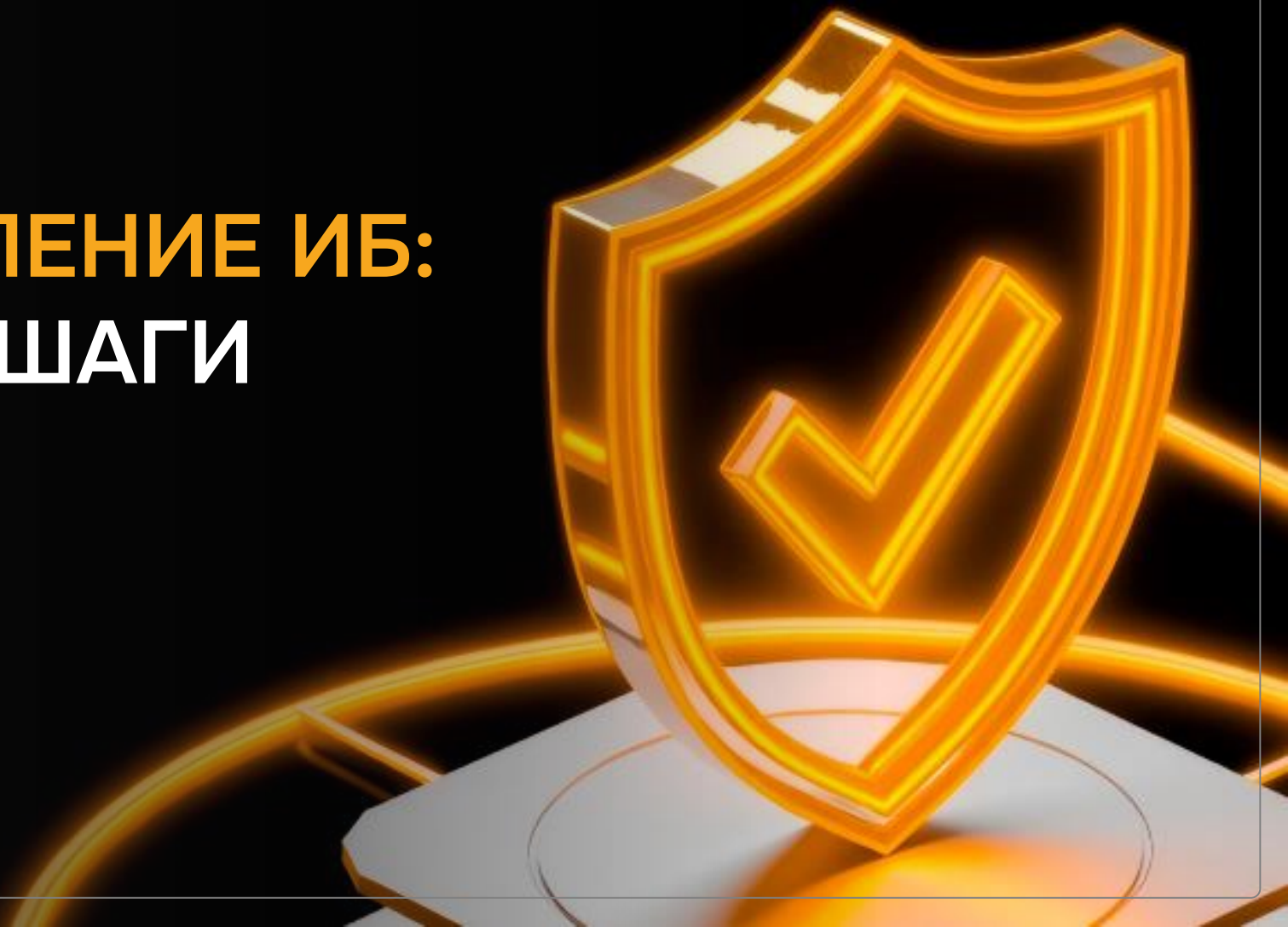
ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

ЭКСПРЕСС-УСИЛЕНИЕ ИБ: ПРАКТИЧЕСКИЕ ШАГИ И ПРИЕМЫ



sec.ussc.ru

АЛЕКСЕЙ ШАНИН

- Директор департамента технической поддержки продаж УЦСБ
- Опыт реализации комплексных ИБ-проектов — от аудита до сопровождения
- Опыт разработки и внедрения средств защиты, мониторинга и контроля состояния защищенности АСУ ТП
- Выявление потребностей и решение задач Заказчиков

