

Моделирование угроз и оценка поверхности атаки в контексте РБПО

_____ Екатерина Рудина

**Все модели
неправильны, но
некоторые
полезны**

Джордж Бокс

Моделирование угроз и оценка поверхности атаки в контексте РБПО

Общие сведения

Модели угроз для РБПО

Рекомендации

Грабли!

Общие сведения по моделям угроз

kaspersky

**совокупность условий и факторов,
создающих потенциальную или
реально существующую
опасность нарушения
безопасности информации**

Модель угроз безопасности информации

Физическое, математическое, описательное
представление свойств или характеристик
угроз безопасности информации

_____Примечание - Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ

Рассуждение	определение условий и вывод следствий
Объяснение	представление объяснений эмпирическим явлениям
Разработка	выбор характеристик, правил, проектная работа
Коммуникация	передача знаний и представлений
Действие	обеспечение стратегии и выбора альтернатив
Прогнозирование	оценка будущих и неизвестных явлений
Исследование	изучение возможностей и гипотез

Модели угроз

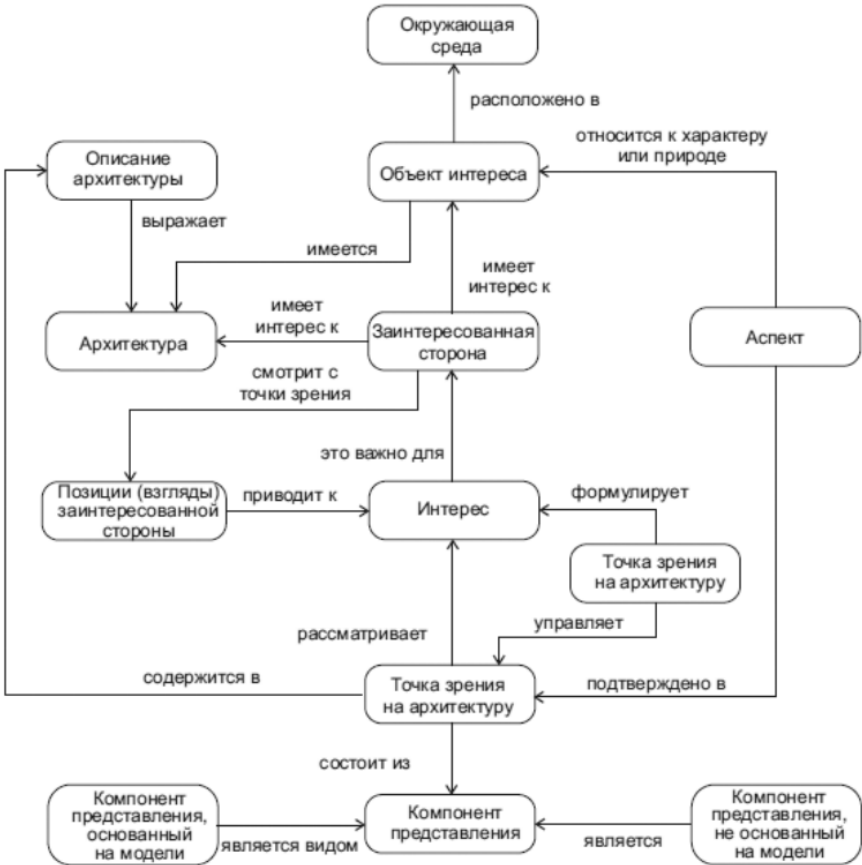
Зачем нужны и какие
бывают

_____ Снизить риски за счет
уменьшения уязвимостей или
применения средств защиты

_____ На разных стадиях ЖЦ
системы будут разными, могут
быть определены для системы,
отрасли, технологии и т.п.

_____ Разной степени
детализации: более общие или
детальные, словесное
описание, формальная модель

Модель угроз – это точка зрения (viewpoint)



