Не допустить недопустимое

роль ИБ-сообщества в обеспечении киберустойчивости организации

Александр Кравченко,
эксперт сообщества Резбез

Коротко о себе:

12 лет в инфобезе

Архитектурная безопасность
Оценка рисков
Развитие проекта Резбез

Александр Кравченко
Эксперт сообщества Резбез

О чем пойдет речь?

- Вспомним, что такое сообщество
- Разберём понятие киберустойчивость
- Обратимся к опыту Резбеза

Сообщество - это

Умные мысли от умных людей

«Единство в сообществе - сила, разделение - слабость» - Жан-Жак Руссо

«Нет ничего более могущественного, чем сообщество, объединенное общей целью» – Джон Локк

«Сила сообщества заключается в том, что оно может поддерживать каждого его члена» - Ральф Уолдо Эмерсон

«Сообщество - это не место, а отношения между людьми» - Платон

«Создавайте сообщество, в котором каждый чувствует себя как дома» – Фридрих Ницше

Сообщество - это группа, объединение людей, народов, государств, имеющих общие интересы, цели

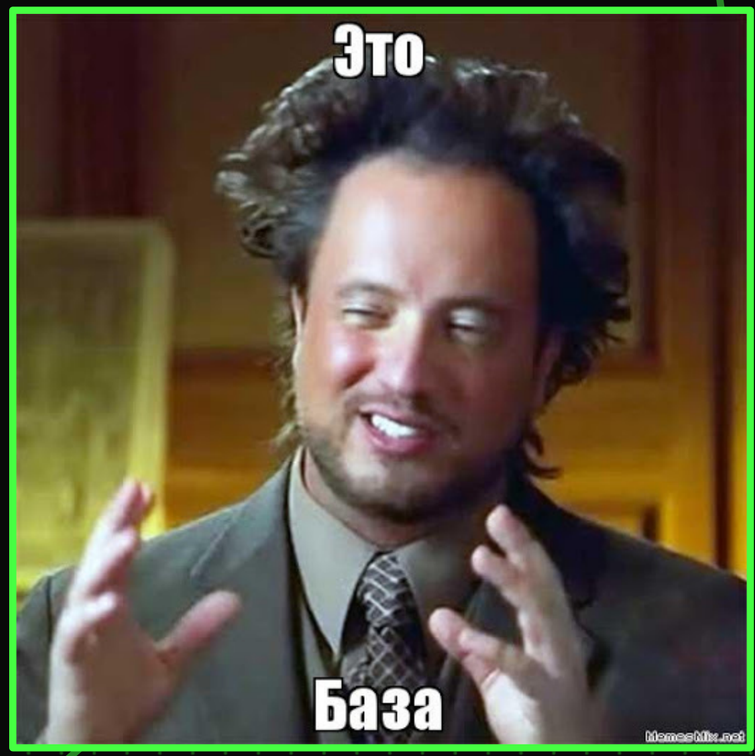
Толковый словарь Ожегова

В социологии

Компоненты сообщества

- Цель (миссия) сообщества
- Привлечение новых участников
- Правила коммуникации
- Платформа для коммуникации
- Контент
- Мотивация участников
- Интересы и потребности участников
- Управление и лидерство

...и еще пара моментов



...еще пара моментов

- Достоверность
- Время
- Результат

Разбираем киберустойчивость

Кибербезопасность

- защита подключенных к интернету систем (оборудования, программного обеспечения и данных) от киберугроз (Positive Technologies)
- совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных (Kaspersky)
- набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от цифровых атак (Microsoft)

Кибербезопасность

Атаки хакеров

Киберустойчивость

Киберустойчивость

способность организации (отрасли, государства) непрерывно функционировать в условиях проведения кибератак, нацеленных на реализацию недопустимых событий*

* для каждой организации могут быть сформулированы события, наступление которых катастрофически повлияет на ее операционную деятельность.