ДМИТРИЙ ЗУБАРЕВ

- Заместитель директора аналитического центра УЦСБ
- Опыт реализации комплексных проектов по анализу защищенности и тестированию на проникновение
- Опыт расследования инцидентов ИБ

О ЧЕМ ПОГОВОРИМ

01 Факторы развития систем кибербезопасности

02 Кейс из транспортной отрасли

03 Практические рекомендации по повышению ИБ

04 Что ещё нужно для быстрого усиления защиты

ФАКТОРЫ РАЗВИТИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ

- ЭВОЛЮЦИОННОЕ РАЗВИТИЕ
- ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ

ФАКТОРЫ РАЗВИТИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ

- ЭВОЛЮЦИОННОЕ РАЗВИТИЕ
- ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ
- КРИЗИСНЫЕ МЕРЫ

VS

ЦЕЛЕВЫЕ АТАКИ

- **77%** Компаний становятся жертвами успешной атаки в течение одного года
- **101** Среднее количество дней от первых проявлений последствий атаки до ее обнаружения
- **73%** На столько снизится ущерб от инцидента, если его удастся обнаружить в течение первой недели

КЕЙС ИЗ ТРАНСПОРТНОЙ ОТРАСЛИ

АНАМНЕЗ

01 Предприятие среднего размера

02 Субъект КИИ, транспортная отрасль

03 Подозрение на присутствие нарушителей

04 Общая тревога в отрасли

05 Отсутствие доверия к внутренней ИБ

ИНСТРУМЕНТАРИЙ

- **01** Сценарии интервью
- **02** Сканер уязвимостей
- **03** Специализированные инструменты
- **ЦК** Творческий подход

ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИБ

ПРОВЕРИЛИ

- Общую организацию ИБ
- Управление ИТ-активами
- Управление обновлениями и уязвимостями
- Процессы восстановления работоспособности
- Взаимодействие с внешними субъектами
- Организацию системы защиты информации, включая архитектуру сети и сегментацию

ВЫЯВИЛИ

- Ответственные назначены, но ресурсов недостаточно
- Состав информационных систем не зафиксирован
- Обновления устанавливаются ситуативно и не на весь парк, управление уязвимостями отсутствует
- Резервные копии сохраняются, но не проверяются
- Недокументированные стыки сегментов и маршрутизация на пограничном оборудовании

СКАНИРОВАНИЕ УЯЗВИМОСТЕЙ

ПРОВЕРИЛИ

- Репрезентативную выборку серверов и рабочих мест (разные информационные системы, операционные системы и др.)
- Тестирование в режиме аудита с предоставлением учетных данных

ВЫЯВИЛИ

- Множество сетевых узлов с уязвимостями CVSSv3 10.0
- Уязвимые сетевые узлы под управлением неподдерживаемых редакций ОС
- Мисконфигурации сетевых сервисов

РЕЗУЛЬТАТ

Отчет с указанием приоритетов и путей устранения уязвимостей

СЛУЖБА КАТАЛОГОВ

ПРОВЕРИЛИ

- Автоматические проверки соответствия настроек лучшим практикам ИТ и ИБ
- Групповые политики
- Политики безопасности
- Учетные записи и их атрибуты

ВЫЯВИЛИ

- Уязвимости и некорректные настройки AD
- Бессрочные пароли привилегированных учетных записей (в т.ч. обезличенных)
- Слабые настройки политик безопасности (парольная политика, отключенный аудит и др.)
- Включенные службы, которые можно использовать для эксплуатации уязвимостей (например, TGT и Spooler)

РЕЗУЛЬТАТ

Отчет по инструментальным проверкам, а также перечень недостатков с описанием путей устранения

ЛОКАЛЬНЫЕ НАСТРОЙКИ СЕТЕВЫХ УЗЛОВ

ПРОВЕРИЛИ

- Локальные политики безопасности
- Учетные записи и их атрибуты
- Установленное программное обеспечение
- Активные сервисы и ПО
- Тестирование в режиме аудита с предоставлением учетных данных

ВЫЯВИЛИ

- Бессрочные пароли привилегированных учетных записей (в т.ч. обезличенных)
- Слабые настройки политик безопасности (парольная политика, отключенный аудит и др.)
- Программное обеспечение, не относящееся к производственным функциям

