ФБК
Grant Thornton

Информационная безопасность

ИТ-риски

Услуги в области информационной безопасности

Тестирование на проникновение

Что это и зачем?

Тестирование на проникновение представляет собой моделирование действий настоящих киберпреступников и направлено на выявление недостатков и слабостей в информационной инфраструктуре организации.

В ходе тестирования проводится сбор информации об инфраструктуре из всех доступных источников; идентификация используемых приложений, служб, сервисов и оборудования; поиск и эксплуатация уязвимостей с целью получения контроля над информационным активом.

Тестирование на проникновение уже является обязательным для большинства участников индустрии платежных карт (требования PCI-DSS), а в 2018 году, в соответствии с поправками в Положение Банка России 382-П, станет обязательным для всех кредитных организаций.

Виды услуг по тестированию на проникновение

В зависимости от актуальных задач, стоящих перед организацией, может быть проведен один или несколько из следующих видов работ:

- Внешнее тестирование периметра корпоративной сети со стороны глобальной сети Интернет
- Внутреннее тестирование из сети организации
- Комплексный анализ защищенности веб-приложений
- Проверка осведомленности пользователей по вопросам информационной безопасности с использованием методов социальной инженерии
- Анализ защищенности беспроводных сетей
- Анализ защищенности мобильных приложений

Нацеленность на результат

Тестирование на проникновение является наиболее эффективным методом определения уровня реальной защищенности и позволяет выявить многие недостатки, часто ускользающие при проведении организационных аудитов информационной безопасности, такие как:

- ошибки конфигурации оборудования, системного и прикладного программного обеспечения
- отсутствие установленных актуальных обновлений и патчей безопасности
- использование слабых и легкоугадываемых паролей
- некорректная сегментация сети
- программные ошибки, допущенные разработчиками бизнес- и веб-приложений

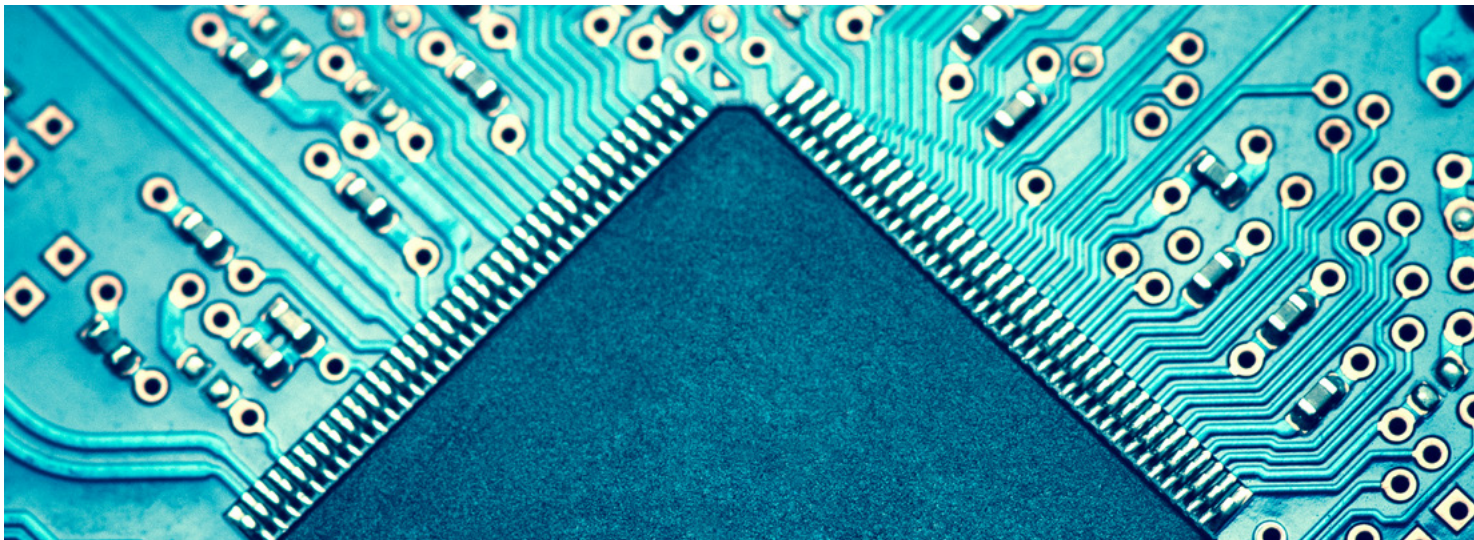
Как мы можем помочь?

