УЦСБ

Мониторинг инцидентов ИБ в ОКИИ

IV вебинар цикла «Обеспечение безопасности объектов КИИ в рамках 187-ФЗ»

УЦСБ

ПЛАН ВЕБИНАРА

01 Основные термины

02 Мониторинг информационной безопасности

03 Взаимодействие с ГосСОПКА

04 Требования к сотрудникам информационной безопасности

05 Практическая часть мониторинга и выявления инцидентов ИБ

УЦСБ

ОСНОВНЫЕ ТЕРМИНЫ

Событие ИБ

Пример

Неудачная авторизация пользователя в ИС

Инцидент ИБ

Пример

Несколько неудачных попыток авторизации пользователя в ИС за короткий промежуток времени

Компьютерная атака, или кибератака

Пример

DDoS-атака

УЦСБ

КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ

Классификация инцидентов:

- по типам / видам
- по степени критичности / степени возможного ущерба для организации

Типы инцидентов:

Вредоносные программы

вирусы, троянские программы
и другое

Утечка данных

несанкционированный доступ
к конфиденциальной информации

Отказ в обслуживании

DDoS-атаки и другие атаки на доступность

Мошенничество

фишинг, мошенничество с использованием
вредоносных программ

Внутренние угрозы

действия сотрудников, нарушающие
политику безопасности

УЦСБ

КЛАССИФИКАЦИЯ НКЦКИ

Компьютерные инциденты

- Вовлечение контролируемого ресурса в инфраструктуру ВПО
- Замедление работы ресурса в результате DDoS-атаки
- Заражение ВПО
- Захват сетевого трафика
- Использование контролируемого ресурса для фишинга
- Компрометация учетной записи
- Несанкционированное изменение информации
- Несанкционированное разглашение информации
- Публикация на запрещенном законодательством РФ информационном ресурсе
- Рассылка спам-сообщений с контролируемого ресурса
- Успешная эксплуатация уязвимости

Компьютерные атаки

- DDoS-атака
- Неудачные попытки авторизации
- Попытки внедрения ВПО
- Попытки эксплуатации уязвимости
- Публикация мошеннической информации
- Сетевое сканирование
- Социальная инженерия

УЦСБ

МОНИТОРИНГ ИБ

ЦЕЛЬ → своевременное выявление и пресечение несанкционированных действий

ОСНОВНЫЕ ЭТАПЫ МОНИТОРИНГА

1. Выявление инцидента
2. Реагирование на инцидент
3. Анализ последствий
4. Устранение негативных последствий
5. Анализ инцидентов информационной безопасности
6. Формирование и реализация рекомендаций по доработке системы защиты, анализ предпринятых действий и предотвращение повторения инцидентов информационной безопасности

УЦСБ

МОНИТОРИНГ ИБ

ПО для мониторинга ИБ

SIEM

IRP

SOAR

Своевременное выявление инцидентов позволяет:

- предотвратить утечку данных, нарушение работы информационных систем
- минимизировать последствия инцидентов и их повторное возникновение
- повысить эффективность реагирования на инциденты
- защитить имеющиеся информационные активы
- соблюдать требования законодательства

УЦСБ

МОНИТОРИНГ ИБ

ВАЖНО

Субъекты КИИ обязаны реагировать на компьютерные инциденты в порядке, утвержденном ФСБ России, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ.

ВЗАИМОДЕЙСТВИЕ С ГОССОПКА

Федеральный закон № 187-ФЗ

«О безопасности КИИ Российской Федерации»

Федеральный закон № 152-ФЗ

«О персональных данных»

Приказ ФСБ России № 367

«Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных…»

Приказ ФСБ России № 196

«Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»

Приказ ФСБ России № 282

«Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах в отношении значимых объектов критической информационной инфраструктуры Российской Федерации…»

Приказ ФСБ России № 77

«Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации…»

Приказ ФСТЭК России № 21

«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Методические рекомендации Банка России от 26.10.2023 № 14-МР

«По выполнению кредитными и некредитными финансовыми организациями мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации…»

Рекомендаций в области стандартизации Банка России РС БР ИББС-2.5-2014

«Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности»

УЦСБ

ОБЯЗАТЕЛЬСТВА И СРОКИ

- **Субъекты КИИ обязаны незамедлительно информировать НКЦКИ (ФСБ России) или ФинЦЕРТ (Банк России) о компьютерных инцидентах:**
  - для значимых ОКИИ – **3 часа**
  - для иных ОКИИ – **24 часа**

- Факт неправомерной или случайной передачи персональных данных третьим лицам необходимо сообщить в Роскомнадзор **24 часов** и предоставить результаты внутреннего расследования в течение **72 часов**

Субъекты КИИ обязаны предоставить информацию о компьютерных инцидентах в ГосСОПКА

