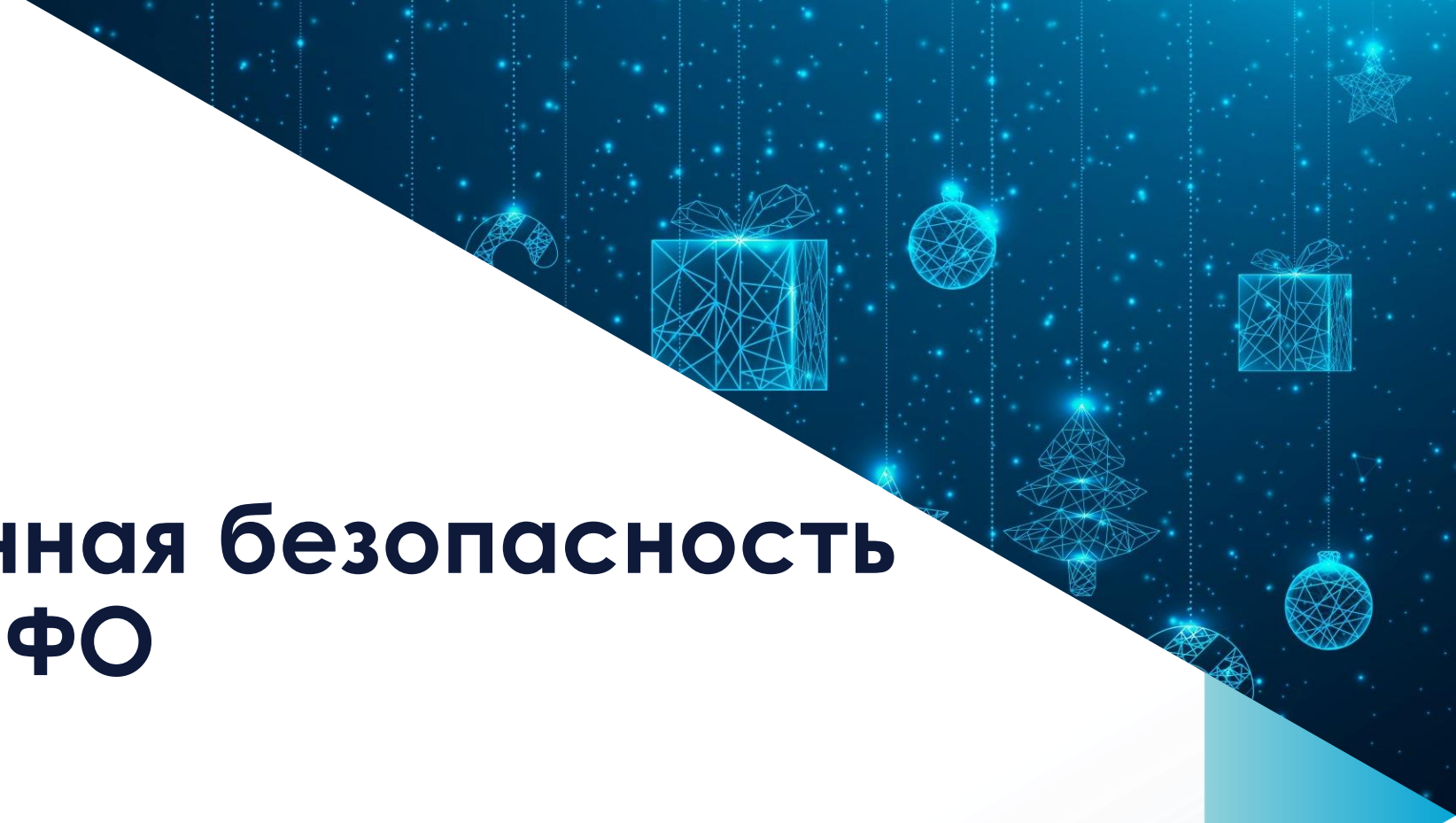
RTM GROUP



Информационная безопасность для Банков и НФО

Самое важное в 2024 году

Эксперт

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

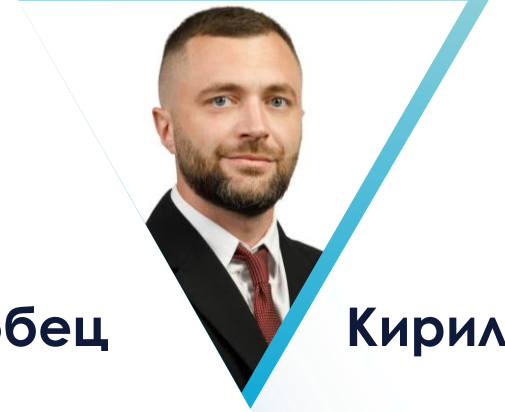
Дмитрий Кобец

Заместитель директора технического департамента

Эксперт в сфере ИБ

Профессиональный опыт в сфере ИТ и информационной безопасности с 2009 года

Участник ТК №122 при Банке России



Кирилл Чекудаев

Ведущий консультант по управлению рисками

Стаж работы по экономическим направлениям с 2003 года

Педагогический стаж с 2007 года

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Работаем на всей территории России, Беларуси и Казахстана, и не ограничиваемся на этом. Головной офис компании находится в Москве, производственное подразделение базируется в Воронеже.

RTM Group ежегодно выполняет сотни проектов, делая свой вклад в стабильность и безопасность киберпространства, а также помогает провести анализ цифровых доказательств для судов и следственных органов.

ПРАВО 300

Входим в рейтинг «Pravo.ru-300» в отрасли Цифровая экономика.

АБИСС

Полноправный член «Ассоциации пользователей стандартов по информационной безопасности»

ТПП РФ

В реестре надежных партнеров торгово-промышленной палаты Российской Федерации

Содержание

Обзор положений и разбор сроков исполнения

Положение № 683-П

683-П

С 1 января 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка по ГОСТ: раз в 2 года
Проверяется лицензиатом ФСТЭК

Положение № 719-П

719-П

С 1 января 2022

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка лицензиатом ФСТЭК (п.1.1)

Положение № 802-П

802-П