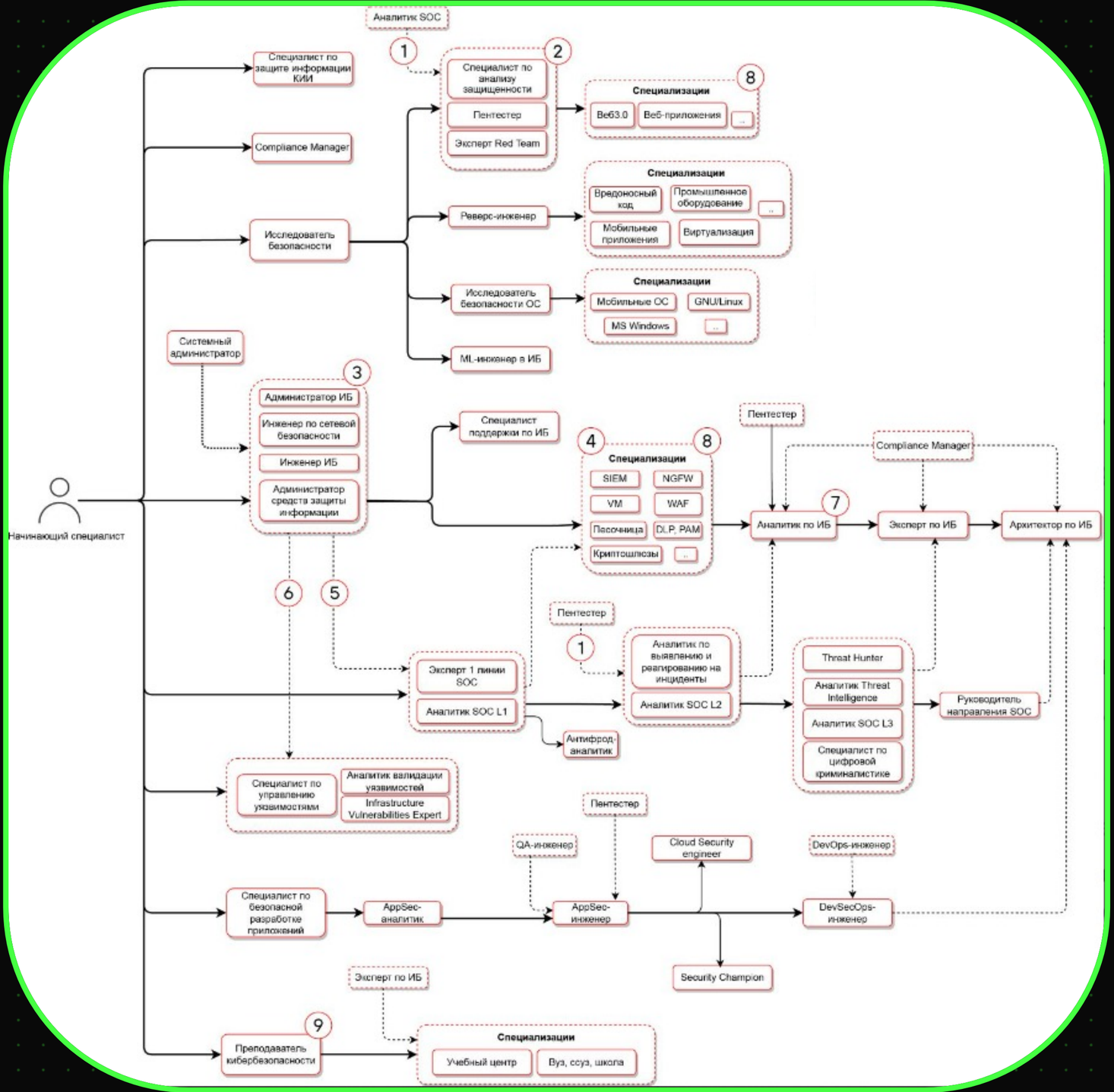
Недопустимые события

- Кража большого объема денежных средств со счетов организации
- Остановка производства
- Полная или частичная потеря данных из государственных систем

Результативная кибербезопасность

состояние защищенности организации, которое обеспечивает ее устойчивость к кибератакам и позволяет в любой момент на практике подтвердить, что злоумышленник не сможет реализовать недопустимые для этой организации события

Пример схемы карьерных треков в кибербезе*



* Positive Technologies

Если эксперт по кибербезопасности

- Проводит оценку рисков
- Разрабатывает стратегию безопасности
- Осуществляет мониторинг и реагирование на инциденты
- Обучает сотрудников
- Проводит тестирование на проникновение.
- Выстраивает безопасную инфраструктуру
- Следит за соблюдением законодательства и стандартов.
- Анализирует угрозы
- Взаимодействует с руководством компании

То ИБ – сообщество

- Облегчает обмен знаниями и опытом + обучение
- Формирует стандарты и рекомендации
- Налаживает межотраслевое взаимодействие
- Способствует расследованию и реагированию на инциденты
- Лоббирует интересы кибербезопасности
- Создает площадки для коммуникаций
- Развивает культуру кибербезопасности

Практический опыт

или опыт из практики

Резбез — некоммерческий проект, объединивший экспертов, которые стремятся поднять кибербезопасность в стране и в мире на новый уровень.

