КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Практическое моделирование угроз

Роман ЖУКОВ
Product Security Manager,
Intel

ABOUT ME

Роман Жуков

Эксперт по кибербезопасности

Connect me:

- 12+ ЛЕТ В СФЕРЕ ИБ
- ЗАНИМАЮСЬ ПРОДУКТОВОЙ БЕЗОПАСНОСТЬЮ
- ВЫВОДИЛ НА РЫНОК ПРОДУКТЫ И СЕРВИСЫ
- РУКОВОДИЛ КОМПЛЕКСНЫМИ ИБ-ПРОЕКТАМИ
- ex. ЧЛЕН РОССИЙСКИХ ЭКСПЕРТНЫХ ГРУПП (ФСТЭК, Банк России, МинЦифра, РКН, АРПП)
- ВЕДУ БЛОГ: **ROZHUKOV.BLOGSPOT.COM** И КУРСЫ ПО ИБ В ВУЗАХ И УЧЕБНЫХ ЦЕНТРАХ

О ЧЕМ СЕГОДНЯ ПОГОВОРИМ

- Зачем ИБ в компании
- Как оценивать риски и причем здесь модель угроз
- Подходы к моделированию угроз
- Подготовка к моделированию
- Практика: моделирование угроз
- Чек-лист и полезные ссылки

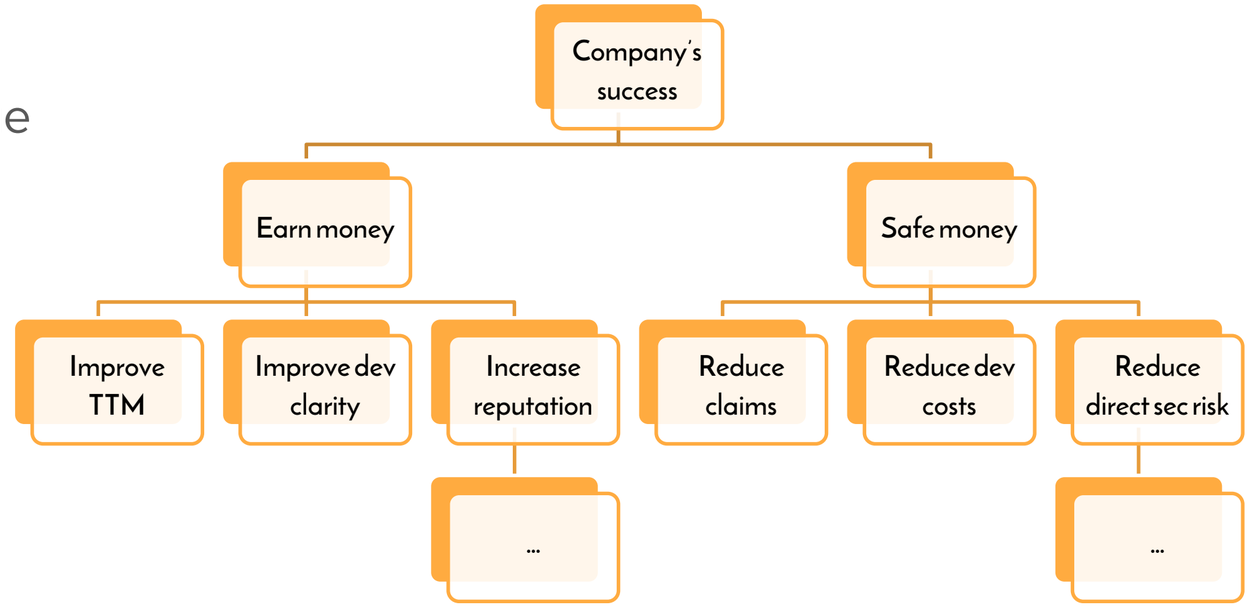
СЕГОДНЯ НЕ БУДЕТ

- Пересказа какого-либо стандарта
- Методики ФСТЭК
- «Здесь нужно купить FW, а тут установить EDR»
- Идеальной или тем более универсальной модели угроз. Наша цель – понять «Как»
- Оценки рисков: подсчета вероятности и опасности

ЗАЧЕМ ИБ В КОМПАНИИ

ПОМОЧЬ УДОВЛЕТВОРИТЬ РАЗНЫЕ ИНТЕРЕСЫ

- Акционеров
  - №1: Сберечь и заработать
- Менеджмента (чтобы достичь №1)
  - **Снизить риски**
  - Увеличить долю рынка или выйти на новые
  - Внедрить лучшие практики в индустрии
  - Цифровая трансформация
  - Улучшение/сохранение репутации
- Регуляторов
  - ☺
- Клиентов, партнеров
  - Удовлетворенность, качество
  - Доверие, уверенность
- Сотрудников
  - Удобство



КАК ОЦЕНИВАТЬ РИСКИ И ПРИЧЕМ ЗДЕСЬ МОДЕЛЬ УГРОЗ

Практика

ЭТАПЫ РАБОТЫ С РИСКАМИ

Расположите в правильном порядке.

Маппинг рисков и угроз

Описание систем и выбор объекта оценки

Оценка рисков: Вероятность + Опасность + Стоимость

Выбор итоговых мер защиты

Рекомендации по реагированию на риски: Избежать, Принять, Переложить, Митигировать

Пересмотр рисков

Моделирование угроз и первичных защитных мер

Описание защищаемых активов для объекта оценки

ЭТАПЫ РАБОТЫ С РИСКАМИ

УРОВНИ РИСКОВ ИБ

NIST SP 800-30. Guide for Conducting Risk Assessments.

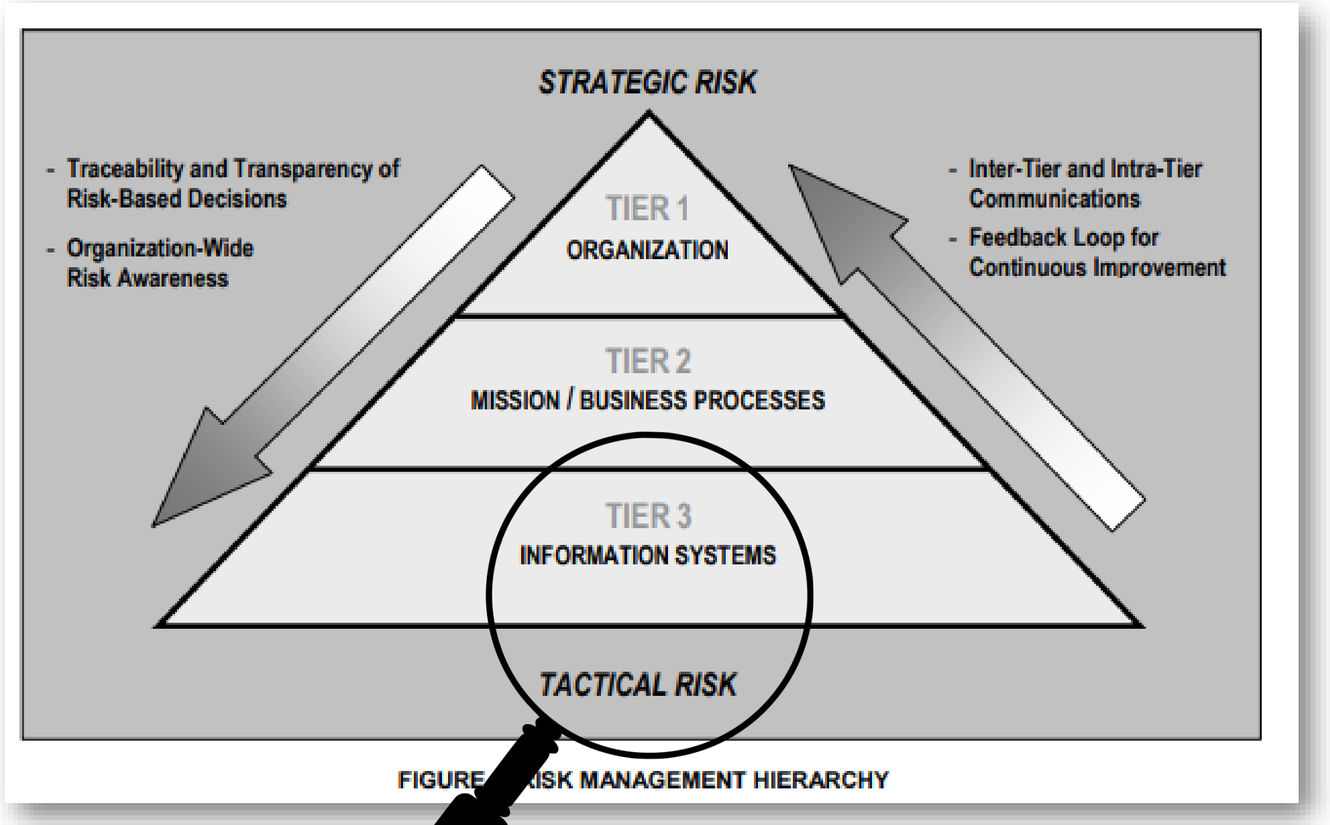
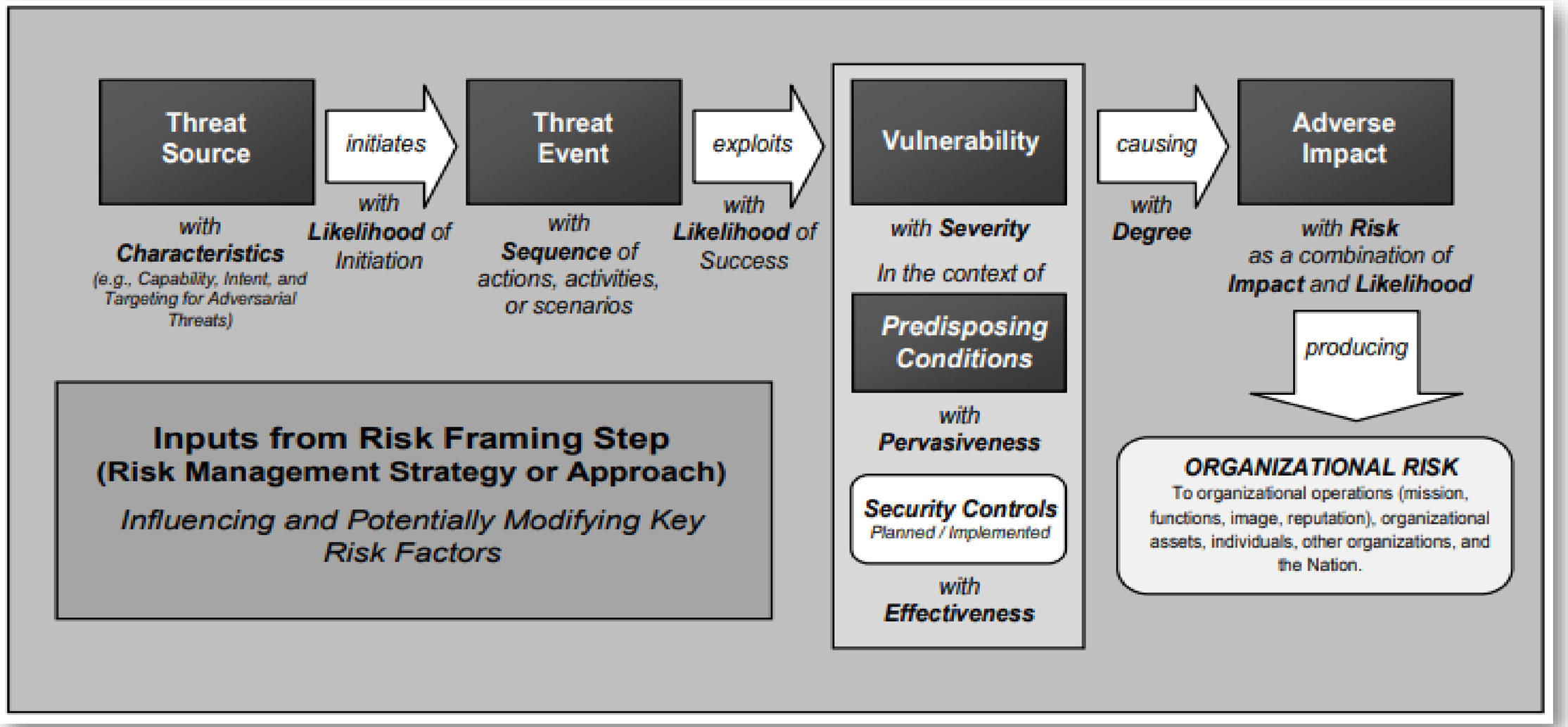