С 1 января 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка не реже одного раза в два года (п.20)
ССНП, СБП, ОУИО СБП — стандартный уровень (уровень 2) ГОСТ 57580
ОПКЦ СБП — усиленный уровень (уровень 1) ГОСТ 57580

Положение № 757-П

757-П

С 1 июля 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка по ГОСТ 57580:

- усиленный (1 уровень) раз в год
- стандартный (2 уровень) раз в 3 года

Привлечение лицензиатов ФСТЭК (п.1.5.1)

Положение № 757-П

Положение № 757-П

Общие обязательные требования **для всех НФО**

п.1.2, п.1.3

Защита информации с помощью СКЗИ

п.1.4.1

Ежегодное определение уровня защиты информации не позднее десятого рабочего дня календарного года.

п.1.8

Фиксация решения о применимости оценки соответствия ОУД4

В 757-П НФО могут быть без уровня
ГОСТ 57580 — не применим

Приказ № 453

Приказ № 453	Не реже одного раза в два года	Уровень соответствия не указан

- **Оценка** лицензиатом ФСТЭК (п.8 пп 2) Приложения 2)
- **Стандартный** уровень (уровень 2) ГОСТ 57580 (п.8 пп 2) Приложения 2)
- **Уведомление ЦБ** (п.8 пп 2) Приложения 2)
- **Ежегодный** аудит СЗПДн (п.9. пп 2) Приложения 2)

Независимая оценка SWIFT

SWIFT

Окно аттестации
с 1 июля
до 31 декабря

Все пользователи: независимая внешняя оценка на соответствие требованиям SWIFT Customer Security Program

Оценка соответствия ПО (ОУД4)

Анализ проводится при каждой смене версии ПО

Пентест:
Тестирование на проникновение и анализ уязвимостей

Федеральный закон № 187-ФЗ

Федеральный закон от 26 июля 2017 г.

«О безопасности критической информационной инфраструктуры Российской Федерации»

187-ФЗ	Категорирование объектов КИИ

Федеральный закон от 26 июля 2017 г.