Резбез в цифрах

октябрь 2024

110 +

Статей и методик

30 +

Авторов статей

2500 +

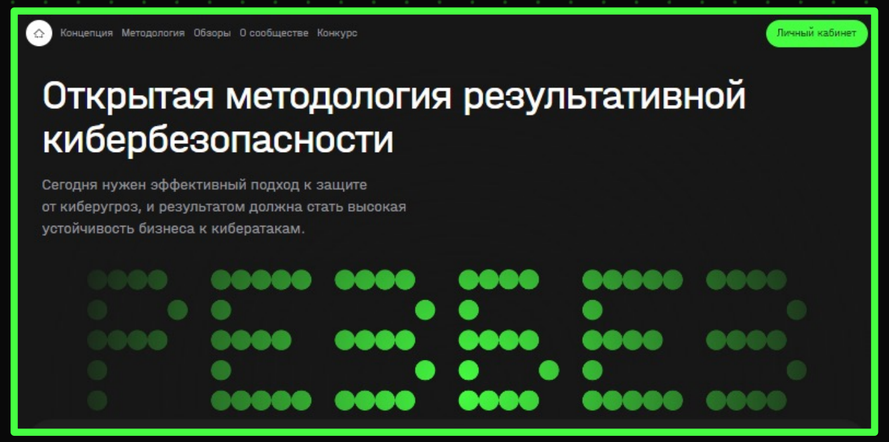
Подписчиков в ТГ-канале

4

Канала коммуникации

Проект Резбез

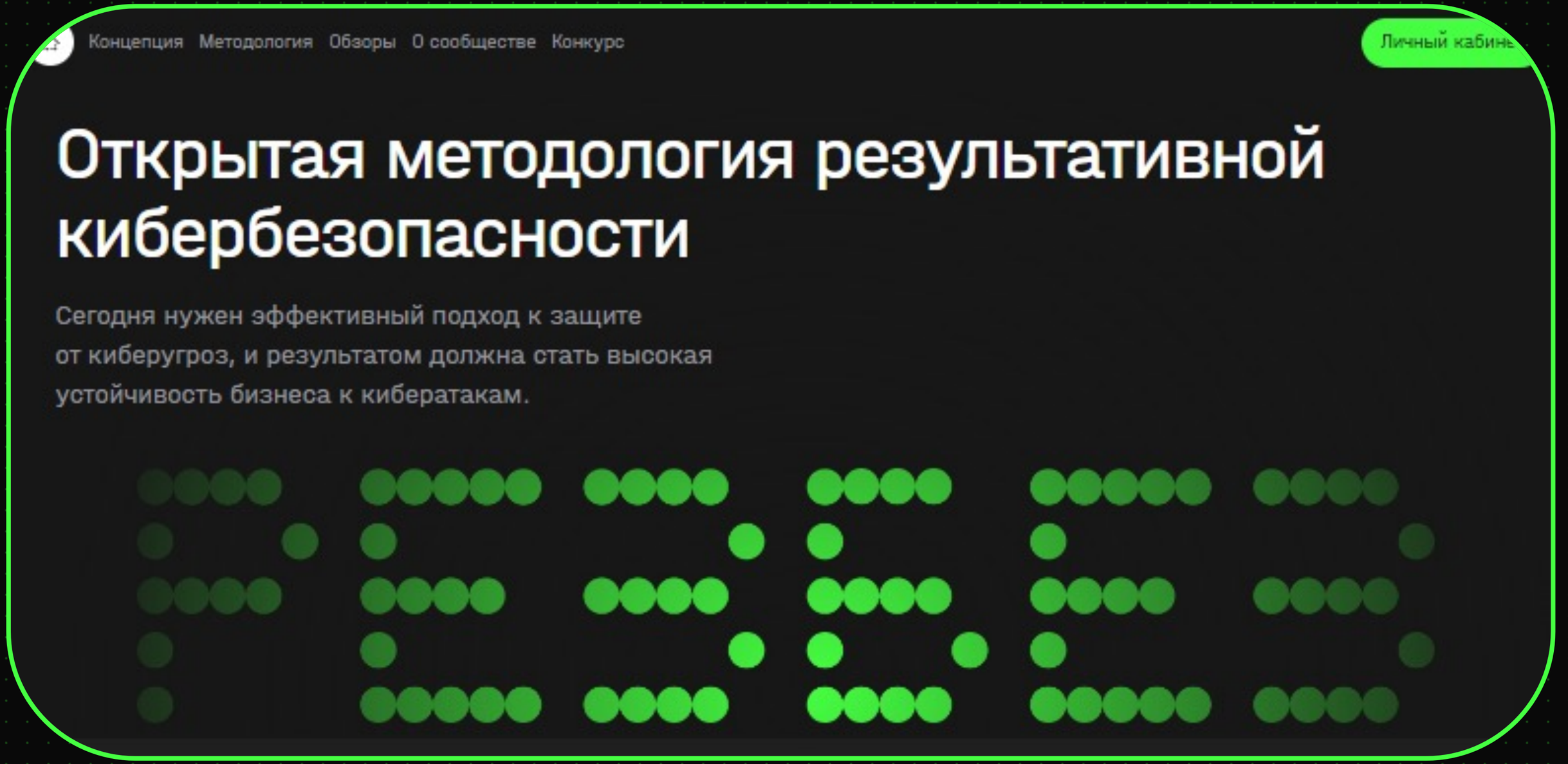
Площадка



Социальные медиа

Сообщество

