ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

ТЕСТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРОНИКНОВЕНИЕ

АНАЛИЗ ЗАЩИЩЕННОСТИ

МЫ ПРОВЕРИМ ЗАЩИЩЕННОСТЬ ВАШИХ СИСТЕМ

КОМПЕТЕНЦИИ НАПРАВЛЕНИЯ

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

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

Защита систем: банковские сервисы, 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:**
OSCP, OSWE, OSCE, OSWP, CISA, CISM, CISSP, CRISC

» **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

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

» **Выступлениями на отраслевых конференциях:** PHDays, ZeroNights, SOC-форум

Пентестеры Центра кибербезопасности УЦСБ взаимодействуют с центром круглосуточного мониторинга информационной безопасности — USSC-SOC, который:

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

Проверим безопасность вашей ИТ-инфраструктуры, информационных систем и программных продуктов. Выявим возможные векторы атаки и дадим рекомендации, как их предотвратить. Поможем принять меры заблаговременно — до наступления события ИБ.

Анализ защищенности

- внешнего периметра
- внутренней сети
- беспроводных сетей
- логического функционала веб- и мобильных приложений
- от атак типа «отказ в обслуживании» (DoS)
- тестирование методами социальной инженерии
- RedTeam: оценка эффективности работы SOC по отслеживанию и предотвращению атак

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.

Отраслевой опыт

Финансы и страхование | Госсектор | ИТ и телеком | Энергетика

Транспорт | Машиностроение | Сельское хозяйство | Нефтегаз

Металлургия | Ритейл

КЕЙСЫ НА ОСНОВЕ ВЫПОЛНЕННЫХ ПРОЕКТОВ

Киберучения для «Союзмультфильма»: как имитация атак помогает закрепить результаты обучения сотрудников основам ИБ

«Союзмультфильм» запланировал внутреннее обучение для повышения информированности своей команды в области кибербезопасности. Организаторы решили не ограничивать сотрудников только теоретическим освоением темы. Для этого потребовалось провести специальные негласные киберучения. В этом помогла команда Центра кибербезопасности УЦСБ.

Зачем компании нужны регулярные аудиты защиты информации? Опыт медиахолдинга Rambler&Co

В Rambler&Co, крупнейшем медиахолдинге России, к информационной безопасности корпоративной сети относятся с особенным вниманием: в компании собственный департамент кибербезопасности, который постоянно совершенствует системы защиты, обучает сотрудников и проводит «полевые» учения, имитируя различные способы взлома и кибермошенничества. Рассказываем, как прошел аудит защищенности корпоративных цифровых ресурсов.

Подробнее об этих кейсах читайте на сайте Центра кибербезопасности УЦСБ

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