FIGURE ISK MANAGEMENT HIERARCHY

Для каждой категории рисков ИБ могут быть разные подходы к их оценке и моделированию угроз, свой уровень технической детализации и даже различные ответсвенные подразделения.

ГДЕ ИСКАТЬ ТЕХНИЧЕСКИЕ РИСКИ ИБ?

NIST SP 800-30. Guide for Conducting Risk Assessments.



ЗАЧЕМ НУЖНА МОДЕЛЬ УГРОЗ

Злоумышленники делают (уже) это за нас.

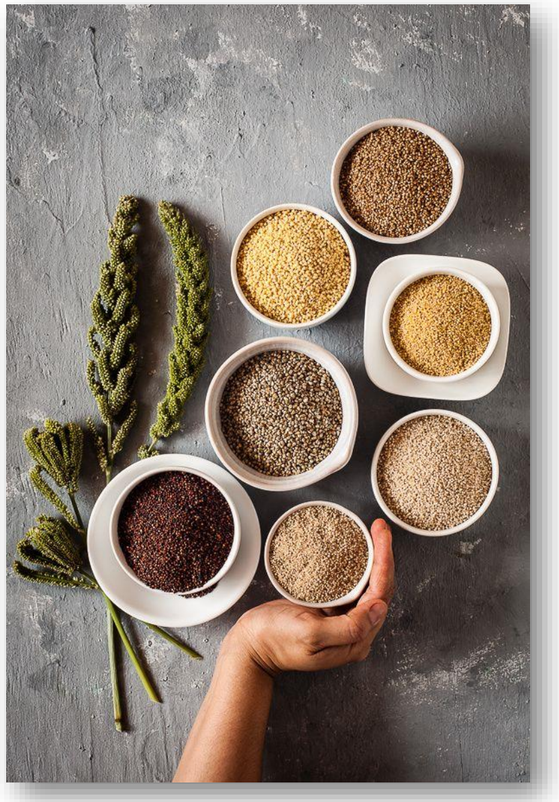
1. Источник для оценки рисков.
2. Для ИБ - понять, как устроена и работает система на самом деле.
3. Определить максимальное число угроз, некоторые из которых не найти с помощью сканов или пентестов.
4. Выстраивать и приоритезировать систему защиты и контр-меры.
5. Воспитывать Security mindset среди инженеров.

Техническое моделирование (выявление) угроз ИБ и оценка риска (вероятность*опасность) – **разные процессы**.

ПОДХОДЫ К МОДЕЛИРОВАНИЮ УГРОЗ

КАКИЕ ВСТРЕЧАЮТСЯ МОДЕЛИ УГРОЗ

1. Высокоуровневые (моделирование рисков для предприятия).
2. Отраслевые (финансовый сектор, телеком, ритейл, ТЭК).
3. Подзаконные (под ПДн, под ГИС, под КИИ).
4. Для определенной технологии (web, container, net).
5. Для определенного процесса или его части (разработка ПО, производство ПАК, выпуск продукции).



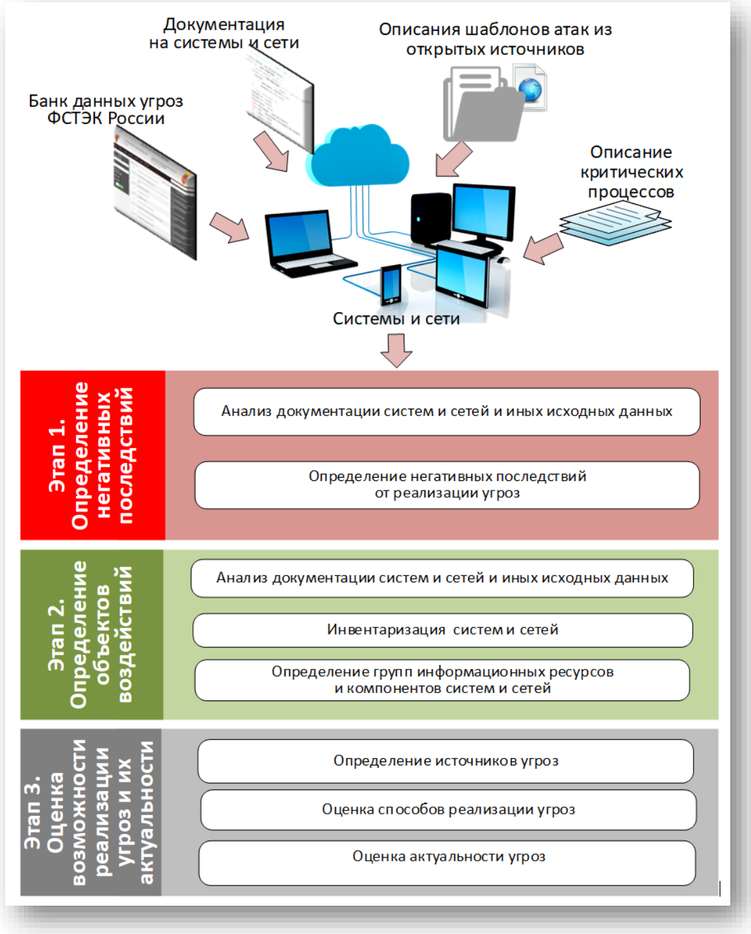
МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ (РФ)

- Модель угроз КСИИ, 2007 год, ФСТЭК (ДСП).
- «Базовая модель угроз для ИСПДн», 2008 года, ФСТЭК.

Правила отнесения угрозы безопасности ПДн к актуальной

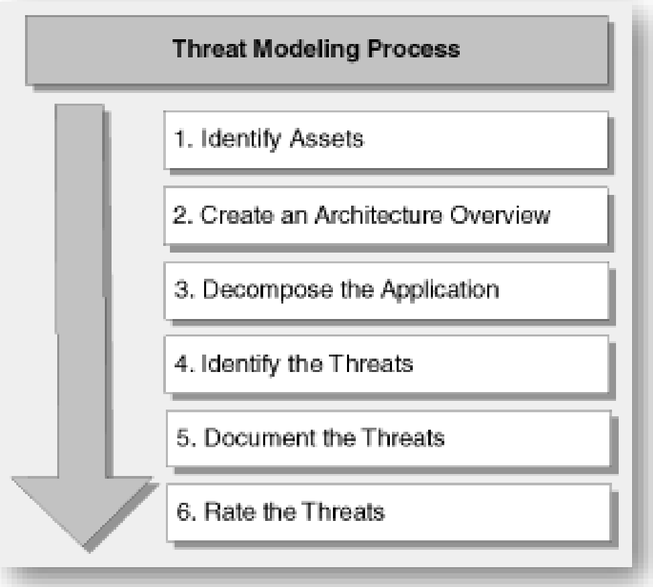
Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

- «Менеджмент риска ИБ», ГОСТ (ISO) 27005, 2009 год.
- СТО БР – оценка рисков ИБ для фин. сферы, 2009 год, Банк России.
- «Методические рекомендации для ИСПДн при использовании СКЗИ», 2015 год, ФСБ.
- «Методика оценки угроз безопасности», 2021 год, ФСТЭК.



МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ (МИР)

STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) + **DREAD** (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability), 1999, **Microsoft** (SDLC).