Площадка Резбез



Концепция

Целевая аудитория

Ценность

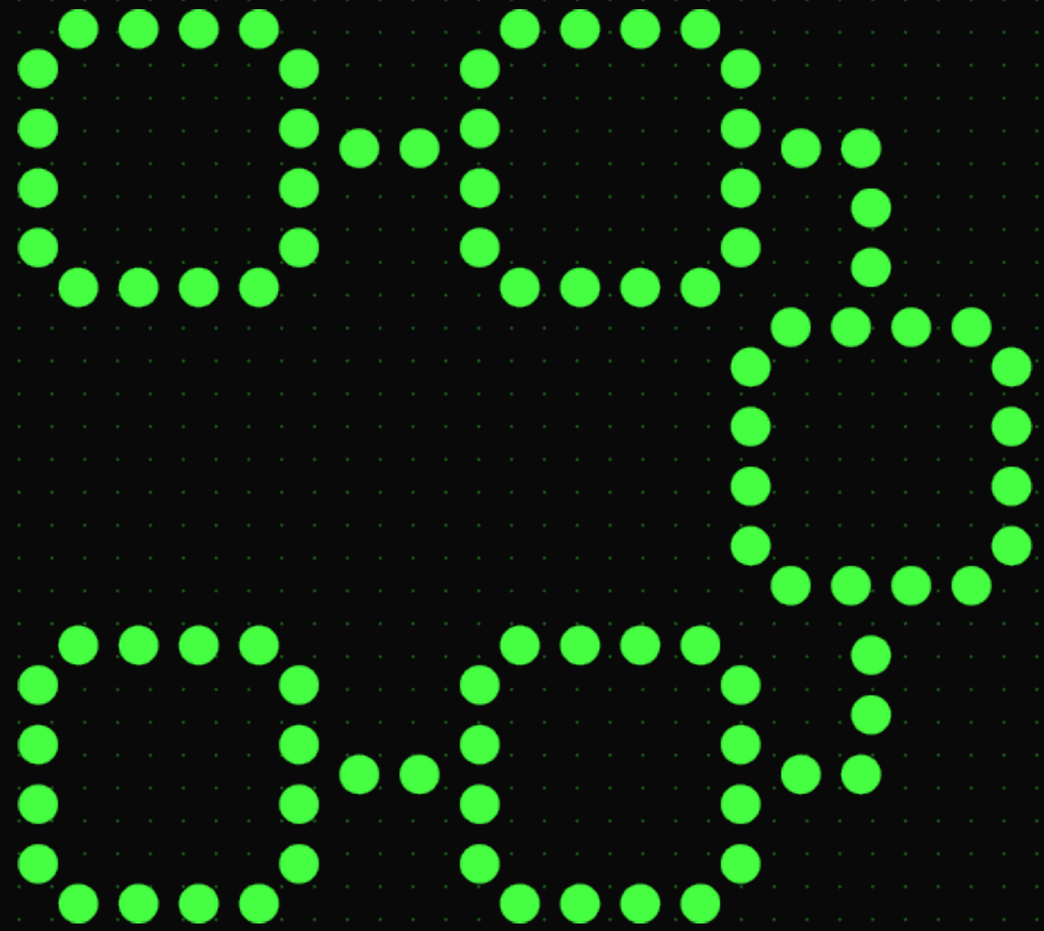
Принципы

Методология

Основа

Типы статей

Структура



Методология

Основа

Типы статей

Структура

Методология

Основа

Типы статей

Структура

Определение недопустимых событий