Данная процедура необходима для организаций что являются субъектами КИИ, а именно:

- Государственные органы
- Государственные учреждения
- Российские юридические лица и (или) индивидуальные предприниматели

Субъекты КИИ обладают объектами КИИ на основании:

- Права собственности
- Аренды
- Ином законном основании

Типы объектов КИИ

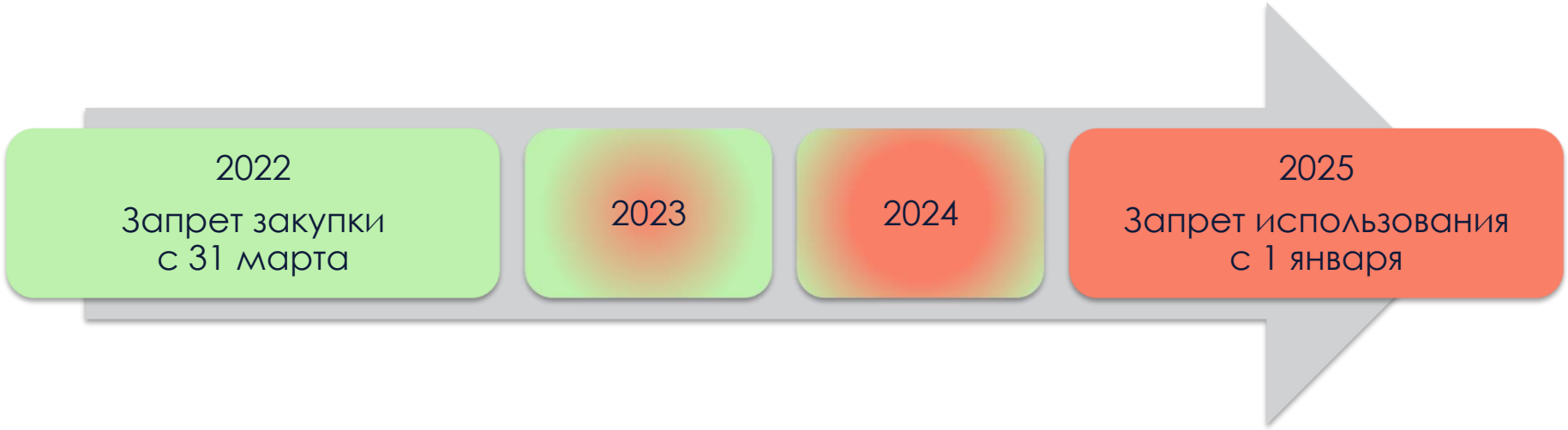
ИС

АСУ

ИТКС

Импортозамещение по Указу Президента №166

- Как быть с импортозамещением?
- Кому в первую очередь?



Указ Президента № 250

Указ Президента Российской Федерации от 01 мая 2022г.

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

На кого распространяется:

- Федеральные органы исполнительной власти
- Высшие исполнительные органы государственной власти субъектов РФ
- Государственные фонды
- Государственные корпорации (компании) и иные организации, созданные на основании ФЗ
- Стратегические предприятия
- Стратегические акционерные общества и системообразующие организации Российской экономики
- ЮЛ, являющиеся субъектами КИИ

Федеральный закон № 152-ФЗ

Федеральный закон № 152-ФЗ
«О персональных данных»

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Аудит проводится на соответствие требованиям Законодательства

«Бумажная» безопасность. Разработка внутренней документации по ПДн

Что требуется сделать:

1. Разработать и ввести в действие организационно-распорядительную документацию в отношении обработки и защиты ПДн

2. Провести моделирование угроз

«Реальная» безопасность. Обеспечение техническими средствами

Организации при обработке персональных данных необходимо самостоятельно обеспечить техническими средствами:

Аутентификация пользователей	Штатные средства ОС как базовый вариант
Физическая защита	Двери, турникеты, видеокамеры, замки и т.д.
Технические средства защиты	Межсетевые экраны, сетевые сканеры, антивирусы, DLP, SIEM и т.д.

