



РУССВИФТ

«Обзор Customer Security Programme и практические рекомендации»

Программа безопасности пользователей SWIFT (Customer Security Programme — CSP) создана в ответ на участвовавшие кибератаки на инфраструктуру пользователей Swift, направлена на поддержание надлежащего уровня кибербезопасности для всех пользователей, снижение риска кибератак и минимизацию финансовых последствий мошеннических транзакций. Так как каждый пользователь несет ответственность за защиту своей собственной инфраструктуры и доступа к сети Swift, программа CSP была введена для стимулирования общепромышленного сотрудничества в борьбе с кибермошенничеством.

Цель обучения: подготовка специалистов к **обеспечению полного соответствия требованиям CSP**. В ходе обучения слушатели должны:

- Изучить принципы построения и область применения **Customer Security Controls Framework (CSCF)**.
- Освоить процесс ежегодной самоаттестации в приложении **KYC-SA**.
- Получить практические рекомендации по защите и настройке «зоны безопасности» (secure zone) и компонентов SWIFT.

Аудитория: специалисты, участвующие в обеспечении безопасности и технической поддержке программно-аппаратного комплекса и операций SWIFT:

- **Офицеры безопасности (Security Officers):** LSO (Left Security Officers), RSO (Right Security Officers) и SwiftNet Security Officers.
- **Системные администраторы и ИТ-специалисты:** ответственные за эксплуатацию и настройку программного обеспечения и оборудования Swift.
- **Администраторы swift.com:** управляющие доступом и правами в экосистеме SWIFT.
- **Специалисты по комплаенсу:** занимающиеся подготовкой к самоаттестации и прохождением независимых проверок на соответствие стандартам CSP.

Продолжительность обучения: три дня с 10:00 до 17:00

Форма обучения: очная

Программа консультационного семинара:

День 1 Обучение: 10:00-17:00 Перерывы: 11:30-11:45, 13:30-14:30, 15:45-16:00	1. Общий подход к разработке программы: <ul style="list-style-type: none">• Customer Security Controls Framework• KYC Self-Attestation• Independent Assessment 2. Customer Security Controls Framework <ul style="list-style-type: none">• Составные части, цели, принципы и область применения CSP• Типы архитектур пользователей
День 2 Обучение: 10:00-17:00 Перерывы:	<ul style="list-style-type: none">• Программное обеспечение и оборудование в зоне безопасности• Элементы контроля: определение, риски, руководство по реализации



Р У С С В И Ф Т

11:30-11:45, 13:30-14:30, 15:45-16:00	<ol style="list-style-type: none">3. KYC Self-Attestation<ul style="list-style-type: none">• Описание приложения4. Порядок предоставления данных Independent Assessment<ul style="list-style-type: none">• Процесс обследования• Отличия процесса обследования от аудита• Результат обследования• Соответствие CSP и Independent Assessment
День 3 Обучение: 10:00-17:00 Перерывы: 11:30-11:45, 13:30-14:30, 15:45-16:00	<ol style="list-style-type: none">5. Рекомендации по настройкам программного обеспечения и оборудования для соответствия требованиям CSP:<ul style="list-style-type: none">• Рекомендации по защите зоны безопасности• Alliance Access• Alliance Gateway/SwiftNet Link• Alliance WebPlatform6. SwiftNet Connectivity7. Роли, область ответственности и инструменты Security Officers<ul style="list-style-type: none">• swift.com администраторы• LSO и RSO• SwiftNet Security Officers