КСБ-СОФТ

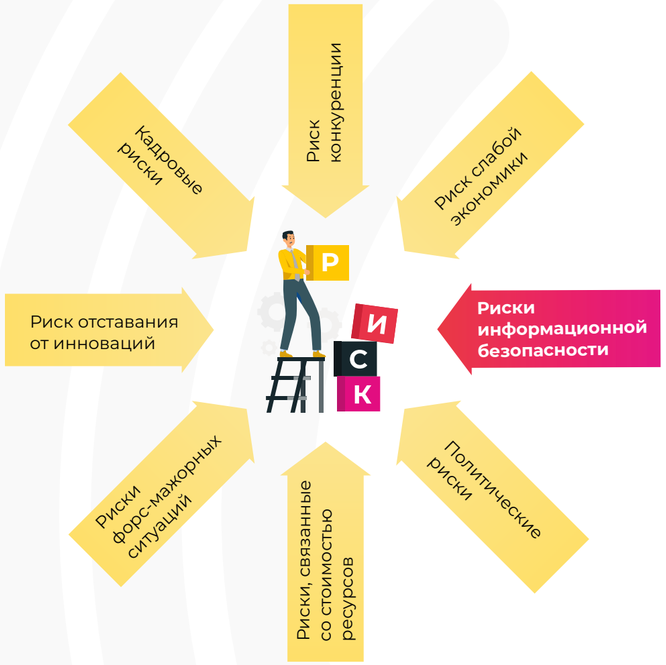
ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

PenTest

ЗАЧЕМ ЗАЩИЩАТЬ ИНФОРМАЦИЮ

Сегодня **информация** – главная нематериальная ценность и основа для раскрытия потенциала бизнеса

И потому она представляет **большой интерес для злоумышленников**



Риски информационной безопасности представляют существенную угрозу для стабильной работы бизнеса и получения прибыли

Чтобы оставаться на конкурентном рынке, бизнесу в своей работе приходится учитывать риски информационной безопасности

Риски информационной безопасности

Утечка данных

Нелегитимный доступ злоумышленника к ресурсам

Остановка деятельности

Потери финансов и репутации

КИБЕРРЕАЛИИ 2023 ГОДА

За последний год значительно увеличилось количество **преступных кибергруппировок** и одиночных **опытных хакеров**

На фоне обострения геополитической ситуации в мире в киберпространстве все больше **начинающих хакеров**

имеют высокий уровень компетенций и возможностей

способны проводить собственные исследования по поиску уязвимостей

разрабатывают новые сценарии для проведения кибератак

размещают готовые сценарии атак в сети

имеют низкий уровень компетенций и возможностей

проводят чаще всего несложные атаки

ищут в сети готовые сценарии для проведения более сложных атак

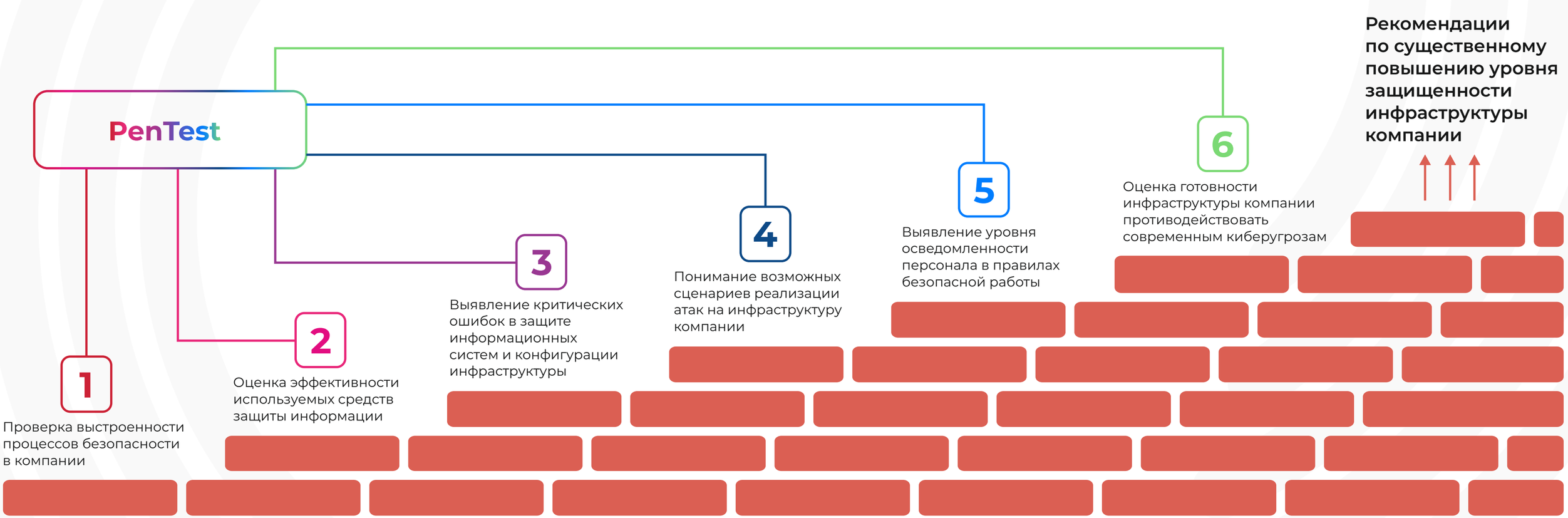
частая цель атак – продвижение политических идей

