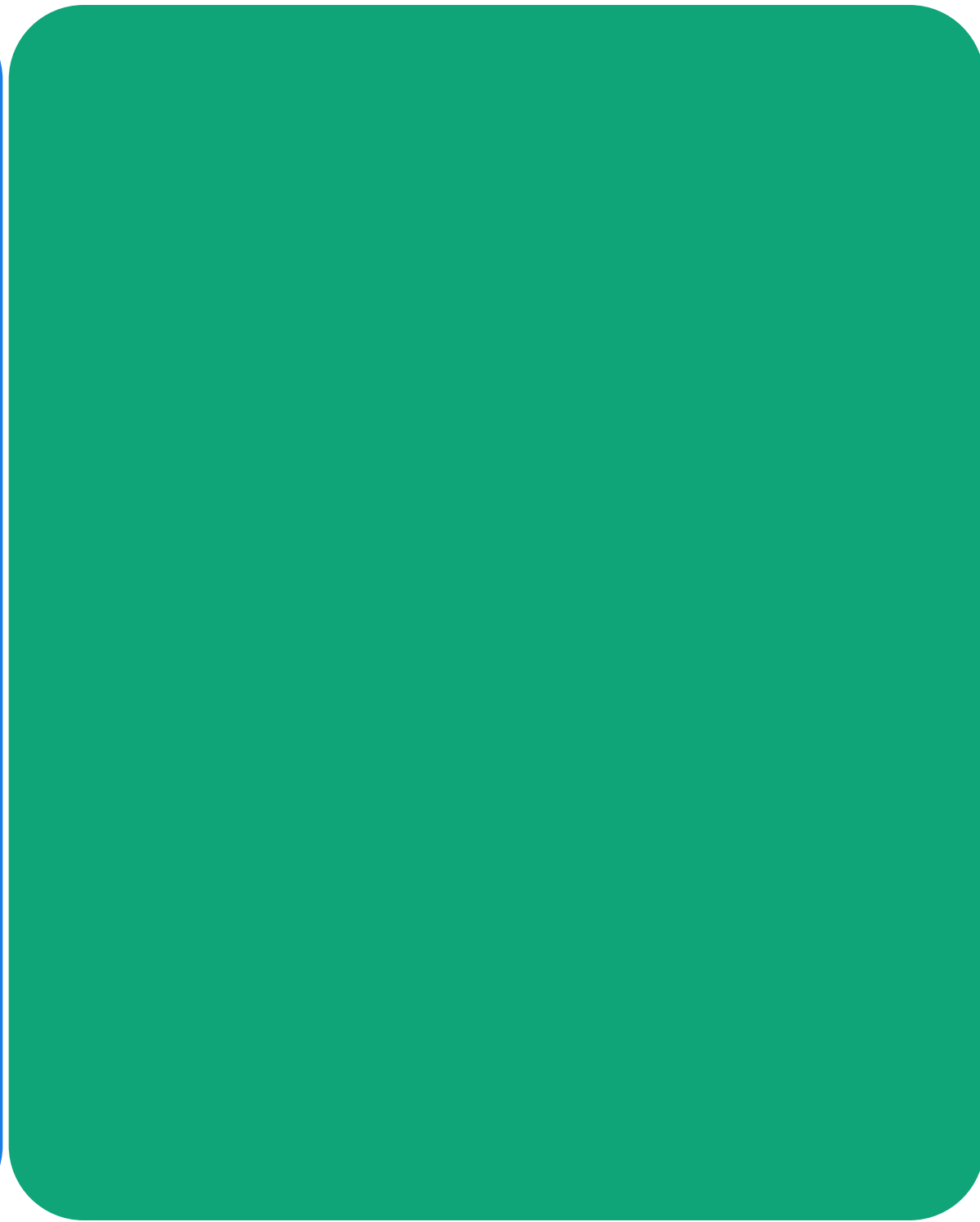
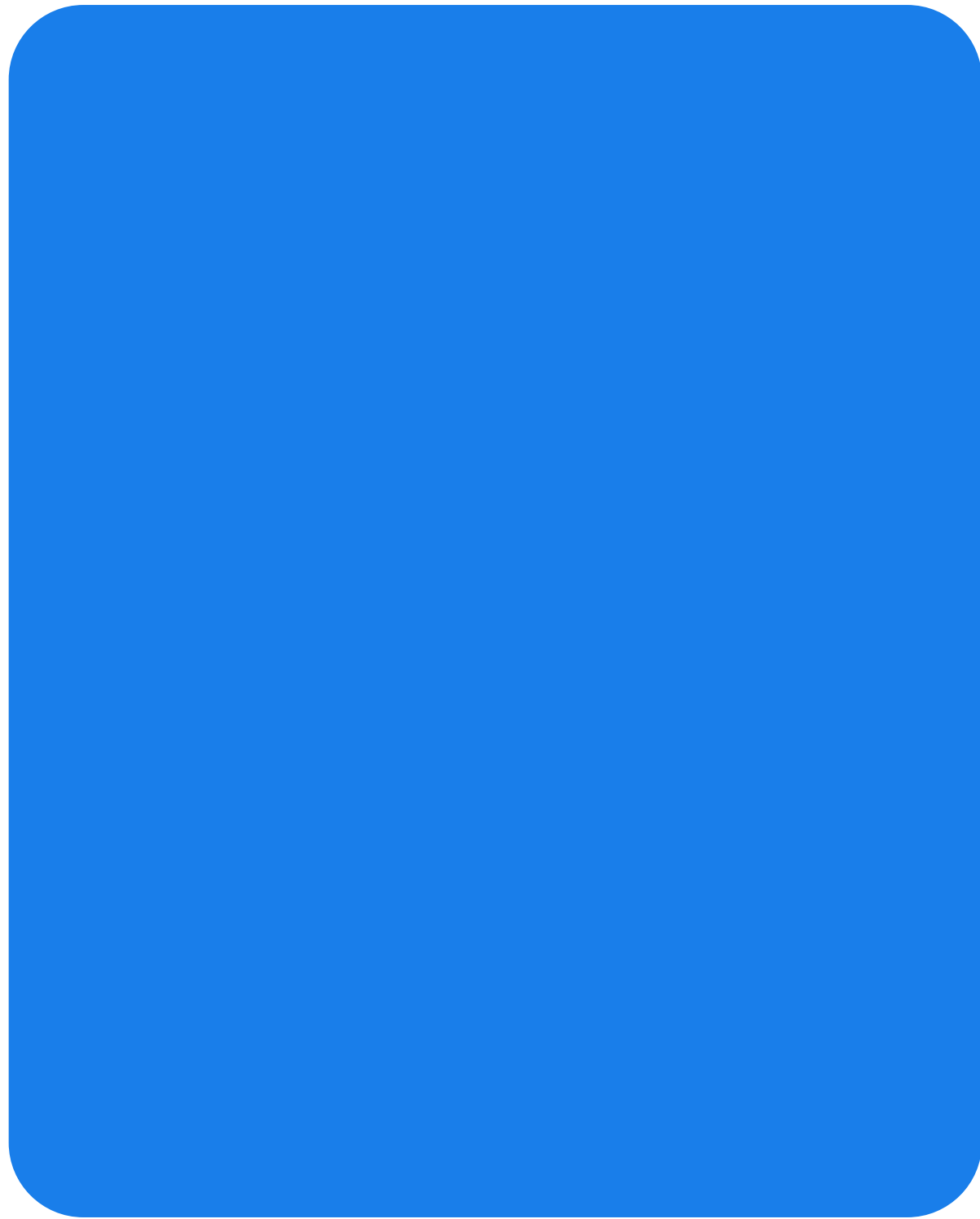
Включает в себя
внешние и
внутренние аудиты,
и это не предел =)