Что нужно для модели угроз

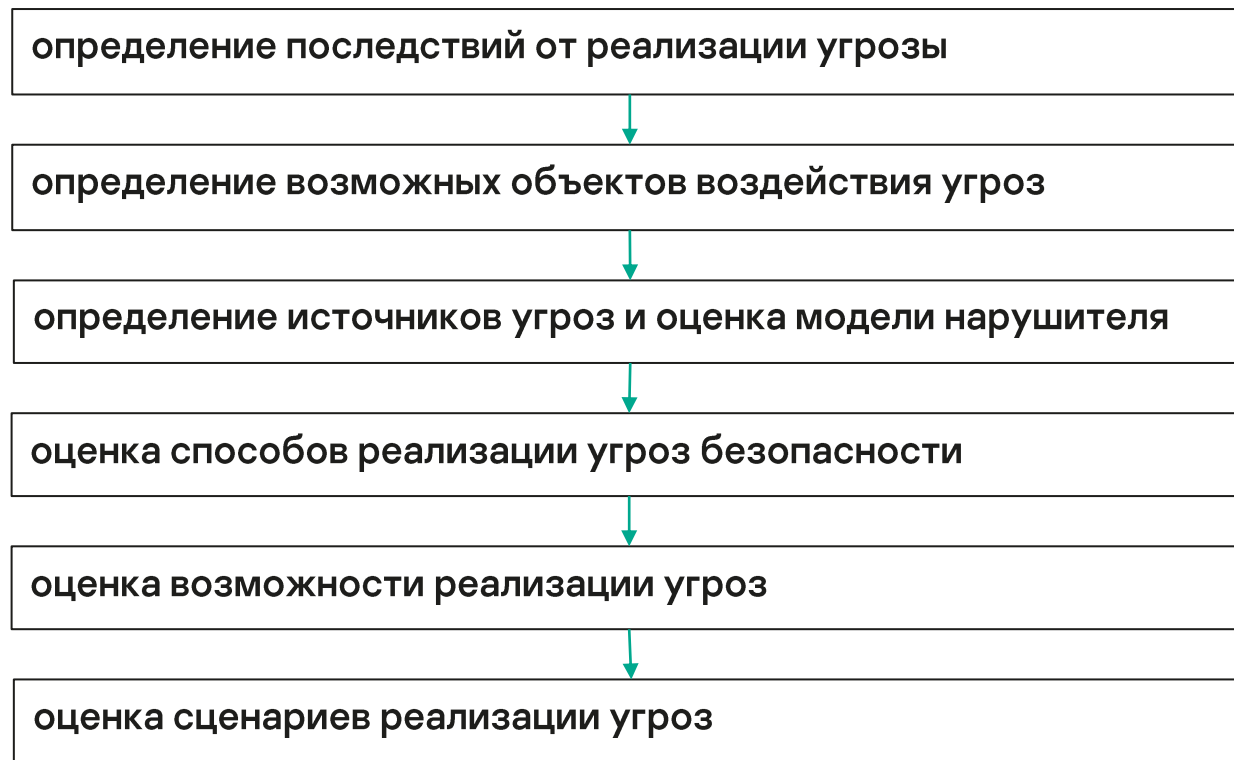
_____ Знания о системе

_____ Знания об угрозах

_____ Методика работы
(определения угроз)

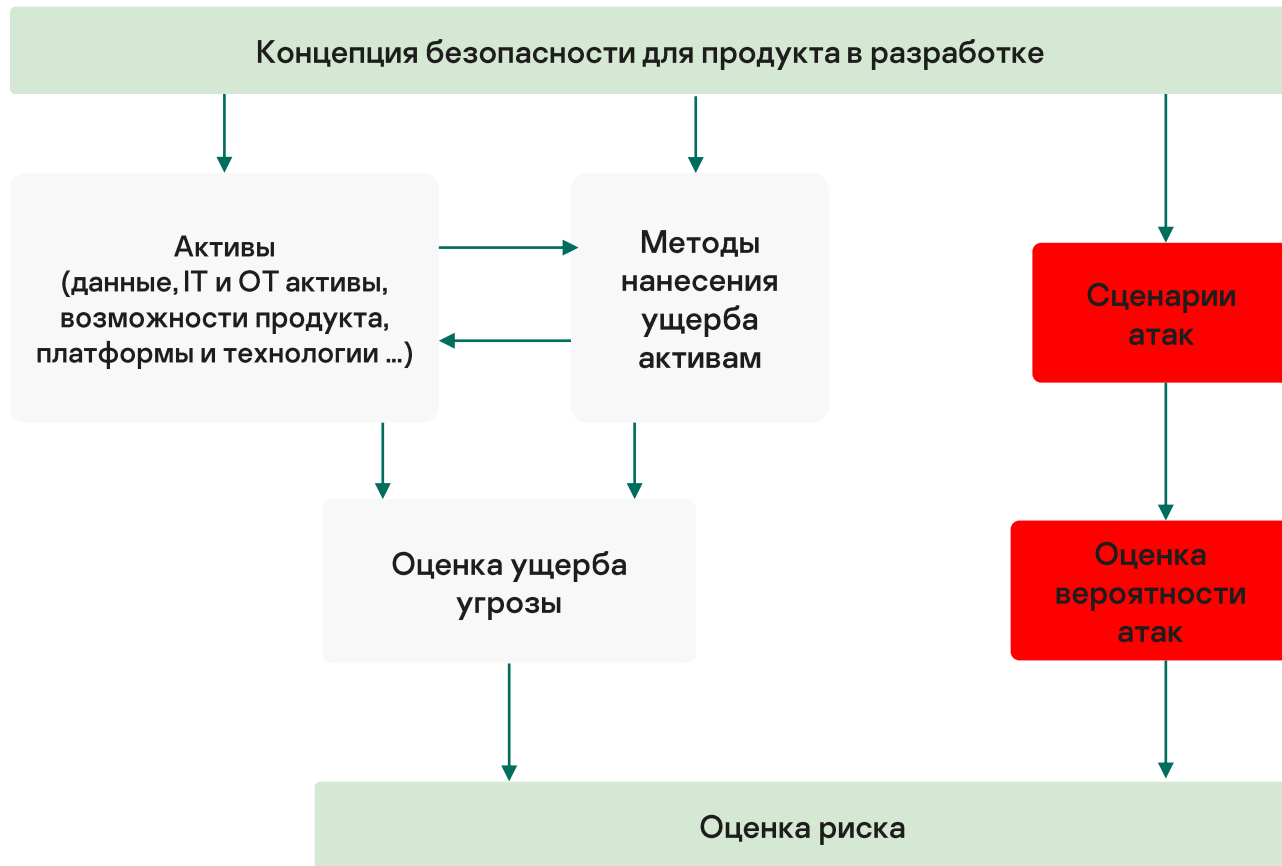
Пример методики определения угроз

11



Пример методики определения угроз

12



TARA (анализ угроз и оценка рисков согласно ISO/SAE 21434)

Идентификация активов

Идентификация сценариев угроз

Оценка величины воздействия

Анализ пути атаки

Оценка возможности реализации атаки

Определение величины риска

Решение по обработке риска

Что нужно знать о системе

Что требуется от системы

