SWIFT CSCF v2026 / Control 7.3A

Протестируй один раз, удовлетвори многих: тест на проникновение SWIFT CSCF v2026 7.3A как межрежимное упражнение

Cambridge Cyber International / 2026

В цикле 2026 Программы Безопасности Клиента SWIFT Контроль 7.3A (Тестирование на Проникновение) несет руководство, формируемое сообществом, которое задает охват и сценарии тестирования, ожидаемые от подключенного учреждения в рамках скользящего трехлетнего цикла (SWIFT 2025). Прочитанный в изоляции, это еще одна строка аттестации для удовлетворения. Прочитанный на фоне более широкого регуляторного ландшафта, он является доказательством единого направления движения: надзорные органы в Европейском Союзе, Соединенных Штатах и Канаде сходятся к тестированию, управляемому разведкой и осведомленному об угрозах, как к способу, которым учреждение доказывает, что его контроли работают, а не просто существуют. Эта статья утверждает, что учреждение, готовящееся к тесту на проникновение 7.3A, должно спроектировать этот тест один раз, до уровня самой современной практики, и собрать те же доказательства относительно Акта о Цифровой Операционной Устойчивости (DORA), второй Директивы о Безопасности Сетей и Информации (NIS2), регулирования кибербезопасности Департамента Финансовых Услуг штата Нью-Йорк (23 NYCRR Part 500) и Руководства B-13 Управления Надзора за Финансовыми Учреждениями, используя Рамки Кибербезопасности американского Национального Института Стандартов и Технологий версии 2.0 (NIST CSF 2.0) как общий хребет.

Проблема с прочтением 7.3A как галочки

Подключенное учреждение, которое относится к каждому режиму как к отдельному обязательству, платит структурный штраф. Оно узко определяет охват теста на проникновение SWIFT защищенной зоной, заказывает отдельный тест устойчивости для DORA, отвечает на анкету NYDFS о ежегодном тестировании и готовит доказательства для канадского надзорного органа по четвертому графику. Каждое задание повторяет ту же разведку, те же правила взаимодействия, тот же цикл устранения, и каждое производит доказательства в форме, которую следующий режим не принимает. Цена не только в деньгах. Фрагментированное тестирование производит фрагментированную картину риска, потому что ни одно отдельное упражнение не видит учреждение так, как увидел бы его реальный противник: от начала до конца, через бэк-офис, рабочие станции операторов, интерфейс обмена сообщениями и подключение к сети.

Довод здесь в том, что сближение, видимое теперь в основных режимах, делает фрагментированный подход устаревшим. Руководство 7.3A, режим тестирования, управляемого угрозами, DORA, ожидание OSFI об управлении разведкой и ежегодный мандат NYDFS это не четыре разных теста. Это четыре надзорных выражения одной идеи, и учреждение, которое проектирует по самому требовательному из них и записывает результат относительно общих рамок, может удовлетворить остальные как побочный продукт.

Чего теперь ожидает Контроль 7.3A SWIFT CSCF v2026

Контроль 7.3A находится в Рамках Контролей Безопасности Клиента как рекомендательный контроль, цель которого подтвердить операционную устойчивость связанной со SWIFT инфраструктуры пользователя путем выявления уязвимостей, которые могли бы привести к компрометации защищенной зоны или бэк-офиса (SWIFT 2025). Суть изменения 2026 года не новый номер контроля, а более четкое руководство о том, как следует определять охват теста и какие сценарии он должен покрывать. Рамки теперь формулируют набор тестовых сценариев для отработки в течение трехлетнего цикла, так что учреждение не может удовлетворить контроль одним узким внешним сканированием, повторяемым ежегодно. Ожидается, что на протяжении цикла программа охватывает тестирование на уровне приложений интерфейса обмена

сообщениями и связанных компонентов, тестирование инфраструктуры защищенной зоны и ее сегментации, а также человеческие пути и пути рабочих станций операторов, которые эксплуатируют реальные вторжения.