Наша команда включает в себя экспертов, обладающих глубокими техническими знаниями и многолетним практическим опытом в области ИТ-безопасности.

Мы понимаем деликатность данного вида услуг, особенности работы информационных систем кредитных организаций и риски, связанные с некоторыми из проверок.

При проведении работ мы руководствуемся как собственной методологией, так и ведущими международными подходами и практиками, такими как:

- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP)



Расследование инцидентов ИБ

Проведение расследований

Число связанных с киберпреступлениями инцидентов, равно как и ущерб от них, неуклонно возрастает с каждым годом. При этом растет и сложность расследований, так как злоумышленники используют более современные средства проведения кибератак.

Услуги в сфере расследования инцидентов могут включать в себя:

- Сбор, систематизация и анализ данных, необходимых для расследования инцидента информационной безопасности
- Исследование образов памяти серверов, рабочих компьютеров, мобильных устройств
- Анализ вредоносного ПО, определение границ заражения
- Консультация правоохранительных органов и сопровождение компании в суде
- Обучение персонала процедурам реагирования на инциденты ИБ
- Консультации по устранению уязвимостей

Сбор и анализ электронных данных

Проведение комплексного анализа данных с использованием современных статистических моделей и средств визуализации позволяет определить мошеннические операции, найти данные, релевантные для юристов и органов правопорядка, обнаружить промышленный шпионаж и факты неправомерного доступа к компьютерной информации.

Компьютерно-техническая экспертиза

Услуги, оказываемые в рамках компьютерно-технической экспертизы:

- Поиск на носителе информации документов, изображений, сообщений и других сведений, в том числе в удаленном, скрытом, зашифрованном виде
- Поиск цифровых следов действий, совершаемых над компьютерной информацией
- Анализ программ для ЭВМ на предмет их принадлежности к вредоносным, к средствам преодоления технических средств защиты авторских прав, к инструментам для осуществления неправомерного доступа к компьютерной информации, к специальным техническим средствам, предназначенным для негласного получения информации
- Анализ функциональности программ, принципа их действия, а также вероятного источника происхождения и распространения
- Установление времени и последовательности совершения пользователем различных действий
- Оценка квалификации и некоторых других особенностей личности пользователя исследуемого компьютера

Как мы можем помочь?

Наша компания помогает бизнесу в расследованиях преступлений, орудием которых был компьютер. Наши специалисты восстанавливают картину произошедшего, собирая и анализируя цифровые доказательства с различных электронных устройств. Мы помогаем найти виновников инцидентов и привлечь их к ответственности.

Эксперты компании при исследовании доказательств используют оборудование от признанных мировых производителей и современное программное обеспечение, которое позволяет сохранять целостность информации, что позволяет использовать полученные сведения в судебных процессах.

Услуги по обеспечению безопасности SWIFT

SWIFT Security Framework

Для всех участников международной сети межбанковского взаимодействия SWIFT разработаны обязательные требования по информационной безопасности. Данные требования представлены сообществом SWIFT в рамках программы Customer Security Programme (CSP), которая направлена на повышение мер по обеспечению информационной безопасности в финансовой индустрии в связи с недавними инцидентами в крупных международных финансовых институтах.

Ключевые требования

Все требования по безопасности, указанные в документе «SWIFT Customer Security Framework. Supplementary Guide», основаны на 3 целях:

- защита своего окружения
- знание и ограничение доступа
- обнаружение и реагирование

В свою очередь, на данных целях базируются 8 принципов и 27 контролей, из которых 16 обязательных и 11 рекомендательных.

Все эти контроли соответствуют уже широко известным требованиям международных стандартов, таких как NIST, PCI-DSS и ISO27002.

Область распространения контролей

- Уровень обмена данными
- Локальная инфраструктура SWIFT заказчика
- Персональные компьютеры пользователей
- Пользователи

Соответствие требованиям

Подтверждение соответствия клиентов SWIFT требованиям безопасности допускается в одном из 3 форматов:

- Самооценка
- Внутренний аудит
- Независимый внешний аудит, направленный на идентификацию распространенных уязвимостей, которые могут представлять собой системные риски для сети SWIFT

Проведение оценки соответствия требованиям SWIFT станет обязательным с января 2018 года.

