Концепция безопасности SWIFT CSCF v2022: обзор изменений и рекомендации участникам в 2022 году.

RTM GROUP

Объединяем IT,
право и безопасность

Далее

СОДЕРЖАНИЕ

Введение. Справка.

Society for Worldwide Interbank Financial Telecommunications (сокр. ***SWIFT****)* – международная межбанковская система передачи информации и совершения платежей.

Данная система позволяет финансовым учреждениям во всём мире отправлять и получать информацию о финансовых операциях в безопасной, стандартизированной и надёжной форме.

Введение. Справка.

Программа безопасности пользователей (*Customer Security Programme, CSP*) была запущена в 2016 году в ответ на изощренные кибератаки на пользователей SWIFT.

CSP устанавливает общий набор элементов контроля безопасности, известный как Концепция обеспечения безопасности пользователей – (*Customer Security Controls Framework, CSCF*), которая разработана с целью помощи клиентам в обеспечении безопасности локальной среды и создания безопасной финансовой экосистемы.

SWIFT CSCF – содержит как обязательные, так и рекомендуемые ЭК, основанные на международных стандартах ИБ, таких как NIST, ISO 27000 и PCI-DSS.

Краткий обзор SWIFT CSCFv2022.

Элементы контроля безопасности (ЭК) базируются на трех всеобъемлющих целях, подкрепленных восемью принципами безопасности.

Цели:
- Обеспечивать безопасность среды;
- Знать и ограничивать доступ;
- Обнаруживать и реагировать.

Принципы
- Ограничение доступа в Интернет;
- Защита наиболее важных систем от общей ИТ-среды;
- Снижение возможностей и уязвимостей для атак;
- Обеспечение физической защиты среды.
- Предотвращение компрометации учетных данных;
- Управление идентификационными данными и разграничение полномочий
- Обнаружение аномальной активности в системах или журналах транзакций;
- План реагирования на инциденты и обмен информацией.

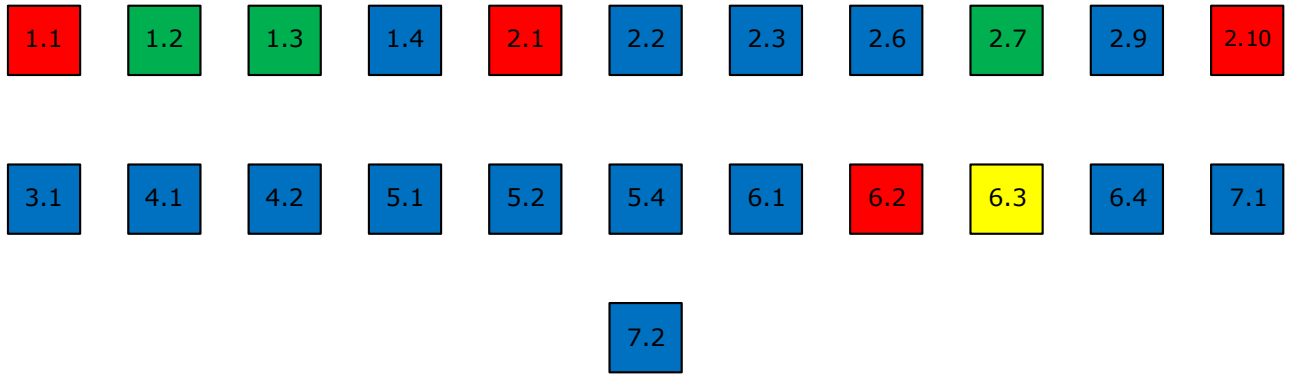
Краткий обзор SWIFT CSCFv2022. Элементы контроля.

Архитектура A1 и A2

Архитектура A3

Архитектура A4

Архитектура B



Независимая внешняя оценка.

Independent Assessment Framework (Концепция независимой оценки) – Данный документ содержит подходы и методы проведения оценки соблюдения положений документа Концепция обеспечения безопасности пользователей SWIFT (SWIFT – CSCF) от 12.07.2021 г.

1. Типы оценки:
- Самооценка (не обеспечивает соответствие с 1 января 2022 года);
- Оценка по стандартам общества (обязательна к концу года);
- Оценка по требованию SWIFT.

2. Область применения оценки.

3. Подход к оценке и риск-ориентированный подход.

4. Имеющиеся ресурсы для оценки.
- документация;
- Независимость ассесора;
- Квалификация ассесора;
- И др.

5. Методология тестирования.

6. Результаты оценки

Assessment Type	Selection Criteria	Assesor	Временная шкала			
			2019	2020	2021	2022 и далее
☐ **Самооценка**	Пока еще возможна, но не обеспечивает соответствие после введения в действие IAF	Первая линия защиты				факт несоответствия будет отражен в отчете регулятору – с января 2022 г.
☐ **Оценка по стандартам сообщества**	Обязательная для всех клиентов после введения в действие IAF	Внутренний или внешний				
☐ **Оценка по требованию Swift**	Обязательная – отобранные клиенты по результатам анализа процесса обеспечения качества (QA Analysis)	Только внешний				

* IAF – Independent Assessment Framework – Концепция независимой оценки

Разбор сроков выполнения положений в 2022 году.

Independent Assessment Framework (Концепция независимой оценки) п.7.2.

В соответствии с Политикой обеспечения безопасности пользователей, во второй половине **каждого года**, все пользователи SWIFT должны подтверждать соответствие обязательным элементам контроля из CSCF, которые действуют на тот момент и которые применимы к ним.

Это должно быть сделано в приложении KYC-SA и должно быть завершено в период **с начала июля до конца года - 31 декабря**.

Краткий обзор основных изменений

Изменения Концепции обеспечения безопасности пользователей SWIFT (версии 2022) коснулись:

1. **Добавлен новый рекомендуемый элемент** контроля 1.5A (Обеспечение защиты среды пользователя).
2. **Добавлен обязательный элемент** контроля 2.9 (средства контроля транзакционной активности).
3. **Элементы контроля 6.2** (Целостность программного обеспечения) и 6.3 (Целостность базы данных) **переведены** в разряд рекомендуемых для архитектуры A4.
4. **Область применения элемента контроля 1.2** (Контроль за привилегированными учетными записями операционной системы) **расширена**, а для архитектуры B стала рекомендательной.

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Кобец Дмитрий Андреевич

Эксперт в сфере информационной безопасности

Заместитель директора технического департамента RTM Group


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


GroupRTM


rtm.group


@GroupRtm


rtm.group.Russia


t.me/kurilka_ib