• ЯДРО МЕТОДОЛОГИИ

Определение точек проникновения в IT-инфраструктуру

• ЯДРО МЕТОДОЛОГИИ

Определение недопустимых событий. Первая встреча с топ-менеджером

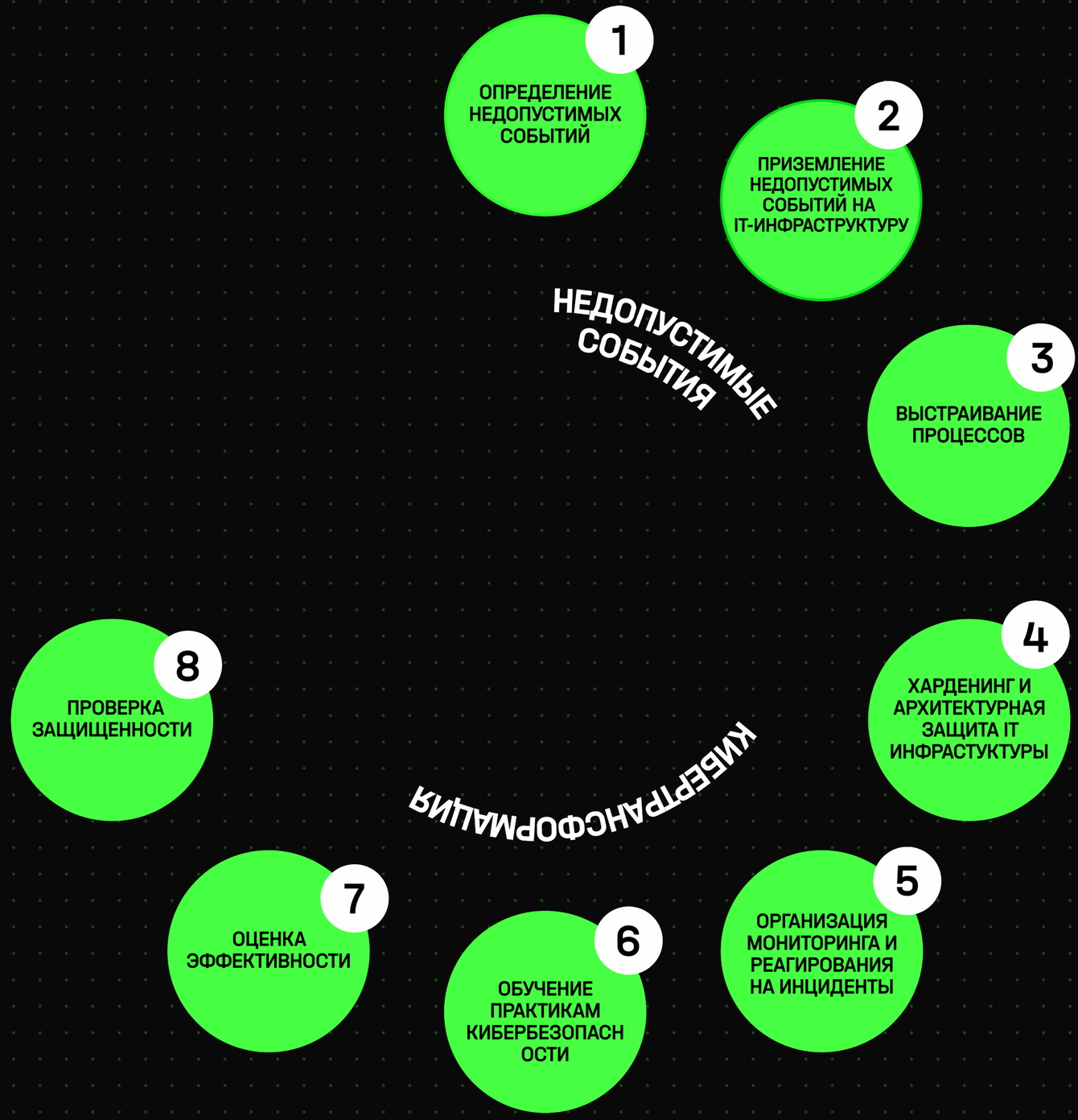
Безопасность контейнеров на примере платформы Docker