Комплаенс Финтеха Яндекса включает себя направления работы:

- Методология
- Управление рисками ИБ
- Контроль соблюдения нормативных требований
- Обучение и осведомленность
- Взаимодействие с внешними сторонами
- Аудит



Три линии контроля ИБ



Три линии контроля ИБ

Операционный уровень

01

Включает в себя
руководителей и
менеджеров подразделений,
которые являются
владельцами рисков и
осуществляют операционные
процессы

Три линии контроля ИБ

Операционный уровень

01

Включает в себя руководителей и менеджеров подразделений, которые являются владельцами рисков и осуществляют операционные процессы

Функциональный уровень

02

Играет вспомогательную и координирующую роль, помогают первой линии управляя рисками и контролем

Три линии контроля ИБ

Операционный уровень

01

Включает в себя руководителей и менеджеров подразделений, которые являются владельцами рисков и осуществляют операционные процессы

Функциональный уровень

02

Играет вспомогательную и координирующую роль, помогают первой линии управляя рисками и контролем

Внутренний аудит

03

Является независимой и объективной функцией, которая является целью оценки эффективности системы управления рисками, корпоративного управления и контроля

Регулярные процедуры

Регулярные процедуры

Фиксируем списки контролей, их владельцев и регулярность по обязательным контрольным мероприятиям с помощью Yandex Tracker

Регулярные процедуры

Фиксируем списки контролей, их владельцев и регулярность по обязательным контрольным мероприятиям с помощью Yandex Tracker

⌵

⌵

🔍

☰

📎

🔗

📄

🗃

🕒

+

✖

🔔

?