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ ИБ

НАСТРОЙКИ ОС LINUX

ПРОБЛЕМА	РЕКОМЕНДАЦИИ
Срок действия паролей	Настроить парольную политику «/etc/login.defs»: ▪ «PASS_MAX_DAYS»: 90 дней или меньше ▪ «PASS_MIN_DAYS»: 1 день или больше ▪ «PASS_WARN_AGE»: 7 дней
Требования к сложности	Настроить требования к паролю «/etc/pam.d/common-password» или «/etc/pam.d/password-auth»: ▪ «minlen»: 12 или больше ▪ «difok»: 5 или больше ▪ «dcredit»: «-1» ▪ «ucredit»: «-1» ▪ «lcredit»: «-1» ▪ «remember»: 5 или больше
Блокировка	Настроить требования к паролю «/etc/pam.d/common-password» или «/etc/pam.d/password-auth»: ▪ «deny»: 3 попытки ▪ «unlock_time»: 1800 секунд
Персональные учетные записи	Создать УЗ для каждого администратора sudo adduser <УЗ> или sudo useradd <УЗ>. Вывести список УЗ с интерактивным входом, установить пароли sudo passwd <УЗ> или заблокировать sudo passwd -l <УЗ> или sudo usermod -L <УЗ> : sudo grep \ -e "/bin/bash" \ -e "/bin/sh" \ /etc/passwd

НАСТРОЙКИ ОС LINUX

ПРОБЛЕМА	РЕКОМЕНДАЦИИ
Удаленный доступ	Создать группу «ssh-users» (sudo addgroup ssh-user или sudo groupadd ssh-user). Добавить в созданную группу УЗ администраторов и служебные УЗ с удаленным доступом: «sudo usermod -aG ssh-user <УЗ>» Добавить в конфигурационный файл «/etc/ssh/sshd_config» строку: «AllowGroups ssh-users» Перезапустить службу ssh: «sudo systemctl restart ssh»
Учетная запись root	В файле «/etc/ssh/sshd_config» изменить строку: «PermitRootLogon no» Перезапустить службу ssh: «sudo systemctl restart ssh» Заблокировать УЗ в ОС «sudo passwd -l root» или «sudo usermod -L root»
Удаленный доступ по паролю	Выпустить для всех УЗ администраторов ssh-ключи с passphrases. Добавить открытые ключи для всех УЗ администраторов на все серверы ОС Linux. Добавить в файл «/etc/ssh/sshd_config» строки: ▪ PasswordAuthentication no ▪ PermitEmptyPasswords no ▪ PubkeyAuthentication yes ▪ AuthenticationMethods publickey Перезапустить службу ssh: «sudo systemctl restart ssh»
Аудит	Настроить параметры и правила службы auditd. Настроить ротирование системных журналов
Неиспользуемые службы	Вывести список активных служб, а также служб, добавленных в автозагрузку: sudo systemctl list-units \ --type=service --state=active Отключить неиспользуемые службы: «sudo systemctl disable –-now <служба>»

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

ПРОВЕРИЛИ

- Средства межсетевого экранирования (NGFW) и другие средства сетевой безопасности
- Средства антивирусной защиты
- Средства резервного копирования и восстановления информации
- Другие средства защиты информации