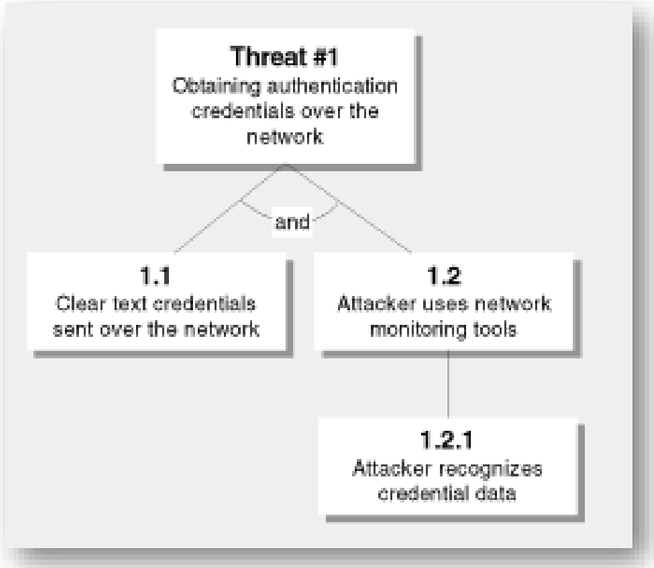


Table 3.7 DREAD rating

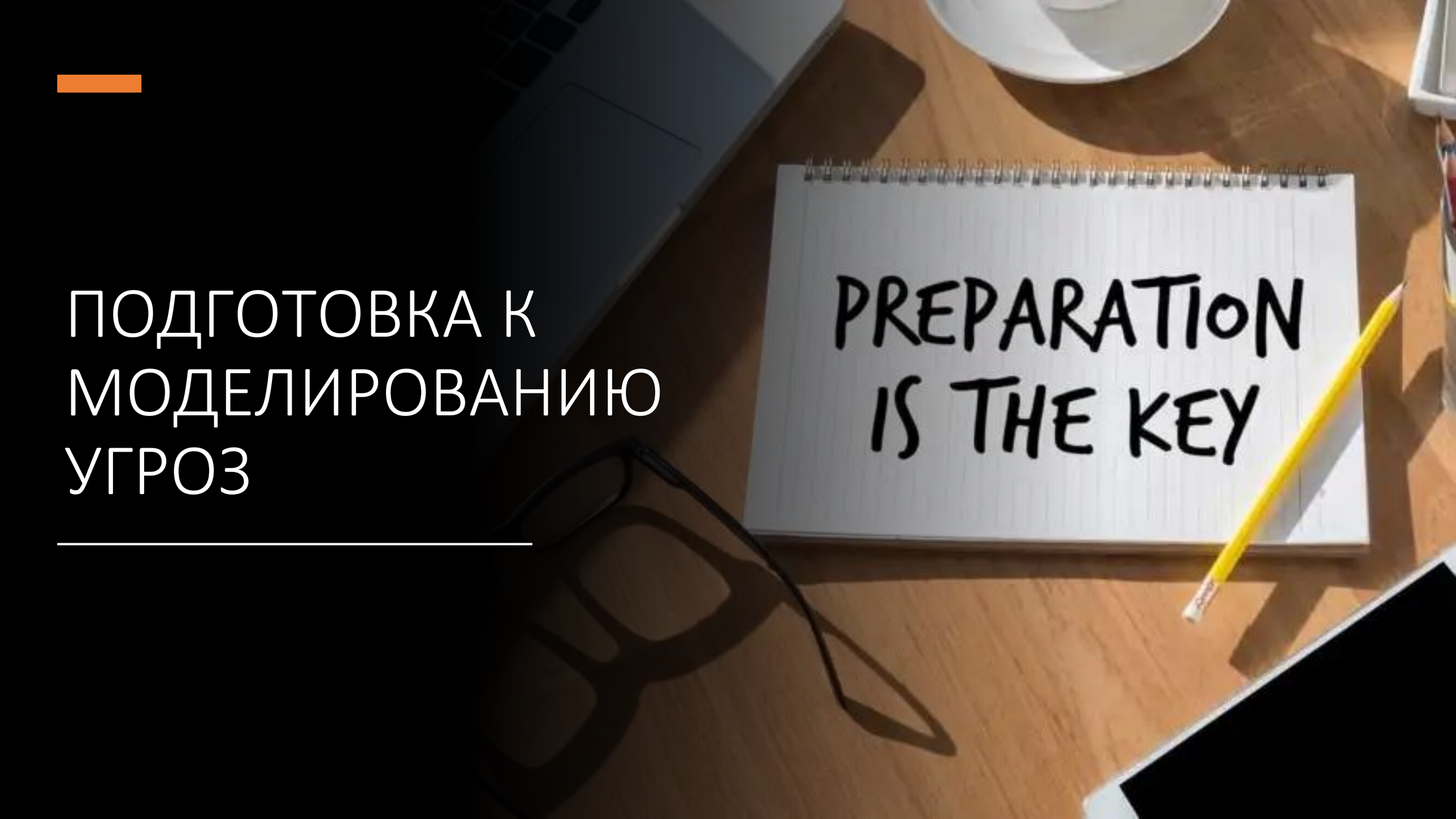
Threat	D	R	E	A	D	Total	Rating
Attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
SQL commands injected into application.	3	3	3	3	2	14	High

МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ (МИР)

- **NIST SP 800-30** (Guide for Conducting Risk Assessments), 2011, NIST.
- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation), 1999, Carnegie-Mellon University.
- **OWASP** (Open Web Application Security Project), 2001, OWASP.
- **TRIKE** (Основана на риск-требованиях к каждому активу и их проверке), 2006, Open Source.
- **P.A.S.T.A.** (Process for Attack Simulation & Threat Analysis), 2012, Versprite.
- **MITRE ATT&CK** (14 Tactics, ~200 Technics), 2013, MITRE.

Рекомендую симбиотический подход к моделированию угроз, чтобы не превращать процесс в бесконечный. И еще для одной цели.

ПОДГОТОВКА К МОДЕЛИРОВАНИЮ УГРОЗ



Практика

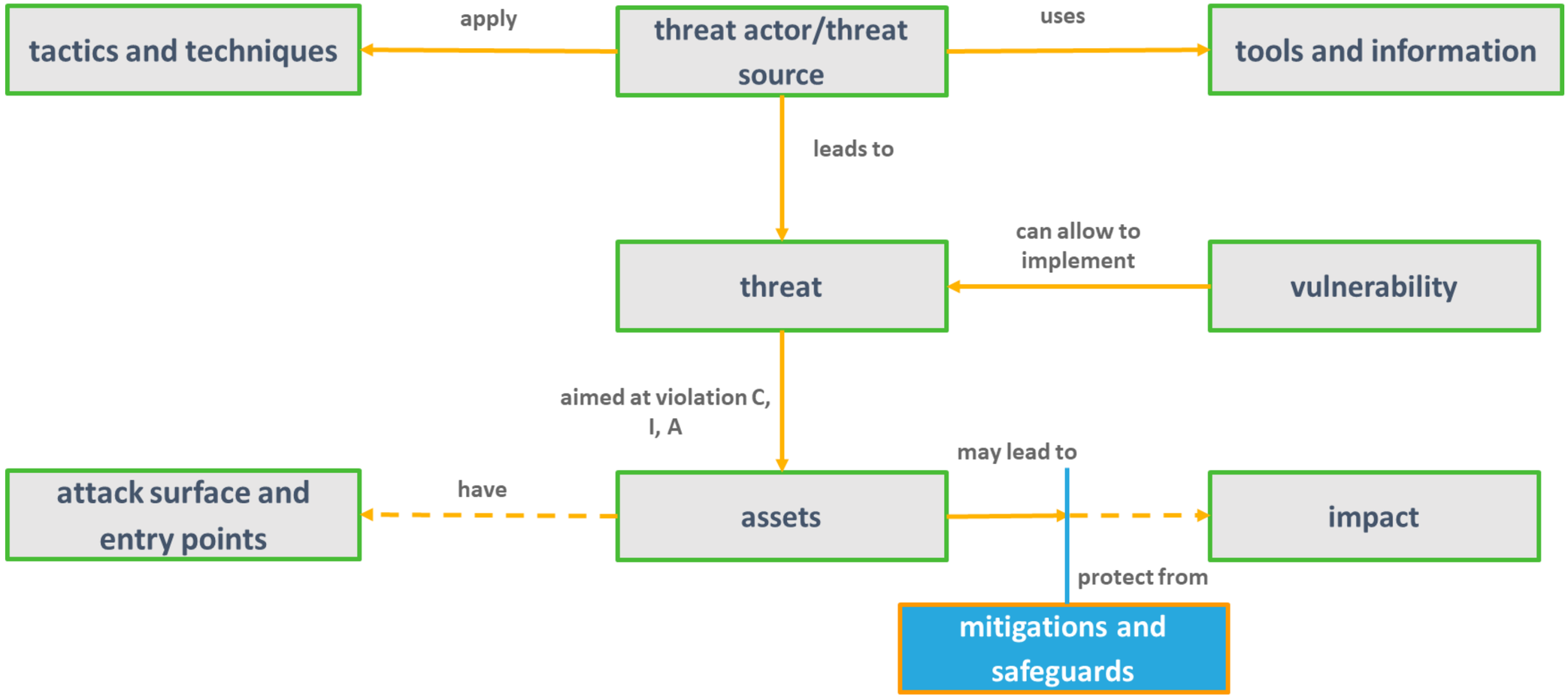
Опишите 1 предложением каждый термин:

- Asset (актив)
- Trusted (доверенный)
- Trust boundary (контролируемая зона)
- Attack surface (поверхность атаки)
- Threat Modelling (модель угроз)
- Threat (угроза)
- Vulnerability (уязвимость)
- Mitigation (защитная мера)
- Model (модель)
- Threat Modelling (модель угроз)

ДОГОВОРИМСЯ О ТЕРМИНАХ

- Asset (актив) – все, что требует защиты.
- Trusted (доверенный) – все, что ведет себя, как задумано.
- Trust boundary (контролируемая зона) – логическая или физическая граница “вокруг” объекта, в которой обработка и передача данных выполняются на одном и том же уровне К, Ц или Д.
- Attack surface (поверхность атаки) – явное или неявное “открытие” границы доверия, позволяющее менее доверенному объекту взаимодействовать с системой.
- Threat (угроза) – потенциальное нарушение К, Ц или Д актива (asset), вызванное действиями злоумышленника (adversary), с помощью некоторой поверхности атаки (attack surface).
- Vulnerability (уязвимость) – дефект, баг, просчет в системе.
- Mitigation (защитная мера) – технический или организационный шаг для нейстрализации угрозы, снижения вероятности реализации или потенциального ущерба от нее.
- Model (модель) – наглядное или упрощенное представление системы в некотором уровне абстракции.
- Threat Modelling (модель угроз) – процесс это концептуального представления системы, ее функционирования и выявления угроз для нее.

ВЗАИМОСВЯЗЬ ТЕРМИНОВ



НЕОЧЕВИДНЫЕ ВОПРОСЫ

Q: Кто должен составлять модель угроз?
A: Архитектор (и его команда) системы/инфраструктуры/сети/ПО. Безопасность – советует. Не обязательно быть экспертом ИБ, чтобы моделировать угрозы.

Q: Когда создавать модель угроз?
A: На этапе проектирования. Если система уже запущена – прямо сейчас, ибо никогда не поздно. Регулярный пересмотр должен быть интегрирован в корпоративные правила.

Q: На чьей полке должна лежать модель угроз?
A: Вместе с документацией на систему, как неотъемлемая часть. И быть доступной как инженерам (ИТ, разработчики), так и безопасникам. Пересмотр архитектуры или состава решений должнын быть триггером для пересмотра.

