ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

ТЕСТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРОНИКНОВЕНИЕ

АНАЛИЗ ЗАЩИЩЕННОСТИ

МЫ ПРОВЕРИМ ЗАЩИЩЕННОСТЬ ВАШИХ СИСТЕМ

КОМПЕТЕНЦИИ

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

› 10 лет опыта | **› 100** Заказчиков | **› 600** защищенных систем

Защита систем: сервисы ДБО, государственные информационные системы, внутренние локальные сети, сайты, системы управления производством и другие.

Эксперты Центра Кибербезопасности УЦСБ обладают необходимым опытом и компетенциями в области выявления уязвимостей. Для каждого проекта мы формируем индивидуальную проектную команду, состоящую из специалистов, квалификация которых подтверждается:

» **Наличием международных сертификатов:**
CEH, CHFI, OSCP, OSWE, OSCE, CISA, CISSP

» **Зарегистрированными бюллетенями безопасности на выявленные уязвимости:**

- CVE-2015-1010: Rockwell Automation RSView32
- CVE-2017-7907: Schneider Electric Wonderware Historian Client
- CVE-2017-9627, CVE-2017-9629, CVE-2017-9631: Schneider Electric Wonderware ArchestrA Logger
- CVE-2018-18981: Rockwell Automation FactoryTalk Services Platform

» **Публикациями в профессиональных журналах и блогах:**

- Блог на Хабре, аккаунт @usscltd
- Блог на Хакере, аккаунт @s0i37

» **Публикации в международных журналах:** Pentest Magazine, HackMag

» **Выступления на отраслевых конференциях:** PHDays, ZeroNights

Аналитический центр УЦСБ взаимодействует с центром круглосуточного мониторинга информационной безопасности — USSC-SOC:

участвует в расследовании компьютерных инцидентов и реагировании на них

осуществляет мониторинг атак в сети Интернет и уведомляет владельцев Интернет-ресурсов о возможной компрометации

предоставляет информацию о выявленных атаках и индикаторах компрометации

СПЕКТР УСЛУГ

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Мы проверим защищенность ваших информационных систем от и до: начиная с безопасности исходного кода приложений и заканчивая уровнем осведомленности специалистов.

- **Анализ защищенности мобильных и веб-приложений, аудит безопасности исходного кода приложений** — находим уязвимые места, которыми можно воспользоваться для доступа к их компонентам, конфиденциальной информации и атакам на пользователей.

- **Внешний и внутренний анализ защищенности корпоративных и беспроводных сетей** — находим уязвимые места, которыми можно воспользоваться для доступа к ресурсам и конфиденциальной информации Заказчика, как внутренним, так и в Интернете.

- **Тестирование методом социальной инженерии** — оцениваем знания сотрудников Заказчика в вопросах информационной безопасности и соблюдение ими внутренних регламентов.

МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

«ЧЕРНЫЙ ЯЩИК»

нет санкционированного доступа

«СЕРЫЙ ЯЩИК»

минимальный или пользовательский доступ

«БЕЛЫЙ ЯЩИК»

неограниченный доступ

РЕЗУЛЬТАТ

Результатом проведенного анализа защищенности является экспертное заключение с перечнем всех выявленных уязвимостей и подробным планом действий для устранения уязвимостей и защиты от атак на ресурсы компании. Все уязвимости подробно описываются, подтверждается возможность реализации атак с их использованием.

МЫ РЕАЛИЗУЕМ КОМПЛЕКСНЫЕ ПРОЕКТЫ ПО АНАЛИЗУ ЗАЩИЩЕННОСТИ.
В ЧИСЛЕ ВЫПОЛНЕННЫХ ПРОЕКТОВ:

- анализ защищенности внешнего периметра, беспроводных сетей, локальной сети и тестирование методом социальной инженерии для крупнейшего агрохолдинга РФ
- тестирование веб-приложения, внешнее и внутреннее тестирование на проникновение для одного из лидирующих российских негосударственных пенсионных фондов
- анализ защищенности веб-сервисов и мобильных приложений на базе Android и iOS, тестирование веб-приложения, внешнее и внутреннее тестирование на проникновение для одного из лидеров рынка добровольных видов страхования
- анализ защищенности веб-сервисов, аудит безопасности исходного кода приложений для федеральной розничной сети российского оператора сотовой связи
- анализ защищенности внешнего периметра и локальной сети для международных аэропортов федерального значения
- анализ защищенности внешнего периметра, веб-сервисов, локальной сети, тестирование методом социальной инженерии для одного из крупнейших банков Уральского региона

ООО «УЦСБ»
+7 (343) 379-98-34
info@ussc.ru
sec.ussc.ru
USSC