Отсюда следуют два проектных следствия. Во-первых, охват должен быть определен относительно защищенной зоны и ее границ доверия, а не относительно удобного сетевого диапазона, потому что цель контроля доказать, что нападающий не может развернуться из бэк-офиса в уровень обмена сообщениями. Во-вторых, тест должен проводиться компетентной и достаточно независимой стороной, а его выводы должны питать отслеживаемый цикл устранения, чье закрытие само является доказательством. Контроль является рекомендательным, а не обязательным для каждого типа архитектуры, но для учреждений, которые сами аттестуются относительно него, асессор будет ожидать увидеть охват, метод, выводы и устранение как связную запись, а не сертификат.

Четыре соседних режима

DORA и тестирование на проникновение, управляемое угрозами

Акт о Цифровой Операционной Устойчивости требует, чтобы все попадающие в охват финансовые субъекты регулярно тестировали свои системы информационных и коммуникационных технологий, и требует от подмножества значимых субъектов выполнения продвинутого тестирования посредством тестирования на проникновение, управляемого угрозами (TLPT), не реже одного раза в три года (European Parliament and Council 2022a). TLPT управляется разведкой: контролируемая симуляция красной команды против живых производственных систем, смоделированная на тактиках, техниках и процедурах реальных акторов угроз, проводимая по методологии, для которой европейским ориентиром являются рамки TIBER-EU (European Central Bank 2018). Учреждение, которое готовит тест 7.3A до стандарта, управляемого угрозами, с текущей разведкой угроз, формирующей его сценарии, уже строит хребет теста DORA, отличаясь главным образом формальным охватом и надзорным управлением, обернутым вокруг назначенного TLPT.

NIS2 и исключение lex specialis

Вторая Директива о Безопасности Сетей и Информации повышает базовый уровень управления рисками кибербезопасности и сообщения об инцидентах среди существенных и важных субъектов, а национальные органы перешли от транспозиции к активному надзору в течение 2026 года (European Parliament and Council 2022b; European Commission 2025). Для финансовых субъектов практический момент касается приоритета: DORA является lex specialis, и статья 4 NIS2 уступает ей там, где правила финансового сектора по меньшей мере равноценны. Поэтому учреждению следует относиться к DORA как к действующему режиму тестирования устойчивости, признавая при этом, что групповые субъекты вне финансового периметра, такие как общая технологическая дочерняя компания, могут оставаться в рамках NIS2 и пользоваться теми же доказательствами тестирования.

Соединенные Штаты: NYDFS Part 500 и ожидания FFIEC

Регулирование кибербезопасности Департамента Финансовых Услуг штата Нью-Йорк требует, чтобы каждый охватываемый субъект проводил тестирование на проникновение своих информационных систем не реже одного раза в год, как изнутри, так и снаружи границ систем, на основе оценки риска субъекта (New York State Department of Financial Services 2023). Измененное

регулирование еще больше ужесточило ожидания об управлении и тестировании (Ropes and Gray 2026). На федеральном уровне Федеральный Экзаменационный Совет Финансовых Учреждений не налагает фиксированного правила, но рассматривает тестирование на проникновение квалифицированными независимыми сторонами как ожидание экзаменатора и индикатор зрелости в своем буклете Безопасности Информации (Federal Financial Institutions Examination Council 2016). Учреждение, которое удовлетворяет 7.3A до высокого стандарта, тестируя как изнутри, так и снаружи границы в определенном ритме, производит именно те артефакты, которых ожидают экзаменатор NYDFS и экзаменация FFIEC.