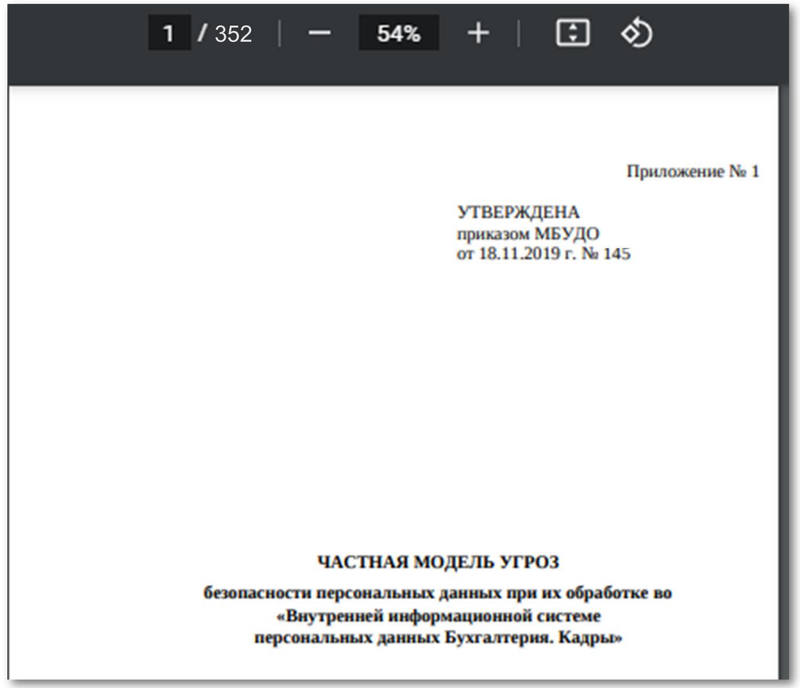
Q: Система никуда не годится, можно ее полностью переделать?
A: Главная цель – снижение рисков, при этом система должна выполнять свои задачи.

Q: Нужно ли учитывать защитные меры перед началом моделирования?
A: Нет, но всегда желательно держать их в голове.

АРХИТЕКТУРНЫЕ ПРИНЦИПЫ И SECURITY BY DEFAULT

Defense in-depth: protect on each layer	Least Privileges: only allow the minimum	Economy of mechanism: keep it simple	Open Design: avoid security through obscurity
Complete mediation: check every access	Permission based: deny by default	Separation of duties: multiple checks	Compartmentalization: isolate and avoid sharing
Psychological acceptability: protection should be easy to use	Secure by default: turn on all, do not rely on user	Fail secure: make sure no access if app failed	Economy of mechanism: minimize protection code

КАК ДОЛЖНА ВЫГЛЯДЕТЬ МОДЕЛЬ УГРОЗ


1 / 352 — 54%

Приложение № 1

УТВЕРЖДЕНА
приказом МБУДО
от 18.11.2019 г. № 145

ЧАСТНАЯ МОДЕЛЬ УГРОЗ

безопасности персональных данных при их обработке во «Внутренней информационной системе персональных данных Бухгалтерия. Кадры»

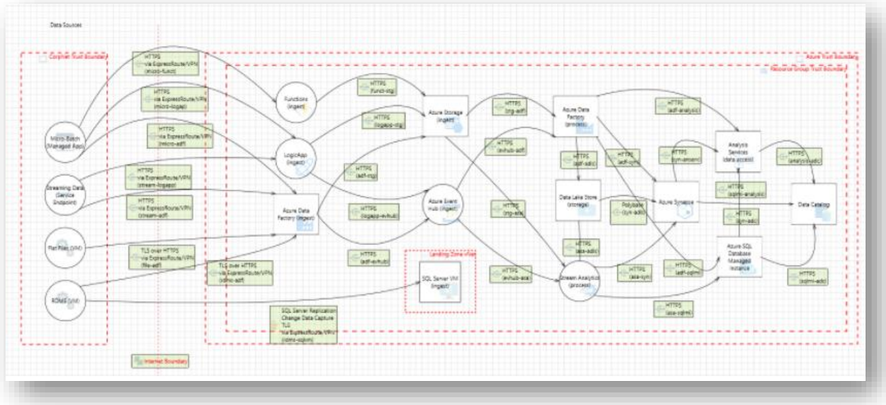
Угроза (ФСТЭК, 2021) – это вектор в виде:

УБИ$_i$ = [

бизнес-процесс;
риски (негативные последствия);
объекты воздействия;
источники угрозы (актуальные нарушители);
способы реализации угрозы;
сценарии реализации угрозы.
//доп. параметры

]

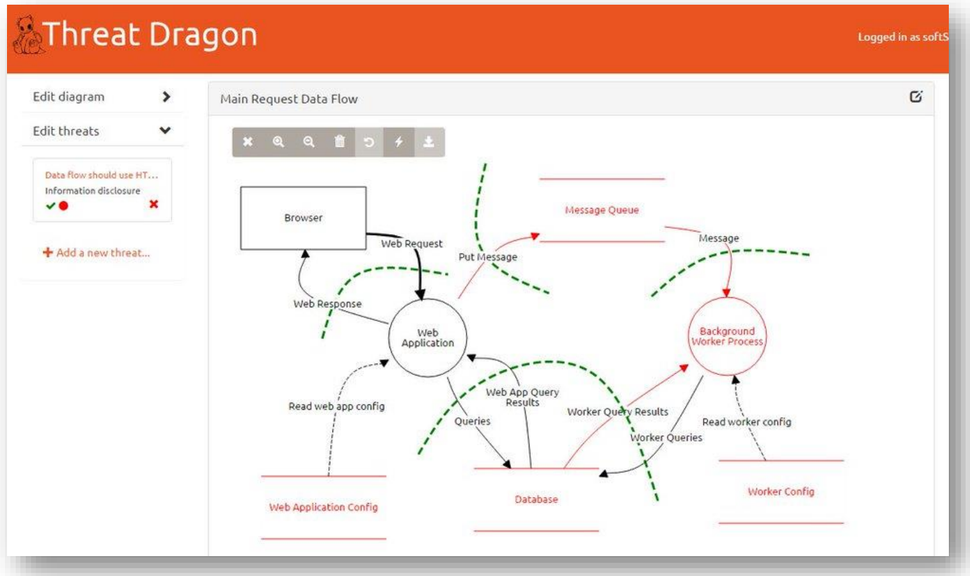
	Threat	Damage	Countermeasure	Evaluation	Passed
Spoofing Identity	attacker acts as server and sends own software to the device.			sending an update package with a wrong signature.	YES
Tampering with Data	attacker intentionally manipulates the update package.				YES
	update package is damaged by accident.	device is useless since wrong software is executed.	signing the update package's payload.		YES
	incorrect transmission of the update package.			sending a manipulated update package.	YES
	incomplete transmission of the update package(due to server failure, border-router failure, node failure).				YES
	manual manipulation of the firmware due to physical access to the device.	undefined behavior of the device.	not part of this work.	programm the device via serial interface with a wrong firmware.	not part of this work.
Repudiation	the sender denies the sending of the update package.	not part of this work.	authentication of the server at the client.	send update package with wrong authentication.	not part of this work.
Information Disclosure	the version number of the firmware is manipulated,or read from the update header.	old versions of the firmware can be installed on the device (fallback).	signing the update package's header.	sending an outdated firmware.	YES
	the key IDs are manipulated or read from the update header.	conclusions about the keys can be drawn from key IDs; wrong keys could be used by the device, rendering signature and encryption useless	signing and encrypting the update package's header.	sending an update package with manipulated key IDs	YES
	the payload size is manipulated or read from the update header.	attackers can damage the update package.	signing the update package's header.	sending an update package with manipulated payload size value.	YES
	the payload is manipulated or read from the update header.	attacker retrieves data and information of customers, etc.	signing and encryption of the update package's payload.	sending an update package with a manipulated payload.	YES
	keys are being retrieved from key storage.	attacker retrieves keys for signature and encryption.	not part of this work.	not part of this work.	not part of this work.
Denial of Service	malware is sent instead of the update package.	device useless	signing the update package.	sending an update package with an invalid signature.	YES
	attacker intentionally manipulates the update package.			sending manipulated update package	YES
	update package is manipulated or damaged by accident.	device useless.	signature.	sending manipulated update package.	YES
	incorrect or incomplete data transmission.			interrupt or stop data transmission by server/client.	YES
	update package manipulated with the intention of DoS attacks.	device unreachable.	signing the update header.	sending faulty firmware.	YES
	manually deleting the firmware due to physical access to the device.	device useless.	not part of this work.	deleting the flash memory via debug interface.	not part of this work.

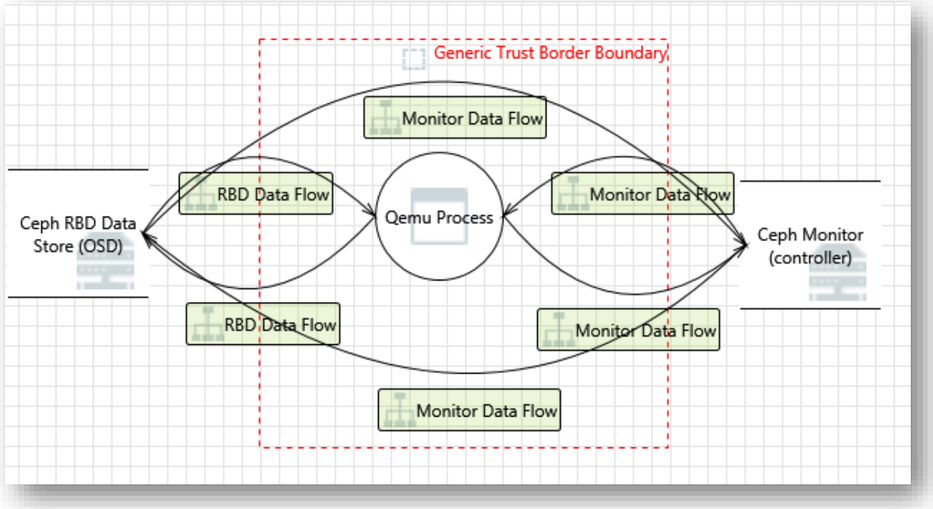


Цель Моделирования угроз – не составить некий конечный список угроз и положить на полку, а быть источником для принятия решения о составе рисков и оптимальных вариантах реагирования на них.
Совет – избегайте «бесконечных» таблиц.

ИНСТРУМЕНТЫ МОДЕЛИРОВАНИЯ УГРОЗ

- Лист бумаги, доска.
- Электронные таблицы и документы.
- Microsoft Threat Modeling Tool
- OWASP Threat Dragon Tool.
- OWASP CheatSheet.
- ThreatPlaybook.
- ThreatSpec.
- SeaSponge.
- Draw.io, Ariz, Bizagi.





ЭТАПЫ МОДЕЛИРОВАНИЯ УГРОЗ

Adam Shostack 4 questions.

1. Model System	**What are we working on?**	Нарисуйте, как устроена и работает система (каждый компонент).
2. Find Threats	**What could go wrong?**	Думайте, как злоумышленник, учитывая тактики и техники, применительно к активам.
3. Address Threats	**What are we going to do about it?**	Опишите меры защиты, первым делом – by design.
4. Validate	**Have we done a good job?**	Мы уверены, что сделали все правильно?

Adam Shostack, Microsoft.
Создатель Threat Modelling tool, один из создателей CVE.