ВЫЯВИЛИ

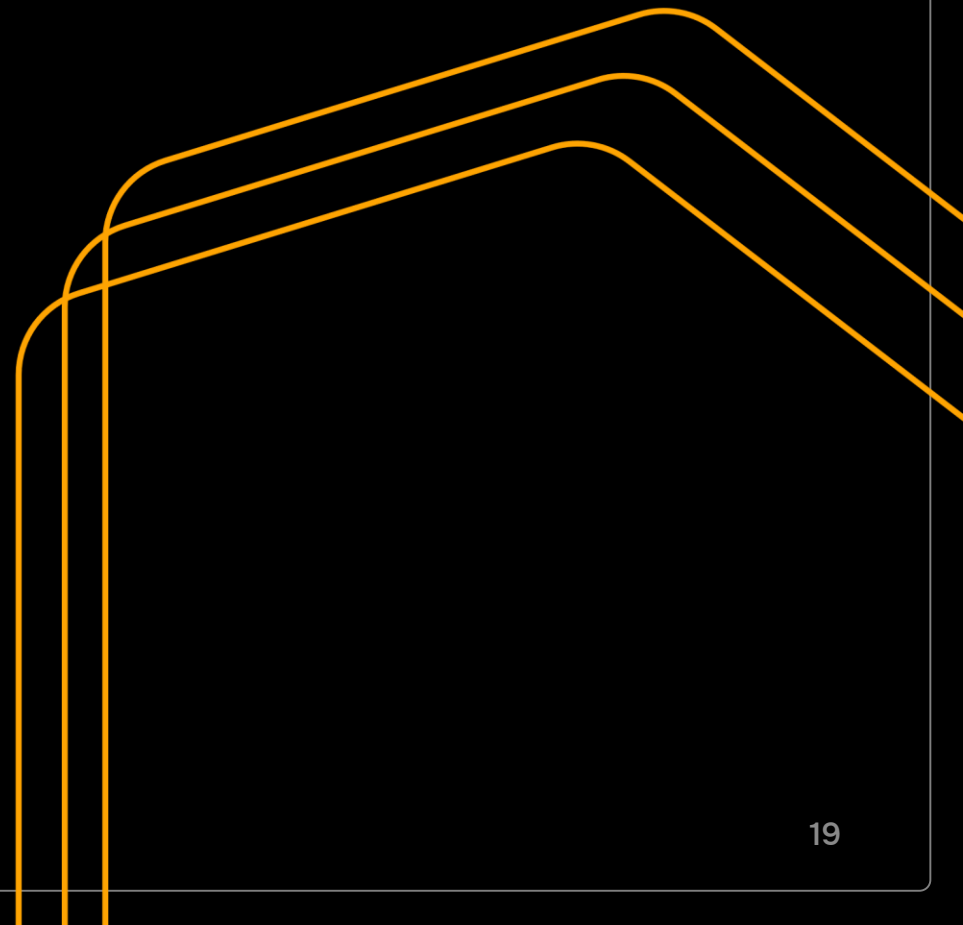
- Триальные лицензии и истекшие сертификаты
- Удаленный доступ по логину/паролю
- Отсутствие ограничений доступа к интерфейсам администрирования
- Неперсональные локальные учетные записи
- Мисконфигурации кластеров NGFW/ACO
- Отключенная инспекция L7 и недостаточная фильтрация сетевых взаимодействий
- Включенные неиспользуемые порты
- Отсутствие задач обновления и проверок

ДОРОЖНАЯ КАРТА

ПЕРВООЧЕРЕДНЫЕ МЕРОПРИЯТИЯ

ЧТО ЕЩЁ НУЖНО ДЛЯ БЫСТРОГО УСИЛЕНИЯ ЗАЩИТЫ?

- Оценка текущего состояния
- Харденинг
- ...



МОНИТОРИНГ

С КАКИМИ ФАКТОРАМИ РИСКА РАБОТАЕТ?

- Когда часть инфраструктуры защищена, а часть нет
- Действия инсайдера
- Скрытые пробелы в процессах ИБ
- Неучтённые активы
- 0day

КАКИЕ ЗАДАЧИ РЕШАЕТ?

- Локализация атаки
- Принятие мер по нейтрализации угрозы
- Расследование инцидента
- Устранение причин инцидента, предотвращение повторений

КОНТРОЛЬ УРОВНЯ ЗАЩИЩЁННОСТИ

ЗАЧЕМ НУЖЕН?

- Позволяет оценить корректность и эффективность принимаемых мер
- Помогает определить слабые места и зоны роста

КАК ПРОВОДИТЬ?

- Самый практичный вариант — быстрый пентест

ОСОБЕННОСТИ МЕР ПО УСИЛЕНИЮ ИБ

Мониторинг и контроль

- Необходимость специфичных компетенций и ресурсов
- При реализации в полном объёме — ресурсоёмкие процедуры
- Для решения обеих задач распространена практика привлечения внешних исполнителей

ОСОБЕННОСТИ МЕР ПО УСИЛЕНИЮ ИБ

Аудит и харденинг

- Задачи частично могут решаться штатным персоналом
- Глубокая проработка также требует специфичных компетенций
- Полный аудит — ресурсоёмкая задача
- Полный аудит с применением настроек силами исполнителя — ещё более ресурсоёмкая задача
- Решение — выделение критичных систем и их типовых конфигураций

ЭКСПРЕСС-УСИЛЕНИЕ ИБ: WRAPPING UP

Быстрый аудит

Оценка текущего состояния ИБ, покрывающая типовые конфигурации критичных систем

Устранение недостатков и харденинг систем

Конфигурация систем по рекомендациям экспертов в области ИБ

Внедрение мониторинга

Постановка на мониторинг наиболее критичных систем для обнаружения атак и нейтрализации угроз

Контрольное мероприятие

Проверка корректности и эффективности принятых ранее мер

ЭКСПРЕСС-ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ

ЭКСПРЕСС-ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ

4 модуля услуги

01
Экспресс-аудит

02
Харденинг

03
Мониторинг и реагирование (опция)

04
Экспресс-пентест (опция)

Для большей результативности мы рекомендуем воспользоваться всеми модулями услуги. Однако вы можете сократить их количество, отказавшись от тех, которые являются опциональными.