Канада: Руководство B-13 OSFI

Руководство B-13 Управления Надзора за Финансовыми Учреждениями, действующее с 1 января 2024 года, требует, чтобы федерально регулируемые финансовые учреждения выявляли уязвимости посредством регулярного тестирования, а для учреждений со значительными технологическими следами оно ожидает тестирования на проникновение, управляемого разведкой и угрозами, и упражнений красной команды, которые симулируют реалистичные многоэтапные атаки (Office of the Superintendent of Financial Institutions 2022). B-13 основано на результатах и не задает фиксированного ритма, поэтому учреждение доказывает соответствие через качество и реалистичность своего тестирования, а не через его частоту. Это тот же стандарт, управляемый разведкой, который выражают DORA и уточненное руководство 7.3A, что делает B-13 канадским членом той же семьи, а не отдельным обязательством.

Один хребет: отображение режимов на NIST CSF 2.0

Ни один отдельный финансовый регулятор не управляет одновременно Соединенными Штатами и Канадой, поэтому трансграничному учреждению нужен нейтральный ориентир, признанный в обеих. Рамки Кибербезопасности NIST версии 2.0 являются таким ориентиром: добровольные, широко принятые по обе стороны границы и организованные вокруг шести функций: Управляй, Идентифицируй, Защищай, Обнаруживай, Реагируй и Восстанавливай (National Institute of Standards and Technology 2024). Используемые как хребет, они позволяют учреждению записать одну программу тестирования на проникновение и выразить результат на словаре, который понимает каждый режим. Тест на проникновение наиболее прямо обращается к функции Идентифицируй, выявляя уязвимости, и к функциям Обнаруживай и Реагируй, измеряя, действительно ли мониторинг и реагирование учреждения улавливают и сдерживают реалистичное вторжение. Функция Управляй несет правила взаимодействия, независимость и отчетность совету, которые требуют все пять режимов. Таблица 1 делает это сближение конкретным.

Таблица 1. Одна программа тестирования на проникновение, четыре режима, один хребет

Измерение	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Характер	Рекомендательный контроль	Обязателен для значимых	Обязательное правило	Ожидание на основе	Добровольный ориентир
Ритм	3-летний цикл сценариев	Не реже одного раза в 3 года	Не реже одного раза в год	Нет фиксированного	Не предписан
Метод	На основе сценариев, фокус на защищенной зоне	Красная команда, управляемая разведкой	Изнутри и снаружи, на основе риска	Управляемый разведкой, красная команда	Функции и результаты

Независимость	Компетентная независимая сторона	Аккредитованные поставщики	Квалифицированная внутренняя или внешняя	Независимое заверение	Результат управления
Главное доказательство	Охват, выводы, устранение	Сценарии угроз, нарратив атаки, устранение	Отчет о тесте, ритм устранения	Реалистичность и результат теста	Отображенные результаты

Прочтение поперек каждой строки и есть тезис: спроектируй тест до самого требовательного стандарта в каждом столбце, метод, управляемый разведкой, охват, осведомленный о защищенной зоне, покрытие изнутри и снаружи, независимое исполнение, отслеживаемое устранение, и единственная итоговая запись удовлетворит все пять.

Модель подготовки, управляемая риском

Руководство 7.3A приглашает к прочтению через призму соответствия, при котором учреждение делает минимум, названный контролем. Более ценное прочтение, и то, которое надзорные органы все чаще вознаграждают, управляется риском: тест на проникновение это инструмент, используемый для выявления и устранения самых значимых уязвимостей учреждения, а соответствие это побочный продукт грамотного выполнения этого.

Подготовка начинается с базы риска и охвата. Учреждение инвентаризирует свое связанное со SWIFT хозяйство, защищенную зону, интерфейс обмена сообщениями, рабочие станции операторов, подключение к сети и системы бэк-офиса, которые его питают, и ранжирует пути по последствиям компрометации, а не по легкости тестирования. Это производит охват, определенный тем, где находятся деньги и доверие, который также является охватом, который выбрал бы реальный противник, и который согласуется с позицией B-13, управляемой последствиями, и позицией NYDFS, основанной на риске.