ЭТАПЫ МОДЕЛИРОВАНИЯ УГРОЗ

0. Subject

- Subject: Определитесь с уровнем и детализацией и выберете объект/систему.
- Context: Изучите суть системы и обязательно бизнес-кейсы.

1. Model System

- Diagram: Подготовьте описание и схему/схемы, отражающие архитектуру и взаимодействие.
- Trust boundaries: Отразите контролируемые зоны (доверенные границы).
- Assets: Опишите защищаемые активы.

2. Find Threats

- Adversaries: Составьте список типов нарушителей.
- Attack surface/Entry points: Определите поверхность атаки.
- Threats. Составьте список всех угроз с указанием нарушения свойств безопасность (КЦД).

3. Address Threats

- Mitigations: Для каждой угрозы опишите меры защиты. Не забывайте про by design.

4. Validate

- Validation: Для каждой меры защиты укажите как проверяется реализация.
- Optional: Добавьте дополнитеьные параметры: protection statement, severity, impact
- Review: Что-то забыли (как правило – да)

SUBJECT


0. Subject
1. Model System
2. Find Threats
3. Address Threats
4. Validate

ПРИМЕРЫ ОБЪЕКТОВ МОДЕЛИРОВАНИЯ

1 ИСПДн «Бухгалтерия и Кадры» или ИС «Отдела продаж».

2 Система удаленного доступа для сотрудников.

3 Облачный сервис.

4 Приложение (ПО).

5 **Приложение в Банке.**

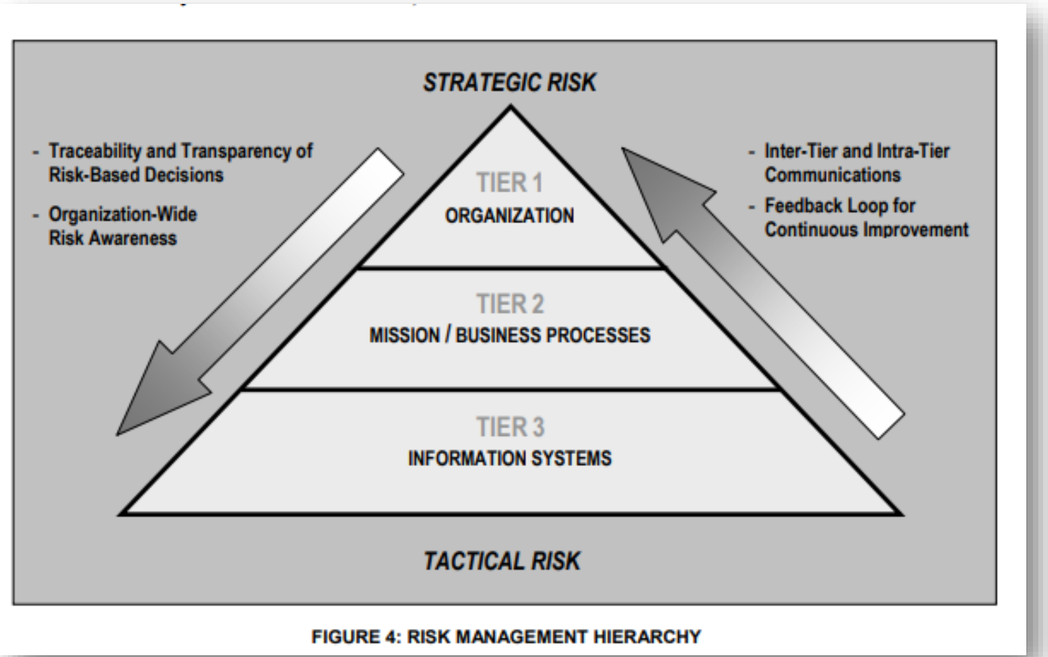


FIGURE 4: RISK MANAGEMENT HIERARCHY

«Используйте картинки. Это стоит тысячи слов.»
Tess Flanders, 1911

MODEL SYSTEM

0. Subject

1. Model System

2. Find Threats

3. Address Threats

4. Validate

ЧТО РИСОВАТЬ?

Концепция «4+1»

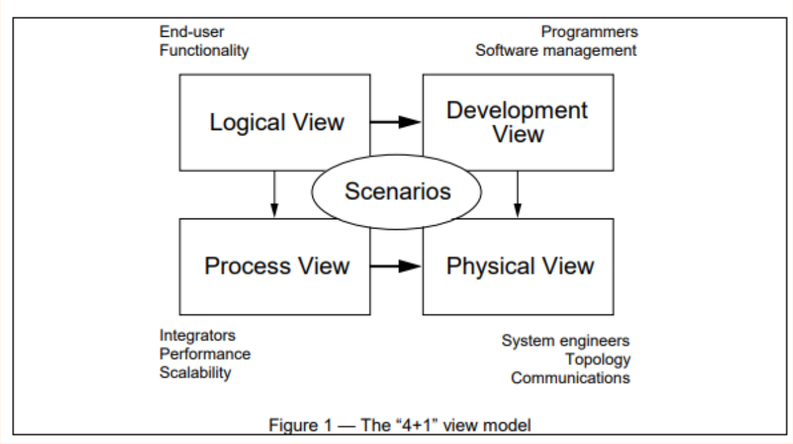


Figure 1 — The "4+1" view model

Диаграмма потоков данных (flowchart)

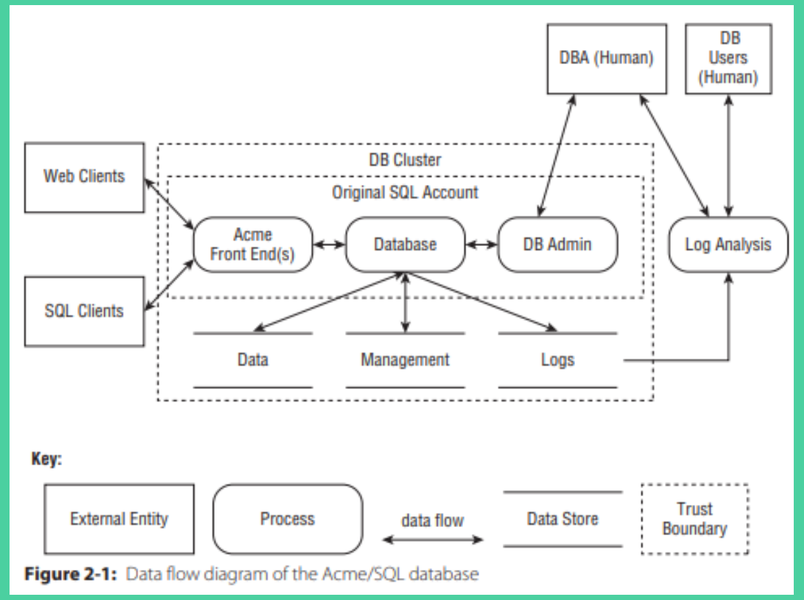


Figure 2-1: Data flow diagram of the Acme/SQL database

Диаграмма состояний (state machine)

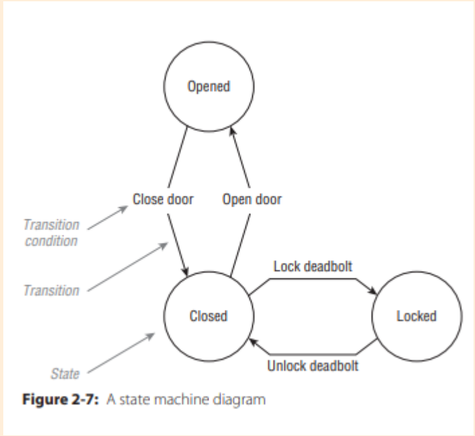


Figure 2-7: A state machine diagram

Swimlane-граф

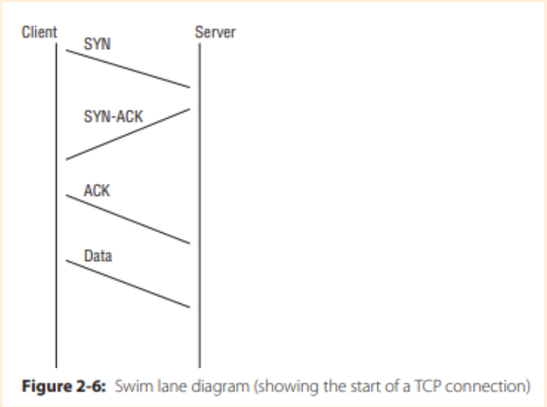
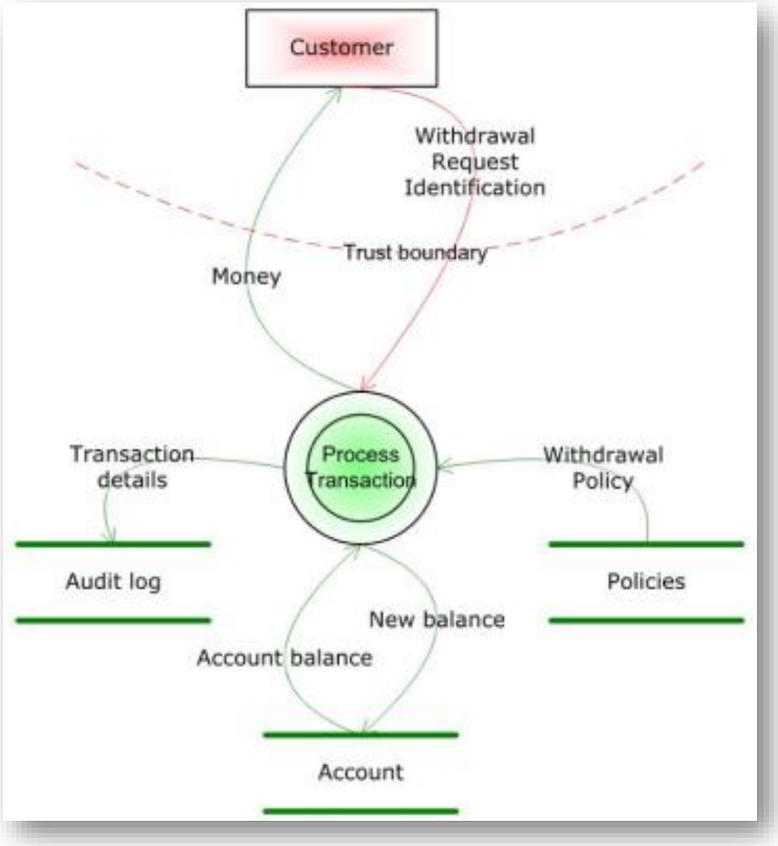


Figure 2-6: Swim lane diagram (showing the start of a TCP connection)