- Цели безопасности или типовые цели безопасности
- Виды ущерба и способы оценки

Как устроена система

- Технологии/типовые технологии
- Архитектура/типовая архитектура
- Специальные методы разработки
- Специфика эксплуатации
- ...

Что нужно знать об угрозах

Типовая информация

- Ландшафт угроз, типовые атаки
- Модель нарушителя, мотивация, ресурсы и методы

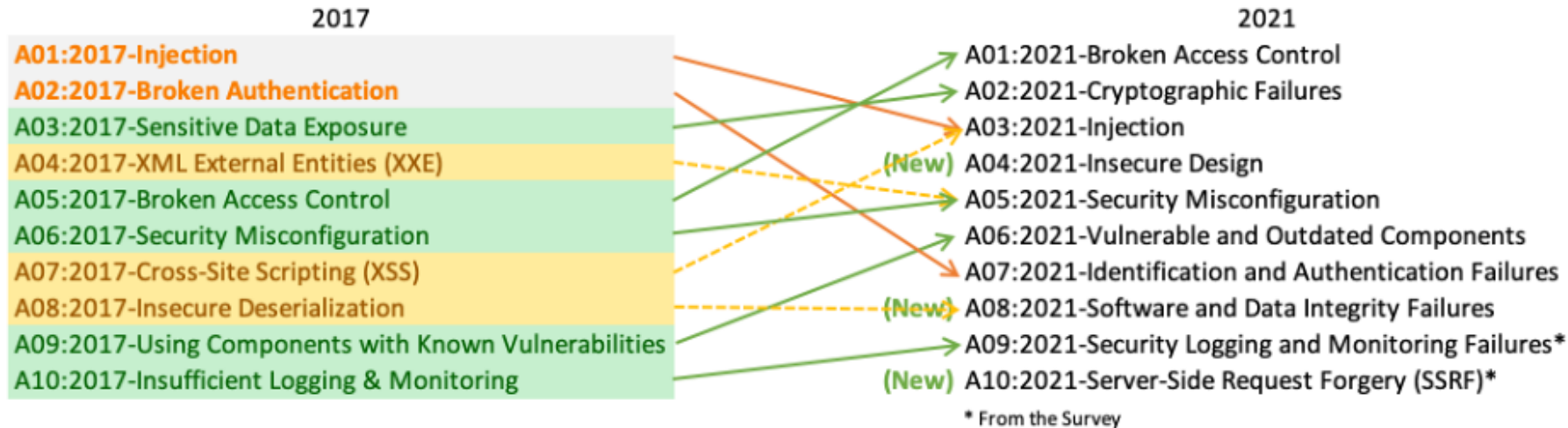
Специфичная для системы информация

- Специфичные вектора, тактики и техники атак
- Цепочка поставок, зависимости
- Уязвимости
- Мотивация внутреннего нарушителя, подверженность сотрудников атаке, культура безопасности...