Как мы можем помочь?

Наша команда включает в себя экспертов по банковским процессам, экспертов по SWIFT и по различным направлениям кибербезопасности.

В рамках аттестации требованиям по безопасности мы проводим анализ всех компонентов локальной SWIFT-инфраструктуры, включая анализ архитектуры и конфигураций системных компонентов, а также проведение практического анализа защищенности методом моделирования действий потенциальных злоумышленников (пентест).

По результатам независимого аудита мы помогаем нашим заказчиками снизить риски, тем самым защищая операционную прибыль, достигая регуляторного соответствия и повышая операционную уверенность.

Соответствие PCI DSS

PCI SSC

Для всех компаний, чей бизнес предлагает возможность оплаты товаров и услуг с использованием банковских карт международных платежных систем, является обязательным выполнение требований по защите данных банковских карт своих клиентов, установленных Советом по стандартам безопасности платежных карт (PCI SSC). PCI SSC является профессиональной структурой, которая была основана со стороны пяти международных платёжных систем (American Express, Discover Financial Services, JCB International, MasterCard и Visa Inc).

Обязательность требований

Требования PCI SSC включают в себя надлежащую защиту данных держателей карт (первичные номера счетов, имена владельцев карт, даты истечения срока действия) и удаление конфиденциальных данных аутентификации транзакций (коды подтверждения, PIN-коды) после того, как сделка была подтверждена.

При этом широко распространенным заблуждением является мнение об обязательности данных требований только в отношении процессинговых центров (банков-эвайеров), банков-эмитентов, платежных шлюзов и хостинг-провайдеров. Однако в том или ином объеме требования PCI DSS распространяются на любого поставщика услуг, принимающего к оплате платежные карты (мерчанты). Например, даже наличие на сайте торгово-сервисного предприятия ссылки «redirect» на страницу ввода платежных данных банка обязывает соблюдать ряд требований PCI DSS.

Типы оценок соответствия

В зависимости от количества ежегодно обрабатываемых транзакций организация может подтверждать соответствие PCI DSS одним из следующих способов:

- SAQ — заполнение мерчантом одного из вариантов листов самооценки
- ISA — проведение внутреннего аудита сертифицированным специалистом
- QSA — внешний аудит с привлечением компании, обладающей сертификатом квалифицированного аудитора систем безопасности (Qualified Security Assessor — QSA)

Как мы можем помочь?

Оценка соответствия PCI DSS осуществляется в отношении каждого системного и сетевого компонента в «среде данных держателей карт» (CDE). Наши специалисты обладают квалификацией для выполнения каждого из тестов и документирования результатов, чтобы обеспечить соблюдение необходимых регуляторных требований.

Компания ФБК является квалифицированным аудитором систем безопасности (QSA-аудитор) и имеет полномочия и возможности проводить сертификационный аудит организаций на соответствие требованиям PCI DSS по всему миру.

Наша компания предлагает следующий комплекс консультационных и аудиторских услуг по подготовке и прохождению сертификационного QSA-аудита либо по оказанию помощи в заполнении листов самооценки и проведении ISA:

- Анализ исходного уровня соответствия компании требованиям PCI DSS
- Разработка рекомендаций по выполнению требований PCI DSS
- Внедрение рекомендаций в информационную инфраструктуру с одновременной интеграцией с другими международными стандартами в области ИБ, такими как ISO 27001
- Разработка документации
- Консультационная поддержка внедрения
- Тест на проникновение — мероприятие по активному обследованию защищенности информационной инфраструктуры заказчика, представляющее собой обязательное требование 11.3 стандарта PCI DSS
- ASV-сканирование — автоматизированное сканирование внешнего периметра сети организации
- Сертификационный QSA-аудит
- Поддержка соответствия PCI DSS, включающая регулярный контроль и тестирование сети заказчика

По результатам успешного проведения сертификационного QSA-аудита заказчик получает Отчет о соответствии (Report on Compliance).

General Data Protection Regulation (GDPR)

Что это и зачем?