01 ЭКСПРЕСС-АУДИТ

ЦЕЛЬ

собрать сведения о критичных узлах и средствах защиты ИТ-инфраструктуры, оценить текущее состояние её защищенности и использовать полученные результаты как основу для последующих этапов работ

Что мы сделаем:

Проведем интервью по ключевым темам:

- Конфигурации АСО
- Политики МЭ
- Сегментирование
- Службы каталога
- Почтовые сервисы
- Веб-серверы
- Платформы виртуализации
- Серверы и АРМ: Windows, Linux
- СЗИ: SIEM, DLP, АВЗ, IDS, SOAR, прокси-серверы
- Политики ИБ

01 ЭКСПРЕСС-АУДИТ

Проведем очное обследование:

- Экспресс-сканирование серверов и АРМ
- Инструментальный сбор данных о службах каталога
- Анализ вашей карты корпоративной сети
- Сбор типовых конфигураций АСО и МЭ

02 ХАРДЕНИНГ

ЦЕЛЬ

повысить уровень защищенности инфраструктуры
за счет совершенствования настроек систем
по лучшим практикам

Что мы сделаем:

- Предоставим инструкции, рекомендации и инструменты для безопасной настройки критичных систем, выявленных в ходе экспресс-аудита
- Выставим приоритеты по выполнению и при необходимости снабдим инструкции экспертными комментариями
- Укажем возможные риски влияния изменений на инфраструктуру и предложим оптимальные сценарии реализации

03 МОНИТОРИНГ И РЕАГИРОВАНИЕ (ОПЦИЯ)

ЦЕЛЬ

обеспечить мониторинг инцидентов ИБ
и эффективное реагирование при их обнаружении

Что мы сделаем:

Основной сценарий – подключение к УЦСБ SOC:

- Подключим критичные узлы: настроим VPN-тоннель, установим ОС и компоненты SIEM, подготовим кластер для приема событий
- Настроим SIEM и подключим источники событий
- Сформируем и адаптируем набор правил корреляции под вашу инфраструктуру

Ограничение по подключению в рамках экспресс-услуги – до 100 активов или 200 EPS

03 МОНИТОРИНГ И РЕАГИРОВАНИЕ (ОПЦИЯ)

Альтернативный сценарий – эффективное использование вашей SIEM:

Предоставим базовый пакет правил корреляции для вашей SIEM, позволяющих выявлять типовые признаки вредоносной активности по принципу «20% усилий для 80% результата»

Проведем краткое обучение ваших сотрудников по использованию пакета правил для обнаружения кибератак

04 ЭКСПРЕСС-ПЕНТЕСТ (ОПЦИЯ)

ЦЕЛЬ

подтвердить устранение наиболее критичных уязвимостей и недостатков ИБ по выданным рекомендациям

Что мы сделаем:

- Проверим отсутствие критичных уязвимостей и недостатков ИБ внешних ресурсов, которые могут дать доступ к внутренней сети
- Проверим отсутствие критичных уязвимостей и недостатков ИБ внутренней сети, позволяющих получить привилегированный доступ к ключевым компонентам ИТ-инфраструктуры
- Сосредоточимся на ресурсах и системах, задействованных в предыдущих блоках, чтобы убедиться, что рекомендации были реализованы корректно и их эффект достигнут

РЕКОМЕНДАЦИИ И СРОКИ

- Для максимальной результативности мы рекомендуем воспользоваться всеми модулями услуги
- Вы можете сократить их количество, однако обязательными остаются модули 1 и 2
- Срок оказания услуги – от 13 рабочих дней при максимальной вовлечённости Заказчика
- Подключение к УЦСБ SOC – 10–15 рабочих дней, срок действия подключения – 6 месяцев

ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

sec.ussc.ru

cybersec@ussc.ru