Операционная надежность

Положение № 787-П

Положение от 12 января 2022 года
№ 787-П

«Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»

Привлечение внешней организации не требуется

Положение № 787-П

Данным положением ЦБ установил требования к:

- Разработке документов по операционной надежности
- Определение критичной архитектуры
- Показателям операционной надежности

Положение № 779-П

Положение от 15 ноября 2021 года
№ 779-П

«Об установлении обязательных для некредитных финансовых организаций требованиях к операционной надежности при осуществлении видов деятельности в целях обеспечения непрерывности оказания финансовых услуг»

Привлечение внешней организации не требуется

Положение № 779-П

Данным положением ЦБ установил требования к:

- Разработке документов по операционной надежности
- Определение критичной архитектуры
- Показателям операционной надежности

Положение № 716-П

Положение Банка России от 8 апреля 2020 г.
№ 716-П

«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Привлечение внешней организации не требуется

Положение № 716-П

ЦБ РФ данным положением:

- Установил требования к системе управления операционным риском в кредитной организации и банковской группе
- Приведен классификатор событий
- Уточнены способы управления
- КИР и КПУОР

Цель ГОСТ Р 57580.3-2022 и 57580.4-2022

Положения 787-П для банков и 779-П для НФО

Цель документов — содействие соблюдению требований к системе управления операционными рисками, информационными угрозами и обеспечения операционной надежности в финансовой системе.

Результат применения — обеспечение операционной надежности к всем бизнес- и технологическим процессам и критичных активов (объекты информации, субъектов доступа, и защищаемой информации)

Состав направлений, процессов и требований

Цели операционной надежности

- Непрерывность процесса
- Защищенность информационной инфраструктуры
- Соблюдение требований 779-П и 787-П
- Определение и выполнение целевых показателей
- Оптимизация технологических и бизнес-процессов
- Взаимодействие элементов информационной инфраструктуры

В пределах обеспечения операционной надежности должны

- Обеспечивать не превышение порогового уровня допустимого времени простоя технологического процесса
- Соблюдать требования к взаимодействию с поставщиками услуг в сфере IT
- Принимать технические и организационные меры
- Вести учет и контроль элементов критичной архитектуры и взаимодействий между ними
- Обеспечить нейтрализацию информационных угроз
- Информировать Банк России о выявленных событиях операционного риска, связанных с нарушением операционной надежности

RTM GROUP

0409072, 0420432, 0420265, 0420721, 0420523, 0420174, 0409071 — что это за цифры?

Отчетности по операционной надежности и ИБ

Банки

Форма 0409071 Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации в соответствии с Указанием Банка России от 08.11.2022 N 5986-У

Форма 0409072 Сведения о показателях операционной надежности в соответствии с Указанием Банка России от 10.04.2023 N 6406-У

Отчетности по операционной надежности

Профессиональные участники рынка ценных бумаг

Организаторы торговли

Клиринговые организации

Форма 0420432 в соответствии с Указание Банка России от 30.09.2022 N 6282-У

Отчетности по операционной надежности

- Оператор инвестиционной платформы
- Оператор финансовой платформы
- Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов
- Оператор обмена цифровых финансовых активов

Форма 0420721 в соответствии с Указание Банка России от 21 сентября 2022 г. № 6243-У

Отчетности по операционной надежности

Управляющие компании	Форма 0420523 в соответствии с Указанием Банка России от 05.10.2022 **№ 6292-У**
Страховые организации	Форма 0420174 в соответствии с Указанием Банка России от 14.11.2022 **№ 6315-У**
Негосударственные пенсионные фонды	Форма 0420265 в соответствии с Указание Банка России от 27.09.2022 **№ 6269-У**

Форма 0409071 и 12-МР

Раздел 1. Сведения об оценке выполнения требований по направлению «Технологические меры»

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 2. Сведения об оценке выполнения требований по направлению «Безопасность программного обеспечения»