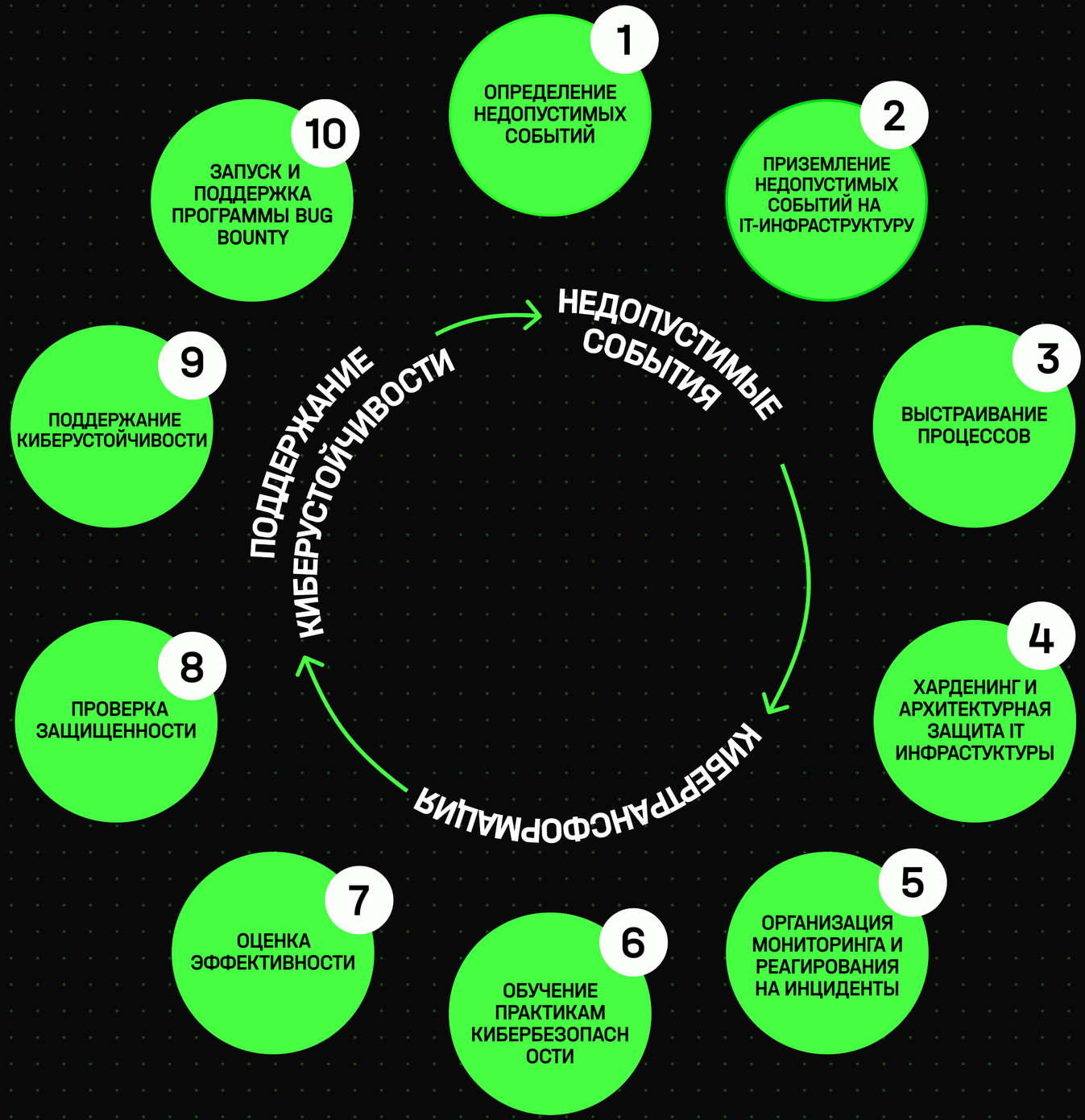
Методология

Основа

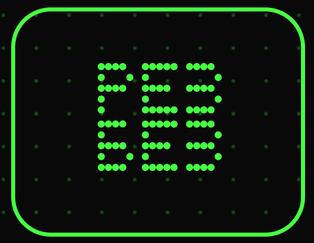
Типы статей

Структура


1
ОПРЕДЕЛЕНИЕ НЕДОПУСТИМЫХ СОБЫТИЙ
2
ПРИЗЕМЛЕНИЕ НЕДОПУСТИМЫХ СОБЫТИЙ НА IT-ИНФРАСТРУКТУРУ
НЕДОПУСТИМЫЕ СОБЫТИЯ
3
ВЫСТРАИВАНИЕ ПРОЦЕССОВ
4
ХАРДЕНИНГ И АРХИТЕКТУРНАЯ ЗАЩИТА IT ИНФРАСТУКТУРЫ
КИБЕРТРАНСФОРМАЦИЯ
5
ОРГАНИЗАЦИЯ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ
6
ОБУЧЕНИЕ ПРАКТИКАМ КИБЕРБЕЗОПАСНОСТИ
7
ОЦЕНКА ЭФФЕКТИВНОСТИ
8
ПРОВЕРКА ЗАЩИЩЕННОСТИ


1
ОПРЕДЕЛЕНИЕ НЕДОПУСТИМЫХ СОБЫТИЙ
2
ПРИЗЕМЛЕНИЕ НЕДОПУСТИМЫХ СОБЫТИЙ НА IT-ИНФРАСТРУКТУРУ
3
ВЫСТРАИВАНИЕ ПРОЦЕССОВ