Общий регламент по защите данных (General Data Protection Regulation, GDPR) — это новый закон Европейского союза о защите персональных данных, который вступает в силу 25 мая 2018 года.

Несмотря на то, что закон принят в Евросоюзе, он экстерриториален и затрагивает большое число российских компаний, обрабатывающих персональные данные граждан Евросоюза, например, в следующих ситуациях:

- Валютные платежи и переводы на территорию ЕС
- Сбор данных посетителей сайта (ip-адреса, cookie-файлы), если они пребывают на территории ЕС
- Наличие филиала или представительства на территории ЕС, а также ряд других ситуаций

Ключевые изменения

GDPR вводит различные изменения, которые требуют тщательного изучения, утверждения менеджментом и соответствующей подготовки к применению в организации. К таким изменениям относятся:

- Расширение прав субъектов персональных данных
- Рост числа обязательств и ответственности
- Официально установленные процессы управления рисками
- Ужесточение требований в отношении согласия на обработку данных
- Ужесточение требований в отношении оповещения об утечке данных
- Подробный учет процессов
- Учет требований по конфиденциальности личных данных на этапе создания систем
- Значительные штрафные санкции

Как подготовиться

Юридические требования по защите данных постоянно меняются, что создает трудности для бизнеса, правительств и государственных органов. Это в особенности касается организаций, которые работают с клиентами через Интернет, в секторе финансовых услуг или обрабатывают персональные данные большого количества субъектов.

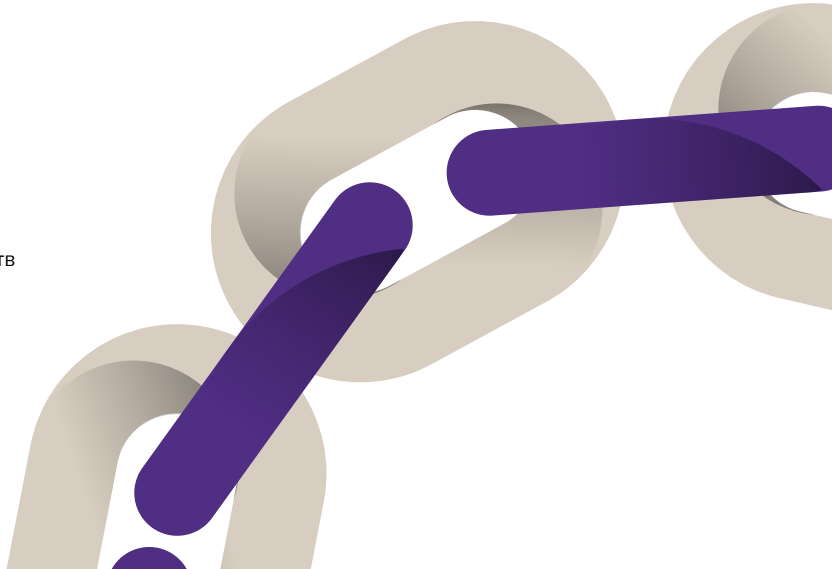
Поскольку срок вступления регламента в силу приближается, необходимо изучить изменения и понять, как они повлияют на деятельность организации. Следует иметь в виду, что регламент GDPR относится не к какому-то конкретному направлению бизнеса или определенным бизнес-процессам, а требует применения процессно-ориентированного подхода для всей деятельности организации.

Вполне возможно, что операторам персональных данных придется изменить сложившуюся практику работы, чтобы соответствовать требованиям нового регламента, а также внедрить новые средства контроля.

Как мы можем помочь?

Наши специалисты по GDPR помогут оценить, разработать, реализовать и проконтролировать новые процессы защиты данных, необходимые для соблюдения регламента GDPR.

В рамках проведения работ нами используется специализированное программное обеспечение GDPR Quick Check для проведения экспресс-оценки, а также полноценная методология, разработанная международной группой «Грант Торнтон» для обеспечения соответствия требованиям GDPR клиентов, подпадающих под нормы законодательства Европейского Союза.