КАК СТРОИТЬ ЭФФЕКТИВНУЮ СИСТЕМУ ЗАЩИТЫ СЕГОДНЯ

Для эффективной защиты информационных систем в компании важно правильно **оценить** существующие угрозы безопасности и возможные сценарии их реализации, а также **проанализировать,** какие из них **наиболее критичны для текущих бизнес-процессов**

Решить данную задачу поможет комплексная услуга по тестированию на проникновение

Тестирование на проникновение (англ. penetration testing, PenTest, пентест) – это моделирование действий потенциального злоумышленника по получению доступа к информационной системе и содержащейся в ней информации



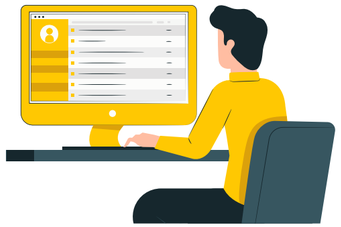
ЧТО МЫ ПРЕДЛАГАЕМ

1 Внутренний пентест информационной системы

Оценим риск компрометации корпоративной сети компании **внутренним нарушителем**

2 Внешний пентест информационной системы

Оценим риск компрометации внутренней инфраструктуры компании через **внешний сетевой периметр**



3 Тестирование безопасности web-ресурса

Оценим возможность реализации наиболее опасных **векторов атак** на web-ресурсы компании

4 Проверка осведомленности персонала

Оценим уровень осведомленности **сотрудников** в вопросах обеспечения информационной безопасности компании

- Согласование условий и времени тестирования
- Работы на специально подготовленном стенде при невозможности тестирования систем в реальных условиях
- Тестирование по ведущим методикам (OWASP, NIST, OSSTM)
- Поиск уязвимостей с помощью автоматизированных инструментов
- Поиск уязвимостей в ручном режиме

КАК МЫ РАБОТАЕМ

Внутренний пентест информационной системы

- оцениваем риск наступления для компании негативных событий*

- получение доступа к конфиденциальной информации или учетной записи пользователя
- получение локальных прав на сервере или рабочей станции сотрудника
- получение доступа к панели администрирования на внутреннем подключенном к сети устройстве или на сетевом оборудовании корпоративной сети
- успешная эксплуатация уязвимости или ошибки конфигурирования безопасности на одном из внутренних сетевых узлов

Внешний пентест информационной системы

- оцениваем риск наступления для компании негативных событий*

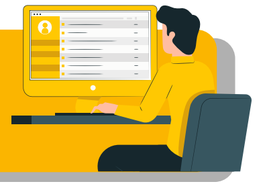
- успешная эксплуатация уязвимости или ошибки конфигурирования на внешнем сервисе
- получение злоумышленником доступа во внутреннюю сеть

Кроме того:

- ☑ **Осуществим** поиск критических уязвимостей и ошибок в настройках оборудования внешнего периметра
- ☑ **Предоставим** свидетельства их присутствия в инфраструктуре организации (при наличии)
- ☑ **Оценим** возможность их эксплуатации злоумышленником

Тестирование безопасности web-ресурса

- оцениваем риск наступления для компании негативных событий*



- успешная эксплуатация как минимум одной уязвимости
- получение доступа к защищаемому сервису и информации в нем
- отказ в обслуживании

Проверка осведомленности персонала

- оцениваем риск наступления для компании негативных событий*

- переход сотрудником по вредоносной ссылке или запуск вложения
- получение злоумышленником идентификационной и аутентификационной информации

---

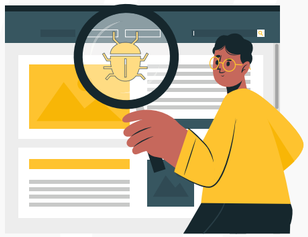
*Невозможность реализации указанных событий в рамках тестирования свидетельствует о высоком уровне защищенности информационного ресурса

ЧТО МЫ ПРЕДЛАГАЕМ ПРОВЕСТИ ДОПОЛНИТЕЛЬНО

Анализ уязвимостей – бесплатное дополнение к пакетам «Внутренний пентест информационной системы» и «Внешний пентест информационной системы»