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

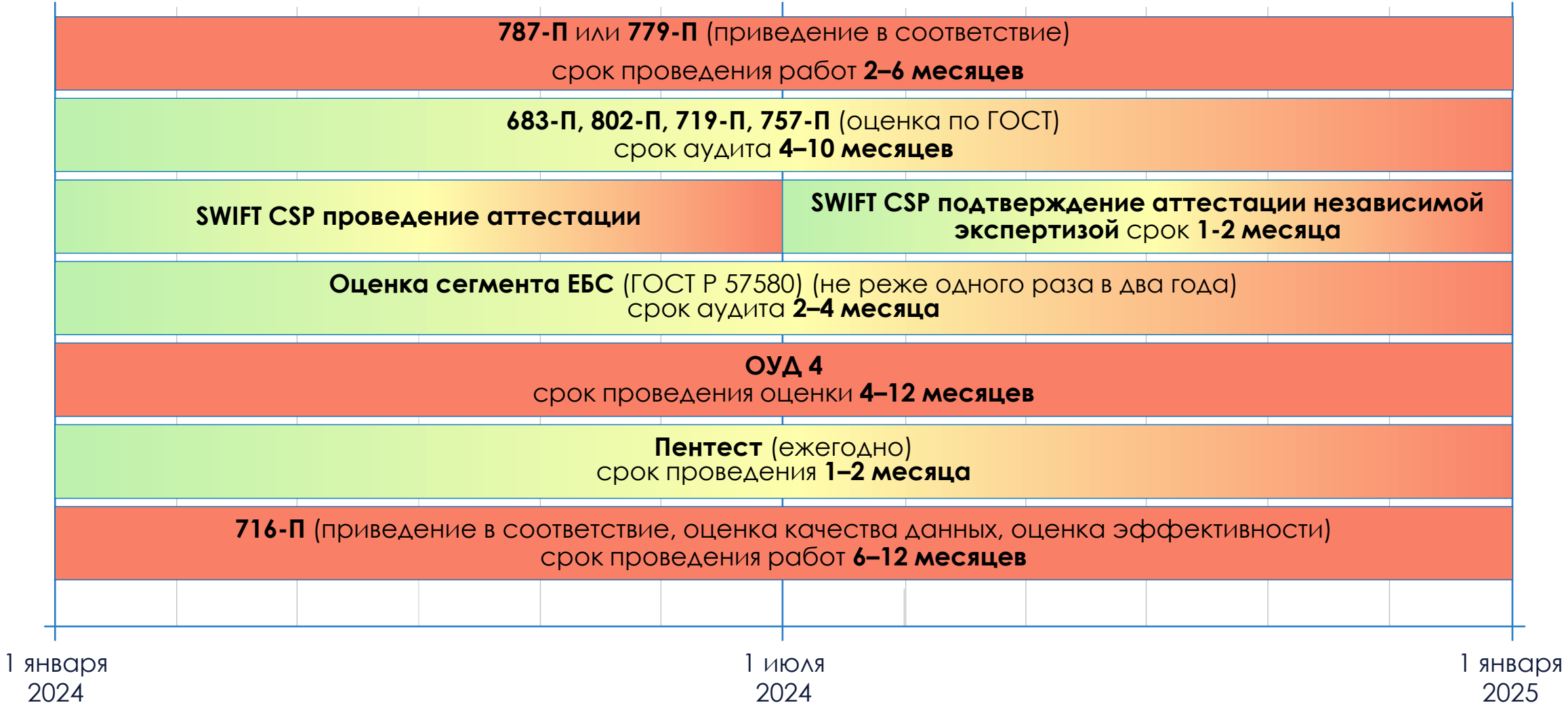
Раздел 3. Сведения об оценке выполнения требований по направлению «Безопасность информационной инфраструктуры»

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
...					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

Раздел 4. Сведения о проверяющей организации.

С 01.10.2022 г. один раз в два года

Сроки исполнения положений



RTM GROUP

Telegram-канал

ИТ. Право. Безопасность

@it_law_security

Экспертный контент и срочные новости из мира ИБ

Спасибо за внимание!

Готовы ответить на Ваши вопросы


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


@RTM_Group


rtm.group


it_law_security