⚙

⚙

▶

Банк. Вопросы ИБ /

📄

☆

Регулярные процедуры

В работу

Нужна информация

Заккрыть

Не будет исправлено

Зонтичный Тикет для фиксации и учета списка контролей, их владельцев и регулярности по обязательным контрольным мероприятиям.

📎

 Прикрепить файлы

📄

 Добавить чеклист

Связи с другими задачами 29 ^

+ Добавить связь

Ключ	Задача	Статус	Исполнитель	Обновлено	⚙
Блокирует 1					
👑	Задачи Compliance в рамках Финтеха	Открыт		10 авг, 12:40	
+ Добавить					
Зависит от 18					
👑	(semiannual) Проверка контура СПФС	Открыт	Александр Мизерин	30 авг, 14:46	
👑	(semiannual) Плановый пересмотр корректности разделения систем по скоупам	Открыт	Александр Мизерин	21 авг, 12:43	
👑	(semiannual) Пересмотр матриц конфликтных полномочий	Открыт		21 авг, 12:43	
👑	(quarterly) Актуализация схем БП и потоков данных	Открыт		21 авг, 12:43	
👑	(semiannual) Актуализация схемы сети и перечня компонентов в скоупе PCI DSS	Открыт		21 авг, 12:43	
👑	(quarterly) Выявление несанкционированных точек доступа	Открыт		26 сент, 13:44	
👑	(yearly) Проведение сертификационного QSA-аудита.	Открыт		21 авг, 12:50	
👑	(yearly) План обучения	Открыт	Александр Мизерин	21 авг, 12:43	
👑	(yearly) Контроль поставщиков услуг	Открыт		02 сент, 13:43	
👑	(yearly) Пересмотр и обновление ВНД	Открыт	Александр Мизерин	21 авг, 12:44	
👑	(yearly) Смена ключей шифрования ДПК	Открыт		21 авг, 12:44	

Некоторым сотрудникам

👤 Действия

Статус

Открыт

Тип

👑 Epic

Приоритет

= Средний

Дедлайн

—

Цели

Автор

Исполнитель

Назначить меня

Наблюдатели

Александр Мизерин

ещё 3

Проект

—

Теги

—

Компоненты

—

Исправить в версиях

—

Доски

—

Нужен ответ пользователя

Александр Мизерин

> Agile

> Безопасность

+ Изменить список параметров

▼

Проведение внутренних аудитов

Проведение внутренних аудитов

- Определяем методику проведения аудитов и делаем понятные для всех чек-листы

Проведение внутренних аудитов

- Определяем методику проведения аудитов и делаем понятные для всех чек-листы
- Составляем понятный план проведения аудитов и определяем, где могут быть слабые стороны

Проведение внутренних аудитов

- Определяем методику проведения аудитов и делаем понятные для всех чек-листы
- Составляем понятный план проведения аудитов и определяем, где могут быть слабые стороны
- Проводя аудиты, мы в контексте того, что происходит на том или ином контуре Банка

Проведение внутренних аудитов

- Определяем методику проведения аудитов и делаем понятные для всех чек-листы
- Составляем понятный план проведения аудитов и определяем, где могут быть слабые стороны
- Проводя аудиты, мы в контексте того, что происходит на том или ином контуре Банка
- По результатам проверок даем рекомендацию по устранению недостатков и точно работаем с коллегами по их устранению

Проведение внутренних аудитов

- Определяем методику проведения аудитов и делаем понятные для всех чек-листы
- Составляем понятный план проведения аудитов и определяем, где могут быть слабые стороны
- Проводя аудиты, мы в контексте того, что происходит на том или ином контуре Банка
- По результатам проверок даем рекомендацию по устранению недостатков и точно работаем с коллегами по их устранению

Банк. Вопросы ИБ

★

[СПФС] Проверка контура Н2 2023

Предоставить информацию

Заккрыть

Не будет исправлено

Привет!

03.04.2023 года проведена проверка выполнения требований (контролей) по защите информации на участке системы передачи финансовых сообщений Банка России (далее - участок СПФС), в соответствии с требованиями, содержащимися в Условиях по защите информации (УпЗИ) и ГОСТ 57580.1 - 2017 (ГОСТ).