STRIDE

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

OWASP Top10 (разные годы)



Методы, основанные на тактиках и техниках атак

- Методика определения угроз ФСТЭК России
- Методики и способы, основанные на тактиках и техниках MITRE Att&ck
- Другие

Инструменты описания и моделирования

- Текстовые и табличные описания
- Схемы взаимодействия, зон безопасности, поверхности атаки
- Диаграммы потоков данных
- Алгоритмические схемы
- Иерархические схемы (деревья атак)
- Специальные языковые средства
- ...

Модели угроз для РБПО

kaspersky

Модель угроз

- Модель угроз должна включать совокупность угроз безопасности, актуальных для разрабатываемого ПО
- Каждая угроза безопасности представляется в виде совокупности свойств (характеристик), включающей, как минимум, краткое описание угрозы, предполагаемый объект воздействия и возможные последствия реализации угрозы

Поверхность атаки

- Описание поверхности атаки ... должно включать перечень функциональных подсистем, модулей (компонентов) ПО и их интерфейсов, составляющих поверхность атаки, актуальных для разработанного кода ПО
- Перечень целей ... для проведения дальнейших исследований безопасности ПО должен содержать описание функциональных подсистем, модулей (компонентов) ПО, их интерфейсов, для которых предполагаются дальнейшие исследования в части безопасности при реализации других процессов разработки безопасного ПО

Угроза обусловлена

1) недостатками в реализованных разработчиком ПО мерах контроля доступа и контроля целостности, применяемых к объектам среды разработки ПО, и

2) мерах по разработке безопасного ПО, в частности:

отсутствием мер, связанных с определением требований по безопасности, неполной или некачественной оценкой требований по безопасности, недостатками в мерах, связанных с управлением конфигурацией ПО и обучением работников разработчика ПО в области разработки безопасного ПО

**Прежде – безопасность
инфраструктуры разработки**

Затем – процессы РБПО

ИМХО Это стандарт для проектных менеджеров, не разработчиков

- Сверяться с предложенной классификацией угроз безопасности в процессах разработки
- Проверять, все ли меры предприняты
- Проверять приложение А в применении к процессам

Рекомендации

**Если есть отраслевая или
рекомендованная (например, головной
организацией) методика – используйте**

**Не забывайте давать обратную связь и
улучшать методику**

При моделировании угроз для разработки ориентируйтесь на **ущерб для потребителя в отрасли**

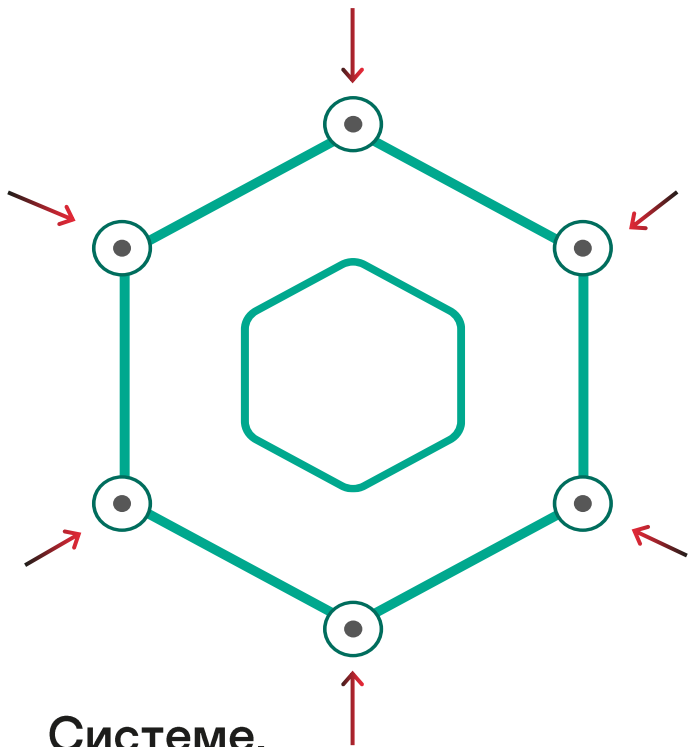
Это «мерило важности»