Необходимо обеспечить хранение зарегистрированных событий ИБ:

- в банковской сфере: обнаруженных в рамках банковских платежных технологических процессов — в течение **5 лет**, об иных событиях ИБ – в течение **3 лет**
- для остальных сфер — в течение **6 месяцев**

УЦСБ

ТРЕБОВАНИЯ К СОТРУДНИКАМ ИБ

Руководитель

Высшее профессиональное образование

или

Пройденное обучение по программе профессиональной переподготовки по направлению «Информационная безопасность»

Стаж работы — не менее 3х лет

Линейный специалист

Высшее профессиональное образование

или

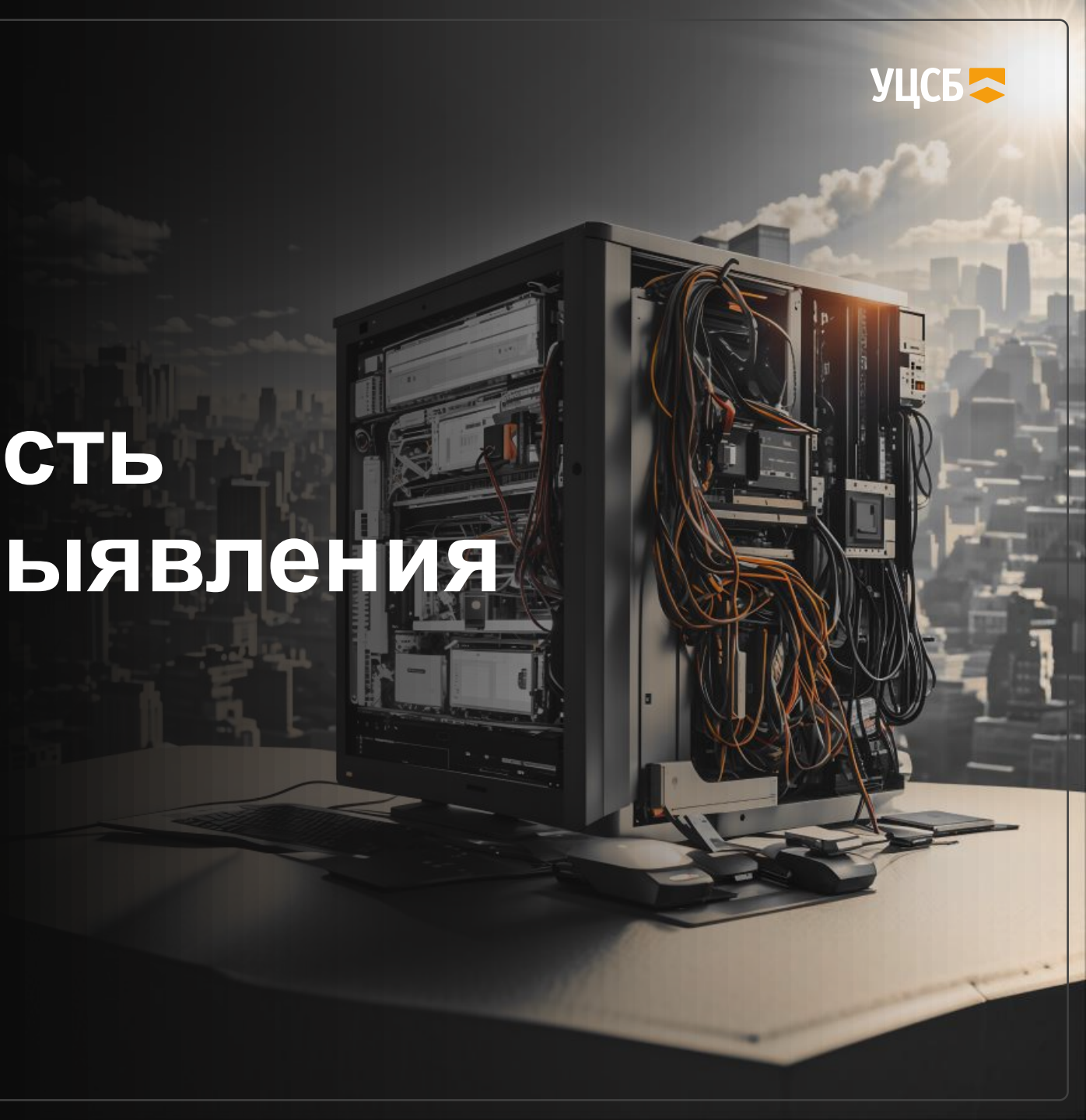
Пройденное обучение по программе профессиональной переподготовки по направлению «Информационная безопасность»

Стаж работы — любой

Необходимо повышать квалификации по направлению «Информационная безопасность» каждые **3 года**