В ХОДЕ ПРОВЕРКИ ПРИМЕНЯЛИСЬ СЛЕДУЮЩИЕ ПРОЦЕДУРЫ:

• проверка помещения N, в котором располагаются автоматизированные рабочие места, относящиеся к участку СПФС (АРМ 1 [0.0.0.0], АРМ 2 [0.0.1.1], в котором осуществляют свою деятельность работники [Отдел N](#) (Попова С.А., Степанова К.О., Кирсанова И.Ю., Иногородняя Н.Ю.);

• настройки средств защиты информации, в том числе средств криптографической защиты информации, функционирующих на участке СПФС;

• проверка автоматизированных рабочих мест участка СПФС;

• полнота и качество документирования участка СПФС.

РЕЗУЛЬТАТЫ ПРОВЕРКИ:

На участке СПФС были проверены 379 контрольных показателя. Сводная оценка степени выполнения контролей на участке СПФС приведена в таблице:

Кол-во показателей с полным выполнением требований (оценка - 1)	Кол-во показателей с частичным выполнением требований (оценка - 0,5)	Кол-во показателей с полным невыполнением (оценка - 0)	Кол-во неопениваемых показателей (оценка - н/о)
N	N	N	N

МЕРОПРИЯТИЯ ПО УСТРАНЕНИЮ ВЫЯВЛЕННЫХ НЕСООТВЕТСТВИЙ:

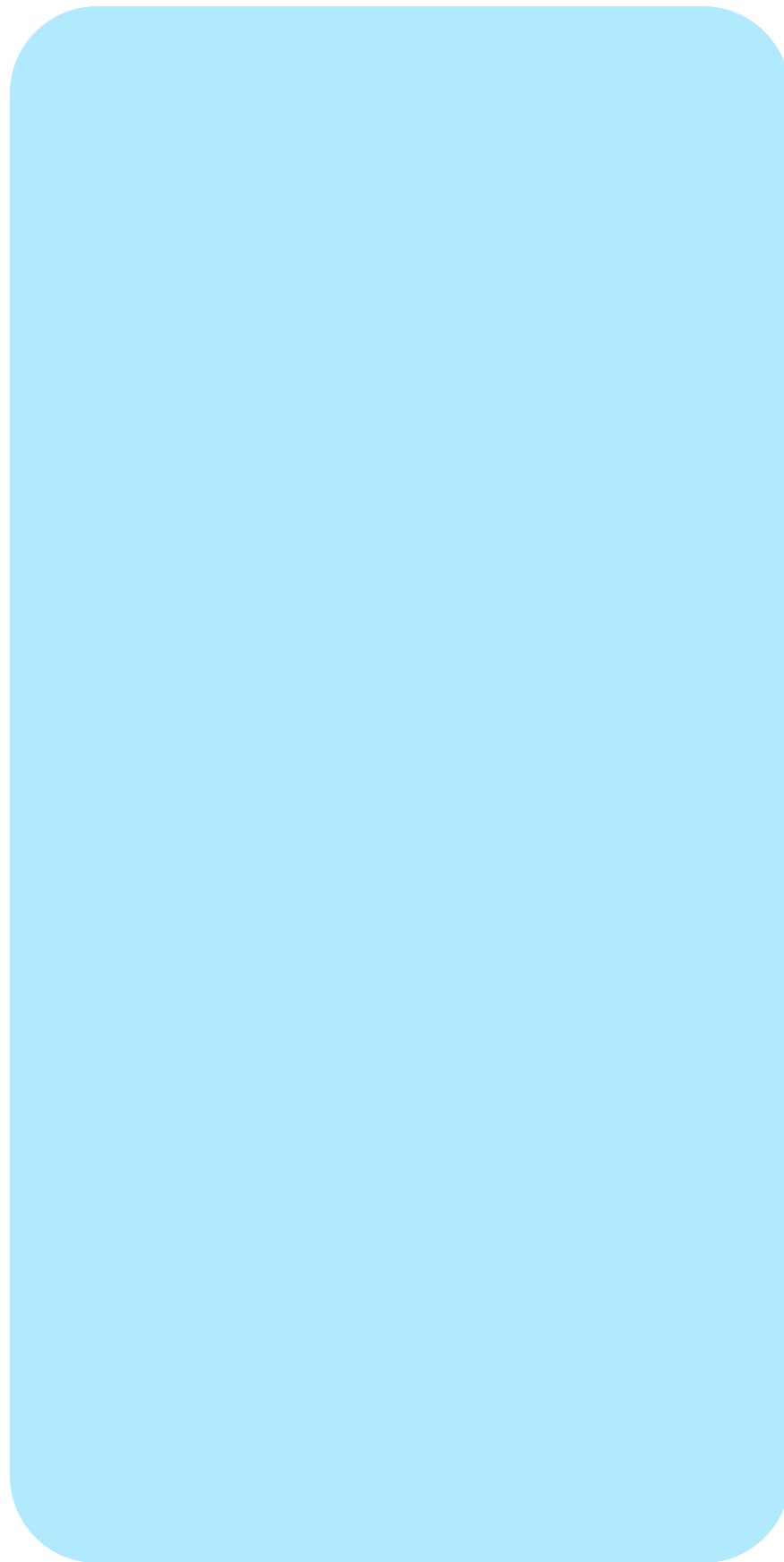
№ п/п	Несоответствие	Что нужно сделать:	Тикет:	Ответственный:	Статус исправления:
1.	ГОСТ: Требование 1 Требование 2 Требование 3	N	Требуется информация [СПФС] Устранение недостатков по	Илья Островский Александр Иванов	
2.	ГОСТ: Требование 1 Требование 2	Реализовать организационную меру в виде контрольных процедур: Соответствию Приказу	Открыт [СПФС] Устранение недостатков по организационным мерам	Александр Мухомов	