ЧТО ОБЯЗАТЕЛЬНО ДОЛЖНО БЫТЬ НА СХЕМЕ

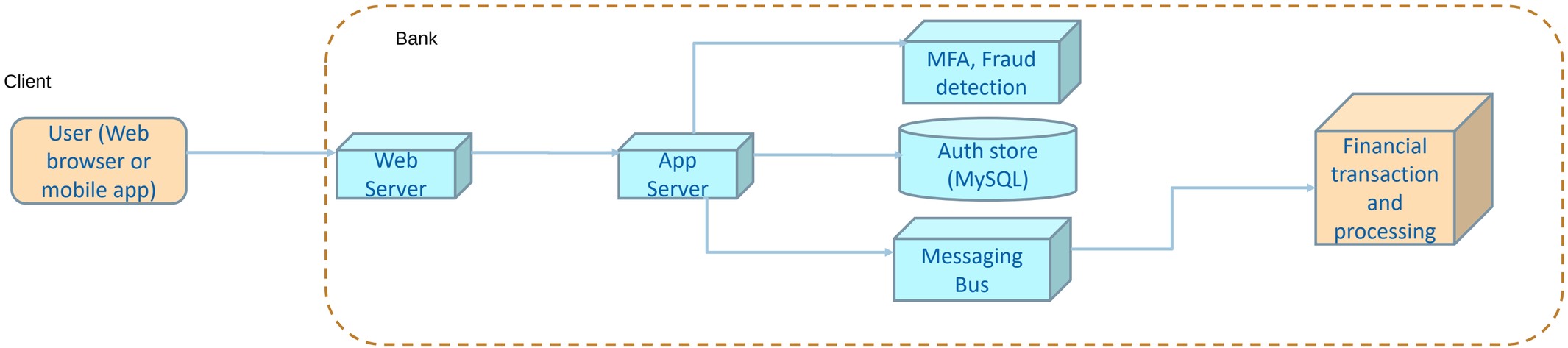
1. ЛОГИЧЕСКИЕ компоненты системы, понимаемые как единое доверенное целое. Используйте необходимый уровень гранулярности, чтобы не забыть про все защищаемых объекты. – *Components*
2. Помечайте объекты - *In scope and Out of scope*.
3. Контролируемые зоны - *Trust boundaries*
4. Потоки данных, включая прямой или непрямой контроль, управление, API и т.п. – *Data Flows*
5. Укажите запросы и ответы для каждого взаимодействия. – *Interconnection's labeling*
6. Определите источники и получатели данных для каждого взаимодействия: не должно быть запросов/ответов «в пустоту».
7. Спросите себя, все ли отражено, и если что-то еще, что поможет подумать «что может пойти не так».



СХЕМА

- Components
- In Scope/Out of scope
- Trust boundaries
- Data Flows
- Interconnections' labeling

1. Банковское приложение (ДБО)
2. Клиенты заходят через браузер, либо мобильное приложение.
3. Все сервера банка расположены в 1 здании (контролируемая зона).
4. Не рассматриваем антропогенные угрозы (т.е. должен быть нарушитель).
5. Не рассматриваем ошибки персонала.
6. Вопросы к схеме? Перерисуйте.



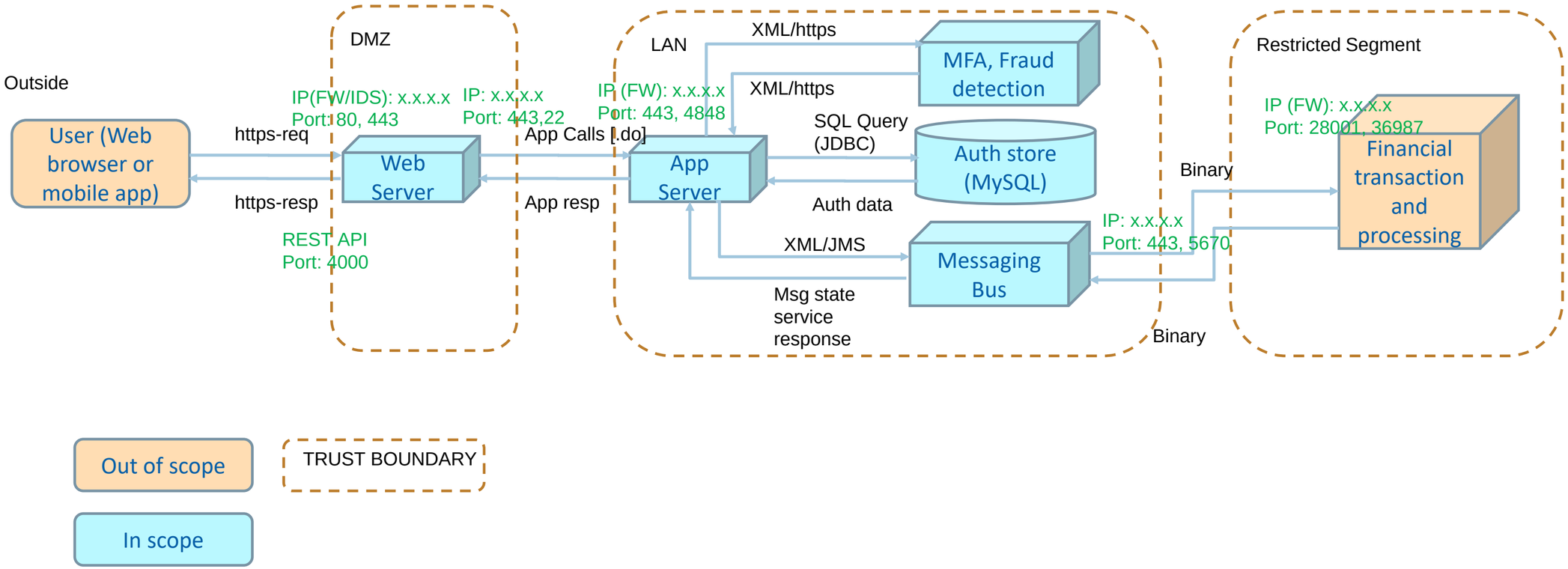
Out of scope

TRUST BOUNDARY

In scope

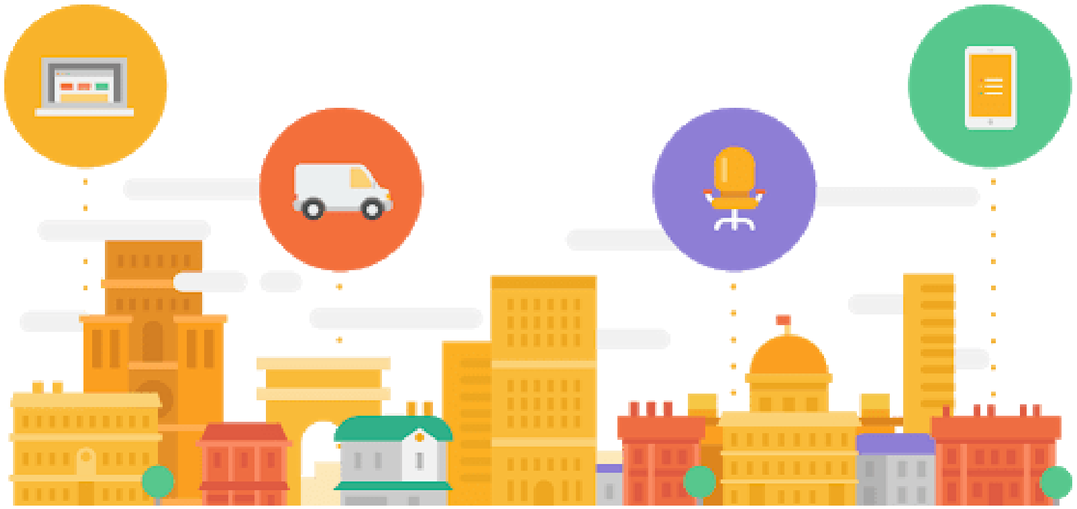
ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ (НА БУДУЩЕЕ)

1. Key management?
2. Key storage?
3. If mobile app – why out of scope?
4. MFA breakdown?

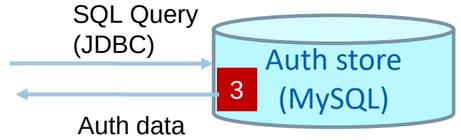


ASSET

ASSET (защищаемый объект) – любой ресурс, который контролирует и которым владеет компания и который может быть использован для создания экономической ценности (business value).



- Device
- Web session, cookies
- Proper System function (system integrity)
- System Availability
- Data integrity
- Local execution
- Meta data
- Collected and Processed Data
- Passwords, Keys, Certificates
- Config Files, Startup Scripts
- Personal Data
- Publicly Available Data (Potential Integrity Issues)
- Intellectual Property
- Source Code and Secrets in Build and Deployment Pipeline
- Logs, Alerts
- Confidential company data

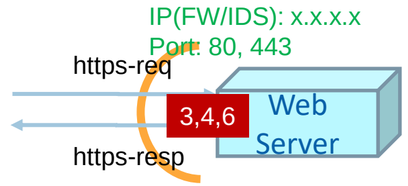


Assets:
3.User credentials

ATTACK SURFACE

ATTACK SURFACE (поверхность атаки) – пути, через которые злоумышленник (adversary) атакует систему и активы (assets).

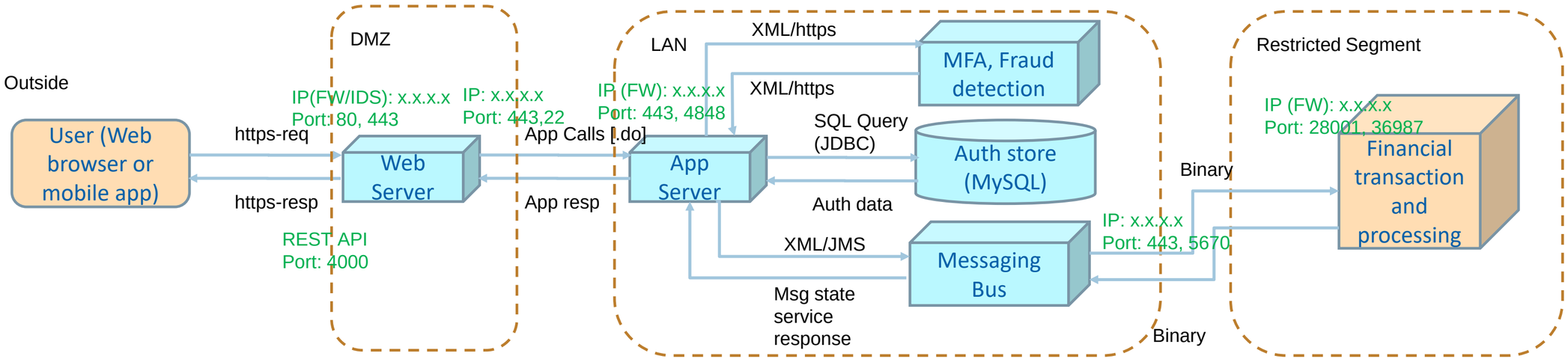
- IP
- DB Port
- Network port
- File system
- Web browser
- Resp API
- Any external interface



- Proper System function (system integrity)
- System Availability
- Data integrity
- Collected and Processed Data
- Passwords, Keys, Certificates
- Publicly Available Data (Potential Integrity Issues)
- Data

ПРИМЕР

1. Активы?
2. Поверхность атаки (точки входа)?