УЦСБ

Практическая часть мониторинга и выявления инцидентов ИБ



УЦСБ

САМЫЕ АТАКУЕМЫЕ ОТРАСЛИ*

15%
Госсектор

11%
Медицина

10%
Наука и образование

9%
Финансовые учреждения

8%
ИТ-компании

8%
Промышленность

* Отчет PTSecurity Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть пятая. 19.12.2023

САМЫЕ РАСПРОСРАНЕННЫЕ АТАКИ

- Взаимодействие пользователя
  User Execution: T1204
- Целевой фишинг с вредоносным вложением
  Spearphishing Attachment: T1566.001
- Эксплуатация служб удаленного доступа
  Exploitation of Remote Services: T1210

Популярные векторы атак

Зараженные съемные носители

Небезопасные Wi-Fi

Небезопасное подключение к сети Интернет с АРМ инженеров и администраторов

УЦСБ

ЗНАЧИМЫЕ УТЕЧКИ ДАННЫХ

В 1,5 раза

Вырос объём украденных данных в крупных компаниях в сравнении 2022 и 2023 года*

1 из 10 утечек

Публично подтверждается

2023

- Ретейл и финансы — лидеры по объёму утечек пользовательских данных
- Ретейл и интернет-сервисы — лидеры по числу фактов утечек
- Telegram — основной канал распространения публичных утечек

* Отчёт о значимых утечках данных в России за 2022-2023 года от «Лаборатории Касперского»

УЦСБ

КАК ЗАЩИТИТЬСЯ

- использовать защитные инструменты с функциями контроля приложений, блокировки сетевых атак, проверки репутации веб-сайтов и сканирования загружаемых файлов
- регулярно повышать осведомлённость сотрудников о современных методах и приёмах злоумышленников
- защищать основные корпоративные каналы
- применять технологии изоляции приложений против эксплуатации удаленных служб
- применять Sandbox для выявления фишинговой активности

МОНИТОРИНГ СРЕДСТВ ЗАЩИТЫ

- системы обнаружения / предупреждения вторжений
- межсетевые экраны
- приложения для безопасного тестирования и анализа потенциально опасного программного кода или файлов
- системы антивирусной защиты
- системы контроля приложений
- средства защиты от целевых атак и сложных угроз
- средства предотвращения утечек конфиденциальной информации
- системы NTA и XDR

ЗАЧЕМ НУЖЕН МОНИТОРИНГ

Мониторинг информационной безопасности позволяет предотвратить или существенно снизить негативные последствия от атаки или инцидента ИБ:

- прерывания бизнес-процессов
- нарушение конфиденциальности, целостности или доступности информационных систем компании
- потерю производительности
- ущерб с точки зрения материальных затрат или репутации
- утечка конфиденциальных данных, кража интеллектуальной собственности

УЦСБ

SOC

Функции центра мониторинга безопасности:

- активный мониторинг IT-среды и сбор данных об инцидентах
- анализ подозрительных событий и определение характера и степени опасности угроз
- реагирование на угрозы и принятие мер по их устранению и минимизации ущерба
- восстановление после инцидента, включая восстановление пострадавших систем и файлов из резервных копий
- расследование инцидентов для определения причин и предотвращения подобных ситуаций в будущем
- ведение реестра ресурсов и обеспечение их безопасности с использованием соответствующих информационных технологий и продуктов

УЦСБ

КАК ВЫБРАТЬ НУЖНЫЙ SOC?

+ соответствует всем требованиям законодательства РФ в области ИБ
+ обладает лицензией ФСТЭК России на мониторинг ИБ, средств и систем информатизации
+ является корпоративным центром ГосСОПКА класса А
+ подключен к Национальному координационному центру по компьютерным инцидентам (НКЦКИ) и ФинЦЕРТ
+ работает с отечественными производителями ПО в области обеспечения ИБ, в статусе Managed Security Service Provider (MSSP)
+ сформирована команда экспертов из области защиты информации, мониторинга, исследования и атрибуции угроз

УЦСБ

КАК ВЫБРАТЬ НУЖНЫЙ SOC?

- \+ соответствует всем требованиям законодательства РФ в области ИБ
- \+ обладает лицензией ФСТЭК России на мониторинг ИБ, средств и систем информатизации
- \+ является корпоративным центром ГосСОПКА класса А
- \+ подключен к Национальному координационному центру по компьютерным инцидентам (НКЦКИ) и ФинЦЕРТ
- \+ работает с отечественными производителями ПО в области обеспечения ИБ, в статусе Managed Security Service Provider (MSSP)
- \+ сформирована команда экспертов из области защиты информации, мониторинга, исследования и атрибуции угроз