Другие услуги

по направлениям информационной безопасности и информационных технологий

Обеспечение соответствия требованиям (комплаенс)

Аудит и приведение в соответствие по следующим направлениям:

- Требования ГОСТ Р 57580.1-2017«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»
- Требования стандарта Банка России по обеспечению информационной безопасности (СТО БР ИББС-1.0)
- Требования, предъявляемые к участникам Национальной платежной системы (Положение Банка России №382-П)
- Требования в части обеспечения защиты информации в локальном сегменте сети, с размещенным АРМ КБР (Положение Банка России №552-П)
- Требования законодательства РФ в области обработки и защиты персональных данных
- Требования международного стандарта ISO 27001

ИТ-аудит

- Комплексный ИТ-аудит
- Аудит процессов разработки ИТ-систем
- Оценка эффективности контролей в сервисных организациях
- Аудит ИТ-составляющей системы внутреннего контроля

ИТ-консалтинг

- Разработка ИТ-стратегии
- Поддержка в выборе ИТ-решений в соответствии с бизнес-требованиями заказчиков и организация закупок
- Построение системы управления ИТ-рисками
- Анализ и повышение эффективности инвестиций в ИТ

Консалтинг в области информационной безопасности

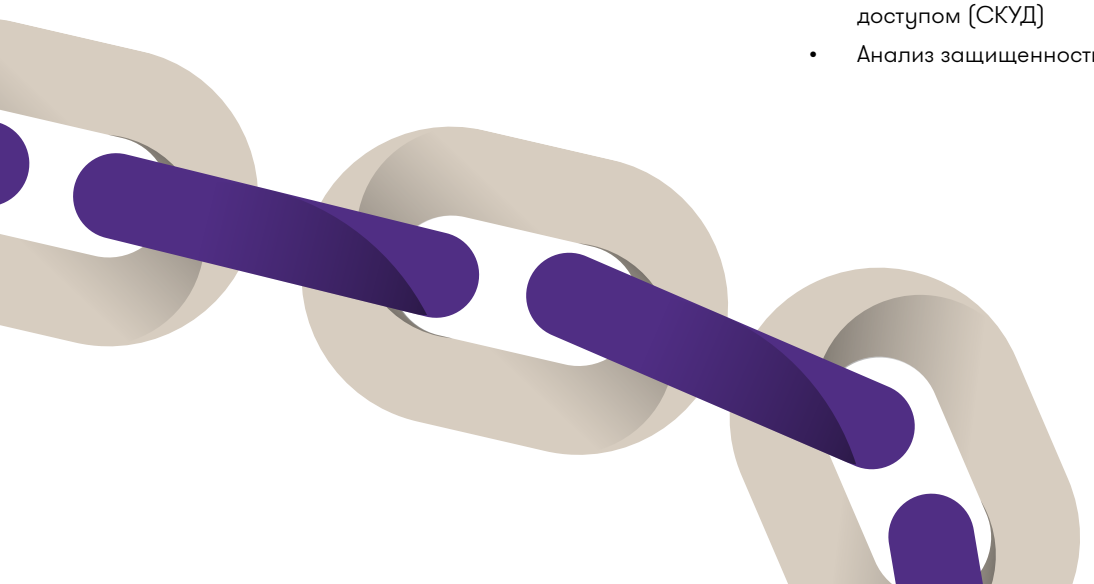
- Построение системы управления информационной безопасностью
- Обеспечение непрерывности бизнеса
- Построение системы управления инцидентами информационной безопасности
- Построение системы управления рисками нарушения информационной безопасности
- Обучение основам информационной безопасности

Blockchain

- Аудит смарт-контрактов
- Тестирование реализации blockchain-решений
- Обеспечение ИБ при проведении ICO

Аппаратная безопасность

- Тестирование защищенности банкоматов
- Тестирование защищенности платежных терминалов
- Аудит безопасности систем контроля и управления доступом (СКУД)
- Анализ защищенности IoT-устройств (Internet of Things)



Контакты

Обратитесь к представителям нашей компании для получения консультаций по интересующим вас вопросам

Алексей Терехов
Вице-президент, Партнер
E bank@fbk.ru

Александр Черненко
Руководитель Отдела по анализу и контролю ИТ-рисков
E ChernenkoA@fbk.ru

ФБК
Grant Thornton

ул. Мясницкая, д. 44/1
Москва, Россия, 101000
Т. +7 495 737-53-53
Ф. +7 495 737-53-47