Свод требований стандартов

Свод требований стандартов

Наименование блока/направления	Наименование требования	Пункт требования в ГОСТ 57580 Ур.1	Пункт требования в PCI DSS	Пункт требования в приказе ФСТЭК 21	Пункт положения 683-П	Пункт положения 719-П	Пункт положения 802-П	Пояснение
Обеспечение защиты информации при управлении доступом	Осуществление логического доступа (ЛД) пользователями и эксплуатационным персоналом (ЭП) под уникальными и персонифицированными учетными записями	УЗП.1	7.1.1, 8.2.1	ИАФ.1, ИАФ.6	Отсутствует	2.9	Отсутствует	
Обеспечение защиты информации при управлении доступом	Контроль соответствия фактического состава разблокированных учетных записей(УЗ) фактическому составу легальных субъектов ЛД	УЗП.2	7.2.4	УПД.1, АНЗ.5	Отсутствует	Отсутствует	Отсутствует	
Обеспечение защиты информации при управлении доступом	Контроль отсутствия незаблокированных УЗ уволенных работников; работников, отсутствующих на рабочем месте более 90 календарных дней; работников внешних (подрядных) организаций, прекративших свою деятельность в организации	УЗП.3	7.2.4, 8.2.5	УПД.1, АНЗ.5	Отсутствует	Отсутствует	Отсутствует	Контроль реализуется через процедуру аннулирования доступа для прекращенных пользователей
Обеспечение защиты информации при управлении доступом	Контроль отсутствия незаблокированных УЗ неопределенного целевого назначения	УЗП.4	7.2.2	УПД.1, АНЗ.5	Отсутствует	Отсутствует	Отсутствует	
Обеспечение защиты информации при управлении доступом	Документарное определение правил предоставления (отзыва) и блокирования ЛД	УЗП.5	7.1.1, 7.2.3	УПД.5	Отсутствует	Отсутствует	7.1	
Обеспечение защиты информации при управлении доступом	Назначение для всех ресурсов доступа распорядителя ЛД (владельца ресурса доступа)	УЗП.6	7.1.2, 7.2.2	УПД.2	Отсутствует	Отсутствует	Отсутствует	
Обеспечение защиты информации при управлении доступом	Предоставление прав ЛД по решению распорядителя ЛД (владельца ресурса доступа)	УЗП.7	7.2.3	УПД.2	Отсутствует	Отсутствует	Отсутствует	

Выводы



Объединение
общих усилий
сотрудников Банка
поможет достичь
высокого уровня
ИБ

Объединение
общих усилий
сотрудников Банка
поможет достичь
высокого уровня
ИБ

Информационная
безопасность
является одним из
основных
приоритетов
любого
современного
банка

Объединение
общих усилий
сотрудников Банка
поможет достичь
высокого уровня
ИБ

Информационная
безопасность
является одним из
основных
приоритетов
любого
современного
банка

Используйте
современные
подходы в
безопасности

Объединение
общих усилий
сотрудников Банка
поможет достичь
высокого уровня
ИБ

Информационная
безопасность
является одним из
основных
приоритетов
любого
современного
банка

Используйте
современные
подходы в
безопасности

Не делайте свою работу «для галочки»

Спасибо!



10.10.23

mizerinas@yandex-team.ru