USSC SOC

УЦСБ

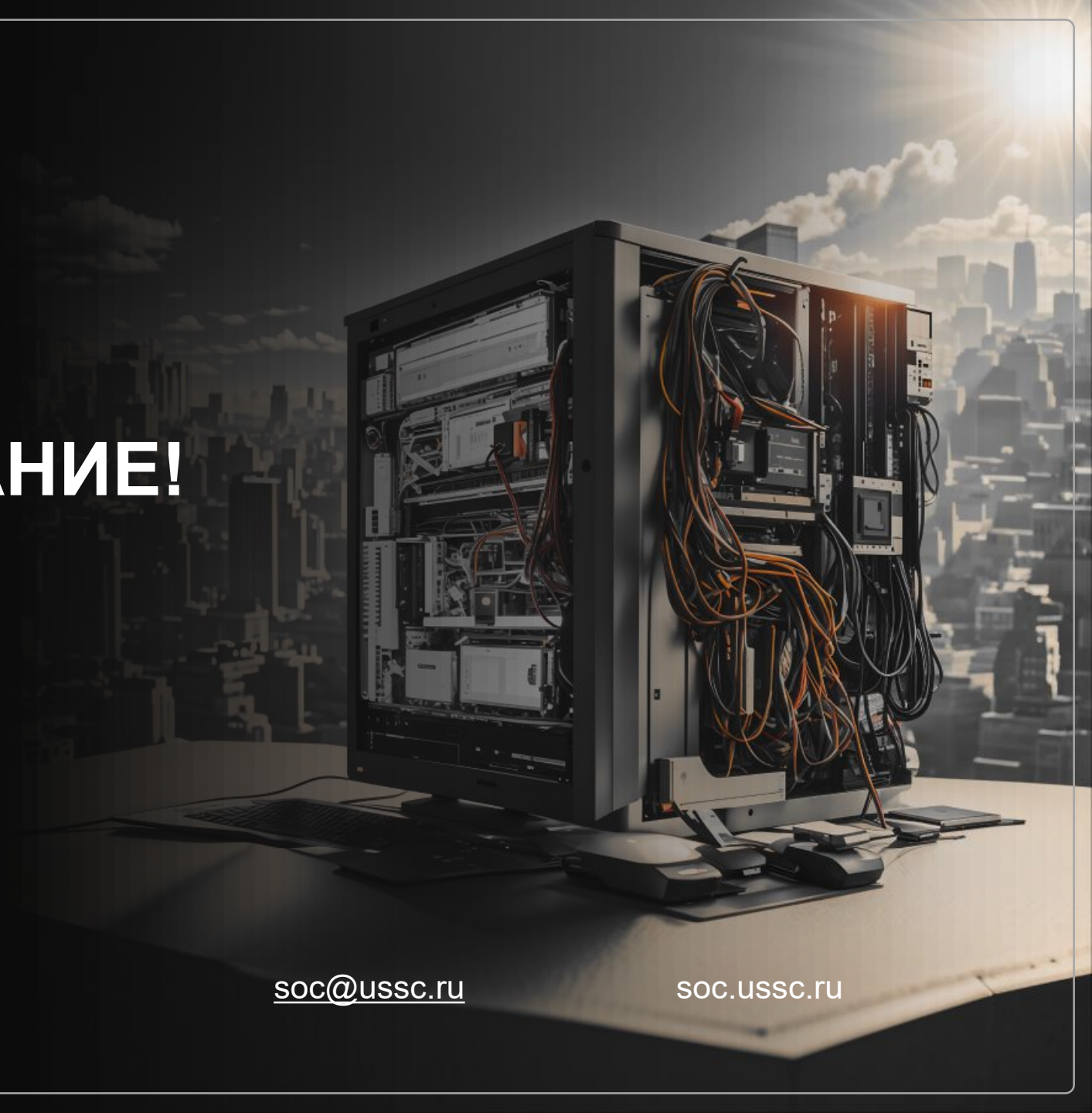
ПРОГРАММА ВЕБИНАРОВ

19.03	Как защитить КИИ от киберугроз? (Категорирование КИИ)
09.04	Как построить эффективную систему обеспечения ИБ объектов КИИ
25.04	Практические кейсы построения СОИБ
28.05	Мониторинг ЗОКИИ (SOC)
04.06	PAM или пропал: как обеспечить эффективное управление привилегированным доступом для защиты КИИ
	Безопасная разработка ПО для значимых объектов КИИ
	Оценка защищенности для ЗОКИИ (с учетом Указа Президента РФ № 250)
	Подготовка к прохождению госконтроля

Подписывайтесь на наш канал в Телеграме

- Ежемесячные обзоры изменения законодательства
- Разбор часто задаваемых вопросов по теме КИИ
- Экспертные статьи и кейсы

УЦСБ USSC SOC



СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

Анна Трохалева

Руководитель направления
анализа инцидентов ИБ

2024

soc@ussc.ru

soc.ussc.ru