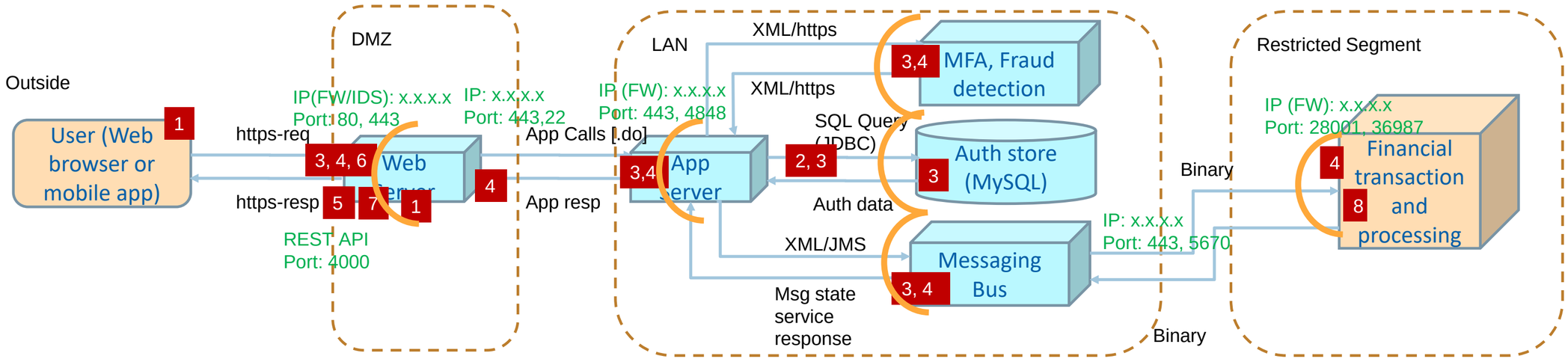
Out of scope

In scope

TRUST BOUNDARY

ПРИМЕР

1. User's web session
2. DB credentials
3. User credentials
4. Client data
5. Web server availability
6. API tokens
7. Service integrity
8. Bank property (data)



Out of scope

In scope

TRUST BOUNDARY

Attack surface

Еще вопросы:

1. Insider threats?
2. Vendor-specifics?
3. Update/provisioning systems?

ASSET VIEW

ID	Asset	Description	Location	Security violations	Business or client Impact	Who should have access (Trust Model)	Attack Points
1	User’s web session	Session logs and cookies stored on local machine	User’s machine, non-controllable	Confidentiality, Integrity	Low (only one user compromised without direct impact)	User, User’s browser, System OS, web server	Client/Web Browser after auth, Server during session lifetime
4	Client data	User’s personal and payment info	• Public Internet • Web Server – App Server • MFA/Fraud detection, Messaging bus • Messaging bus – Financial transaction	Confidentiality, Integrity	Medium (only one user compromised, but impact may be)	User, MFA/Fraud Server, Financial server	During all communications, on servers-at-rest
5	Web server availability	24/7 any authorized user should be able to use the service from the wide Internet	Web server	Availability	High (huge impact if the service is not available)	User	Web server external IPs/interface

В зависимости от понимания системы и для удобства может быть полезно составить таблицы, отталкиваясь от других представлений («развернуть»):

- System element view
- Attack surface view

Именно поэтому «одна портянка» может быть не лучшим решением.

FIND THREATS

0. Subject

1. Model System

2. Find Threats

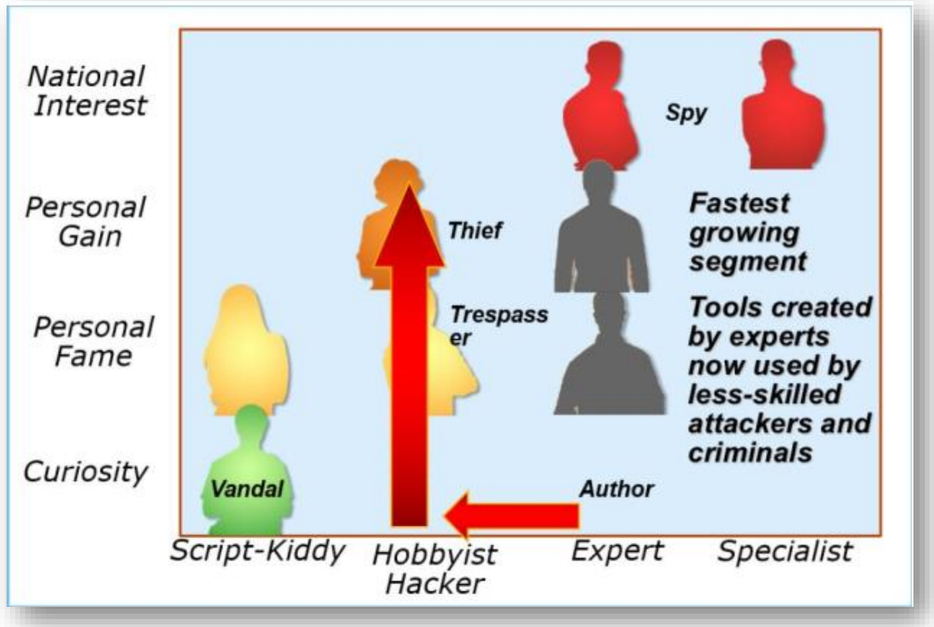
3. Address Threats

4. Validate

ADVERSARIES (НАРУШИТЕЛИ)

Individual	Group	Organization	Nation-state
Outsider	Ad hoc	Competitor	
Insider	Established	Supplier	
Trusted Insider		Partner	
Privileged Insider		Customer	

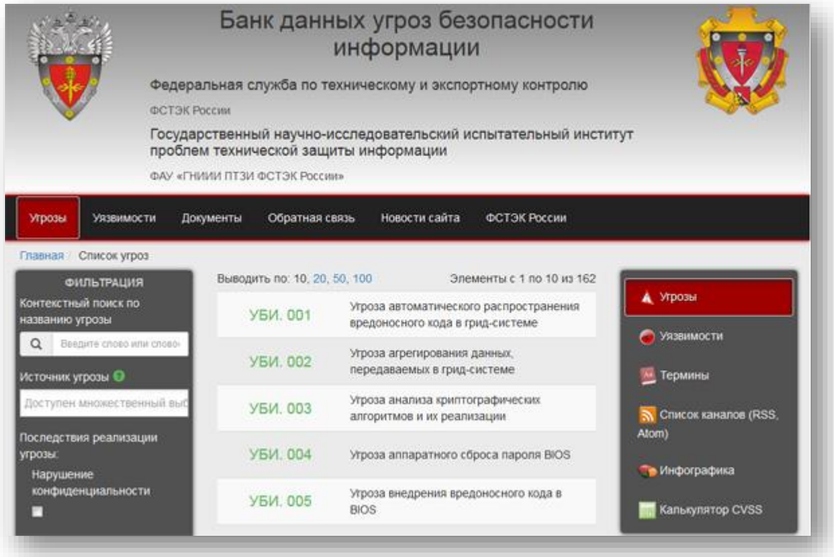
ID	Persona	Motivation	Starting Privilege Level	Skill and Potential Effort level
1	Malicious System administrator	Insider who wants to exfiltrate data.	High privilege level	Highly skilled, dedicated
2	Malicious external user	Wants to increase amount/bonuses for themselves	User-level privileges (service account only)	Unskilled, gives up easily
3	Hired hacker	Works for competitor, wants to harm the service	No privileges, access to published service	Highly skilled, dedicated



Можно использовать любой классификатор (даже H1, H2...), но важно составить упорядоченный список нарушителей.

КАК СОСТАВЛЯТЬ ПЕРЕЧЕНЬ УГРОЗ

1. Можно использовать любой классификатор угроз для вдохновения (рассмотрим далее).
2. Каждый актив (asset) каждая точка входа (attack surface) должны быть рассмотрены.
3. Учитавая каждый тип нарушителя, его возможности и МОТИВАЦИЮ, что он может сделать плохого?
4. Делайте предположения (assumptions): даже если не нашли в классификаторах как это правильно сформулировать в виде угрозы.
5. Постарайтесь избегать «портянок».