Далее приходит обрамление разведкой угроз. Текущая разведка об акторах, которые нацеливаются на финансовые сообщения, формирует сценарии, так что тест репетирует правдоподобные вторжения, а не общие. Это шаг, который превращает тест на проникновение в тест, управляемый угрозами, и это шаг, который делает то же упражнение заслуживающим доверия в рамках DORA и B-13.

Исполнение затем запускает сценарии в течение трехлетнего цикла, описанного руководством 7.3A, охватывая пути приложений, инфраструктуры и человеческие, изнутри и снаружи границы, независимой стороной, по документированным правилам взаимодействия. Учреждение измеряет не только то, что было найдено, но и увидели ли его собственные обнаружение и реагирование, что тест происходит, потому что это измерение и есть доказательство, которого требуют функции Обнаруживай и Реагируй.

Наконец, устранение и доказательства замыкают петлю. Выводы входят в отслеживаемый цикл устранения, чье закрытие записывается, а вся запись, охват, сценарии, нарратив атаки, выводы, устранение и производительность обнаружения, подается один раз относительно хребта NIST CSF 2.0 и помечается для каждого режима. Учреждение, которое замыкает эту петлю, не прошло один тест. Оно построило многоразовый доказательный актив устойчивости.

Наша услуга оценки SWIFT CSP определяет охват и проводит тест 7.3A до этого стандарта, а PenTeva проверяет и отслеживает выводы до закрытия, так что доказательства выдерживают под любым из четырех режимов. Там, где моделирование устойчивости DORA в охвате, DORA-MAST переносит те же доказательства в картину операционной устойчивости.

Заключение

Уточненное руководство 7.3A лучше понимать не как изолированное требование SWIFT, а как одно надзорное выражение глобального движения к тестированию, управляемому разведкой и осведомленному об угрозах. Учреждение, которое проектирует свой тест на проникновение 2026 года до этого стандарта, определяет его охват по последствиям, обрамляет его текущей разведкой угроз, исполняет его независимо по защищенной зоне и записывает результат относительно общих рамок, может удовлетворить DORA, NIS2 там, где он еще применяется, NYDFS Part 500 и OSFI B-13 из того же упражнения. Пентест перестает быть повторяющимся издержкой соответствия и становится инструментом, через который учреждение находит и устраняет риски, которые имеют значение. Протестируй один раз, удовлетвори многих.

Акронимы

CSCF, Customer Security Controls Framework (SWIFT). CSP, Customer Security Programme (SWIFT). DORA, Digital Operational Resilience Act. FFIEC, Federal Financial Institutions Examination Council. ICT, Information and Communication Technology. NIS2, Network and Information Security Directive (вторая). NIST CSF, National Institute of Standards and Technology Cybersecurity Framework. NYDFS, New York State Department of Financial Services. OSFI, Office of the Superintendent of Financial Institutions. SWIFT, Society for Worldwide Interbank Financial Telecommunication. TIBER-EU, Threat Intelligence-Based Ethical Red Teaming (европейские рамки). TLPT, Threat-Led Penetration Testing.

Библиография

European Central Bank (2018). TIBER-EU Framework. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

European Commission (2025). NIS2 Directive: transposition in EU countries. https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

European Parliament and Council (2022a). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj

European Parliament and Council (2022b). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Federal Financial Institutions Examination Council (2016). Information Technology Examination Handbook: Information Security. https://ithandbook.ffiec.gov/it-booklets/information-security/

National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

New York State Department of Financial Services (2023). Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Part 500 (as amended). https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

Office of the Superintendent of Financial Institutions (2022). Guideline B-13: Technology and Cyber Risk Management. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management

Ropes and Gray (2026). NYDFS-regulated entities face stronger cybersecurity regulations.

https://www.ropesgray.com/en/insights/alerts/2026/01/nydfs-regulated-entities-face-stronger-cybersecurity-regulations

SWIFT (2025). Customer Security Controls Framework v2026, Customer Security Programme. https://www.swift.com/myswift/customer-security-programme-csp