Второй по важности показатель – ущерб разработчику или эксплуатанту

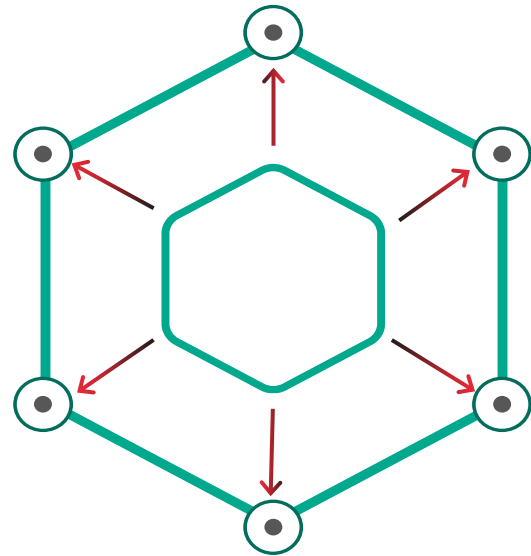
(и забудьте про CIA)

Ущерб может быть нанесен

29



Системе,
которую атакуют



Окружению
системы под атакой

Виды ущерба – что случилось

Утрата или порча активов

Утечка данных

Подделка данных

Простой

Снижение эффективности

Другой (специфичный)

Виды ущерба – на что влияет

30

Финансовый (материальный)

Жизни и здоровью людей

Безопасности частной жизни

Общественной безопасности

Экологический

Репутационный

Другой (специфичный)

Как измерять ущерб

И как сравнивать
различные виды ущерба

Количественно: деньгами

**Использовать известные
рейтинги ущерба или риска**

**Придумать шкалу: например
низкий, средний, высокий**

Выберите определенный способ описания и оценки действий нарушителя, при необходимости адаптируйте под себя и напишите алгоритмы оценки угроз для разработчиков

Это может быть STRIDE, какая-то из классификаций OWASP, выборка угроз из БДУ ФСТЭК

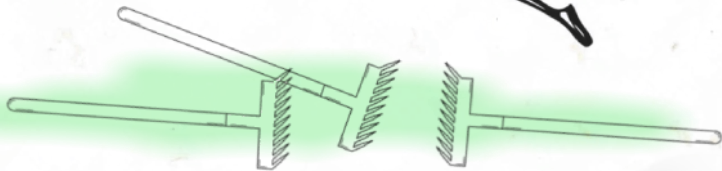
Выберите способ документирования МУ и обмена информацией, который используете в системе управления качеством

Продумайте артефакты для сертификации, если требуется, но не подменяйте одно другим

**Проводите обучение
Собирайте обратную связь
Если модель угроз «пропускает»
угрозы и уязвимости – ее нужно
менять**

**Как говорит Алексей Лукацкий:
«А вы учли это в своей модели угроз?»**

Грaбли!



«Да кому мы нужны»

- ориентироваться на уязвимости, а не на ущерб от их эксплуатации (Утечки! XSS! RCE!)
- ориентироваться на ущерб без учета мотива нарушителя (инвертированное «да кому мы нужны»)
- слишком углубляться в психологию нарушителя, мотивацию – это не дает сделать технический анализ (плохая модель угроз)
- брать в расчет слишком много дополнительных факторов (погодные условия, сбои оборудования, отключение интернета)

Не разобратся, что для вас угроза

- Не отделять способ нанесения ущерба от сценария атаки
- Не сводить «неизвестное к известному», не определить вход и выход процесса

Хорошая, но слишком подробная, модель угроз становится злом

- Мультипликативный анализ:
количество активов, количество видов ущерба, количество способов нанесения ущерба и сценариев атак будут в итоге перемножены. Если это не учесть, количество рисков становится необозримым, его нельзя использовать как источник технических требований.
- Вовремя нужно заменять подход к моделированию угроз, учитывать количество факторов для анализа.

Вместо заключения



Сделайте одну-две модели угроз, походите по граблям и научитесь, как именно делать не нужно.



Останавливаться и делать выводы о том, что «модель угроз бесполезна» на основе небольшого опыта не стоит. Это процесс, который должен быть полезен именно вам.



Подтягивайте стандарты и методики.