4
ХАРДЕНИНГ И АРХИТЕКТУРНАЯ ЗАЩИТА IT ИНФРАСТУКТУРЫ
5
ОРГАНИЗАЦИЯ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ
6
ОБУЧЕНИЕ ПРАКТИКАМ КИБЕРБЕЗОПАСНОСТИ
7
ОЦЕНКА ЭФФЕКТИВНОСТИ
8
ПРОВЕРКА ЗАЩИЩЕННОСТИ
9
ПОДДЕРЖАНИЕ КИБЕРУСТОЙЧИВОСТИ
10
ЗАПУСК И ПОДДЕРЖКА ПРОГРАММЫ BUG BOUNTY
НЕДОПУСТИМЫЕ СОБЫТИЯ
КИБЕРТРАНСФОРМАЦИЯ
ПОДДЕРЖАНИЕ КИБЕРУСТОЙЧИВОСТИ

Роли сообщества



МЕТОДОЛОГИИ РКБ
КАК СТАНДАРТ

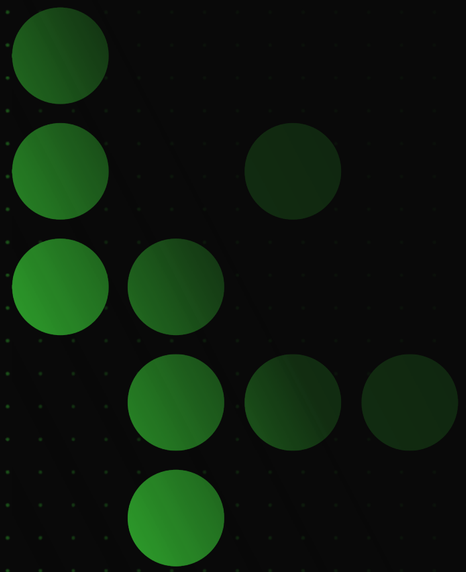
ОБМЕН ОПЫТОМ
+ ОБУЧЕНИЕ

ПЛОЩАДКИ
ДЛЯ КОММУНИКАЦИЙ

ФОРМИРОВАНИЕ
КУЛЬТУРЫ КИБЕРБЕЗА

МАТЕРИАЛ ЭКСПЕРТОВ

МЕЖОТРАСЛЕВОЕ ВЗАИМОДЕЙСТВИЕ



Благодарю
за внимание!