проверим эффективность принятых локальных мер защиты информации и выявим существующие недочеты информационной инфраструктуры компании

Частые ошибки в организации информационной безопасности



Использование уязвимого программного обеспечения

Некорректное разграничение доступа к конфиденциальной информации

Слабые пароли и пароли «по умолчанию»

Передача информации по открытым каналам связи

Тестирование на устойчивость к DoS-атакам – дополнение к пакету «Тестирование безопасности web-ресурса»

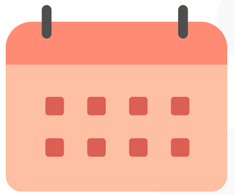
проверим устойчивость внешних web-сервисов и их ресурсов к атакам, направленным на отказ в обслуживании

- Атаки специально сформированными пакетами
- Организация нагрузки посредством специально подготовленных HTTP-запросов
- Имитация повышения пользовательской нагрузки

Тестирование безопасности беспроводных сетей – дополнение к пакету «Внутренний пентест информационной системы»

оценим устойчивость Wi-Fi сети компании к потенциальным атакам

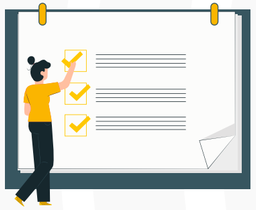
1. Перехват данных, передаваемых между легальным пользователем и точкой доступа
2. Восстановление ключа доступа к Wi-Fi сети
3. Разрыв соединения между точкой доступа и клиентским устройством
4. Имитация поддельной точки доступа для атаки на клиентов беспроводной сети



ЧТО В ИТОГЕ

Оценка риска наступления негативных событий для компании

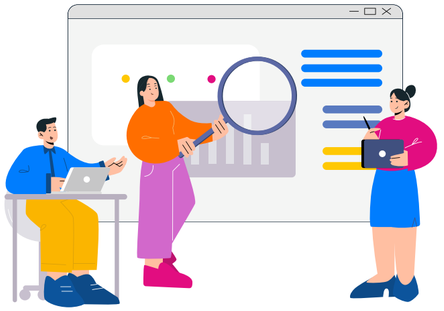
Независимая оценка существующей системы защиты



Рекомендации по устранению существующих критических уязвимостей и ошибок конфигурации

Организационно-технические рекомендации по повышению текущего уровня защищенности

ПОЧЕМУ ИМЕННО МЫ



Тестирование на проникновение от команды пентестеров КСБ-СОФТ – это ваша возможность получить

Индивидуальный подход к потребностям компании и особенностям ее инфраструктуры

Оценку готовности инфраструктуры противодействовать современным киберугрозам

Рекомендации по существенному повышению текущего уровня защищенности инфраструктуры **

Дополнительное бесплатное обслуживание – дополнительный пакет «Анализ уязвимостей»

Постобслуживание - по запросу проверим устранение выявленных уязвимостей и ошибок (проверка до двух раз в удаленном формате)

** – рекомендации для каждой компании носят индивидуальный характер и зависят от многих параметров, в том числе от уровня и обеспечения информационной безопасности инфраструктуры

КСБ-СОФТ

Компания КСБ-СОФТ – системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Лицензия № 110 от 3 апреля 2018
Выдана управлением Федеральной службы безопасности РФ по ЧР

Лицензия № 3111 от 6 декабря 2016
Выдана Федеральной службой по техническому и экспортному контролю

- Анализ уязвимостей и тестирование на проникновение
- Мониторинг и реагирование на инциденты ИБ
- Консалтинг по безопасной разработке и сертификации СЗИ

Наши клиенты – федеральные и региональные органы власти, органы местного самоуправления, государственные и муниципальные учреждения, коммерческие организации, более чем в 80 регионах России

Наша команда ИБ-специалистов реализовала свыше 4000 проектов разной степени сложности. Используя полученный опыт, мы помогаем нашим клиентам подобрать наиболее эффективные решения для защиты их информационных ресурсов

- Аудит информационной безопасности
- Обеспечение безопасности КИИ и АСУ ТП
- Защита информации в ГИС и ИСПДн

Используемые в работе практики и методики

Специализированные утилиты и скрипты, разработанные командой наших пентестеров для тестирования безопасности ИТ-инфраструктуры организаций

Цикл безопасной разработки, созданный в соответствии с передовыми практиками

Активная деятельность в российском комьюнити безопасной разработки

СВЯЖИТЕСЬ С НАМИ

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru

МНЕНИЕ ИНТЕГРАТОРА

ПОДКАСТ «SOCRAT ЗА СТЕКЛОМ»

САЙТ КОМПАНИИ