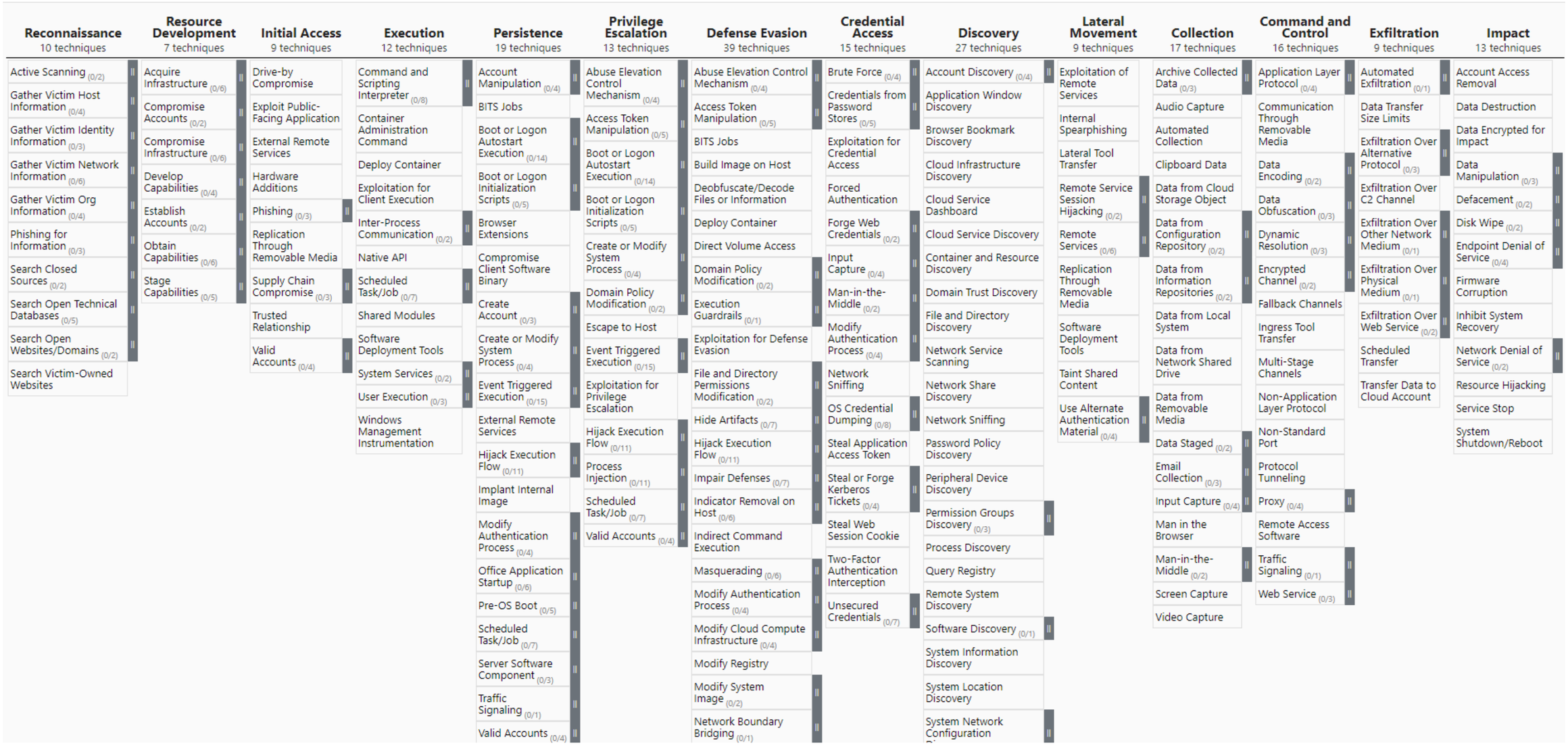


ГДЕ ИСКАТЬ ВДОХНОВЕНИЕ

Name eng	Name ru	Description ru	Examples
Spoofing	**Спуфинг**	Предполагает незаконный доступ к данным пользователя (включая имя пользователя и пароль), используемыми для аутентификации, и их последующего применения.	Failure to prevent users creating weak credentials Use of shared accounts and credentials Weakness in offline process to reset credentials
Tampering	**Незаконное изменение**	Предполагает вредоносное изменение данных. Примеры включают несанкционированные изменения, внесенные в постоянные данные, например хранящиеся в базе данных, а также изменение данных при их передаче между двумя компьютерами через открытую сеть, например Интернет.	Failed to properly assign and check permissions It is possible for attacker to tamper with cookies File upload feature fails to block malware
Repudiation	**Отказ**	Речь идет о пользователях, которые отрицают выполнение действий, если другие пользователи не могут доказать обратное. Например, пользователь может выполнить незаконную операцию в системе, где отсутствует возможность трассировки запрещенных операций. Неподдельность означает способность системы учитывать угрозы отказа. Например, пользователь, который покупает товар, должен расписаться на квитанции при получении товара. Продавец может использовать эту квитанцию как доказательство того, что покупатель уже получил товар.	Lack of integrity signatures on logs for sensitive actions Lack of logging sensitive user actions, such as delete account Lack of logging of administrative activities
Information Disclosure	**Раскрытие информации**	Предполагает раскрытие сведений пользователям, которые не должны иметь к ним доступ, например возможность прочитать файл, к которому этим пользователям не предоставлен доступ, или возможность для злоумышленника считать данные при их передаче между двумя компьютерами.	Secrets are stored in plain text in source control Configuration of TLS is vulnerable to a ‘downgrade’ attack Possible for malicious process to read sensitive information from logs
Denial of Service	**Отказ в обслуживании**	DoS-атака — это буквально отказ в обслуживании для допустимых пользователей, что делает веб-сервер временно недоступным или непригодным для использования. Следует защищаться от определенных типов угроз DoS-атак, просто чтобы повысить доступность и надежность системы.	Exposure of unnecessary services to the Internet Lack response plans to block traffic from a particular source
Elevation of Privilege	**Несанкционированное получение привилегий**	Непривилегированный пользователь получает привилегированный доступ, т. е. достаточные полномочия для нарушения работоспособности или уничтожения всей системы. Угроза повышения привилегий включает ситуации, в которых злоумышленник эффективно обходит все средства защиты системы, сам становясь частью надежной системы. Тем самым он создает действительно опасную ситуацию.	A known vulnerability in infrastructure component is exploited due to failure to apply patches in production Possible to escalate privilege from another system Developer mode tools or default admin credentials are enabled

ГДЕ ИСКАТЬ ВДОХНОВЕНИЕ

MITRE | ATT&CK®



TRIPLE “A” MATRIX

Asset-Attack surface-Adversary Matrix

ID	Asset	Attack Points
1	User’s web session	Client/Web Browser after auth, Server during session lifetime
4	Client data	During all communications, on servers-at-rest
5	Web server availability	Web server external IPs/interface

+

ID	Persona	Motivation	Starting Privilege Level	Skill and Potential Effort level
1	Malicious System administrator	Insider who wants to exfiltrate data.	High privilege level	Highly skilled, dedicated
2	Malicious external user	Wants to increase amount/bonuses for themselves	User-level privileges (service account only)	Unskilled, gives up easily
3	Hired hacker	Works for competitor, wants to harm the service or steel data	No privileges, access to published service	Highly skilled, dedicated

Ответьте на вопрос: Как каждый Asset может быть Атакован Через каждую Attack Surface каким-либо Adversary. Впишите ID Adversary на пересечении.

	Web server external IPs/interface	Web Server File system	Messaging bus port
User’s web session	1, 2, 3	…	…
Client data	-	…	…
Web server availability	2	…	…

TRIPLE “A” MATRIX

Asset-Attack surface-Adversary Matrix

ID	Asset	Attack Points
1	User’s web session	Client/Web Browser after auth, Server during session lifetime
4	Client data	During all communications, on servers-at-rest
5	Web server availability	Web server external IPs/interface

+

ID	Persona	Motivation	Starting Privilege Level	Skill and Potential Effort level
1	Malicious System administrator	Insider who wants to exfiltrate data.	High privilege level	Highly skilled, dedicated
2	Malicious external user	Wants to increase amount/bonuses for themselves	User-level privileges (service account only)	Unskilled, gives up easily
3	Hired hacker	Works for competitor, wants to harm the service or steel data	No privileges, access to published service	Highly skilled, dedicated

Ответьте на вопрос: Как каждый Asset может быть Атакован Через каждую Attack Surface каким-либо Adversary. Впишите ID Adversary на пересечении.

	Web server external IPs/interface	Web Server File system	Messaging bus port
User’s web session	3	1	-
Client data	2	-	1
Web server availability	3	1	-

СПИСОК УГРОЗ (ИЗ МАТРИЦЫ)

Threat ID	Name	Adversary	Asset (From asset table)	Attack Method and Attack Type or Surface
1	Client cookie/session hijacking	Hired hacker	User’s web session	XSS, CSRF, Cookie Theft, Click Jacking on the web browser.
2	Session hijacking from Web server	Malicious System administrator	User’s web session	Stealing session directly from Web server filesystem
3	Account fraud	Malicious external user	Client data	Use bugs or vulnerabilities of the service to manipulate with data
4	Client’s data snooping internally	Malicious System administrator	Client data	Sniffing traffic between Financial transaction and Messaging bus
5	External DDOS attack	Hired hacker	Web server availability	Using tools, bot-net, etc., ruined the service
6	Web server damaging from internal network	Malicious System administrator	Web server availability	Utilizing access to web server, damaging OS or applications

Матрица – лишь один из способов пересечь «всех со всеми». Необходимо добавить угрозы из классификаторов и ваши предположения (assumptions).

ADDRESS THREATS

MITIGATIONS (КАК ЗАЩИЩАТЬСЯ)

1. Можно использовать любой классификатор мер защиты для вдохновения.
2. Пока размышляем над кажой митигацией, это хороший шанс исключить некоторые угрозы.
3. Меры могут быть и организационные, даже для глубоко технической угрозы.
4. Вопрос итогового выбора мер и защищаться ли вообще – лучше проводить на этапе оценки рисков.
5. Защитная мера может повлечь новый актив (помните, СрЗИ всегда входили в состав ИСПДн).

УГРОЗЫ И ЗАЩИТНЫЕ МЕРЫ

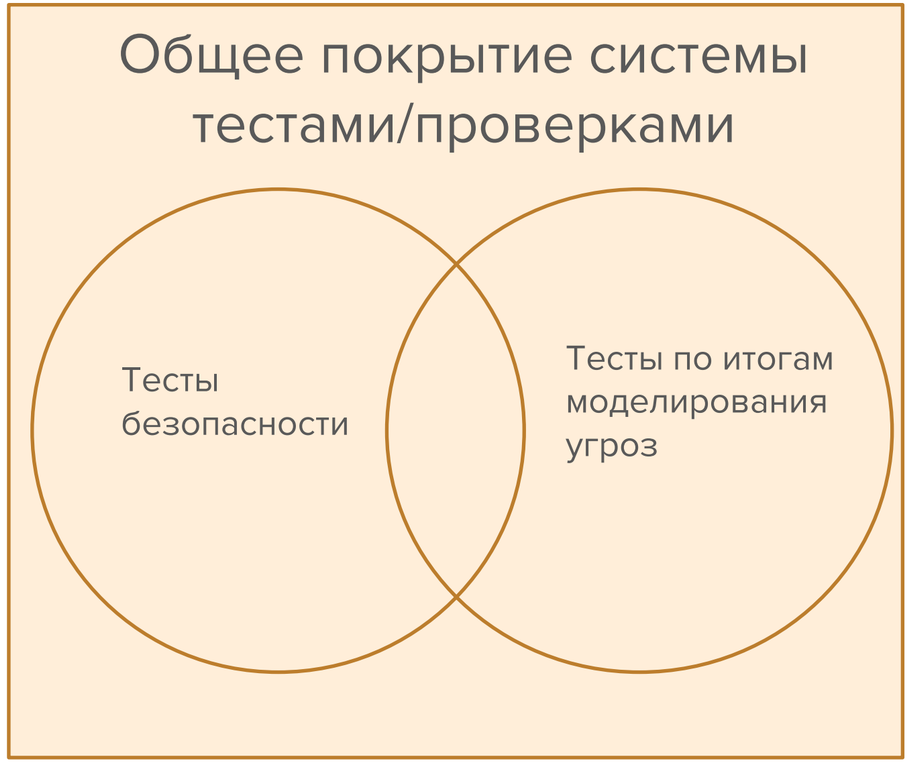
Threat ID	Name	Adversary	Asset (From asset table)	Attack Method and Attack Type or Surface	Mitigation by design	Safeguards (mandatory/recommended)
1	Client cookie/session hijacking	Hired hacker	User's web session	XSS, CSRF, Cookie Theft, Click Jacking on the web browser.	Utilizing a web framework that provides the defenses. Do not store sensitive data in cookies without encryption.	Implement WAF (M)
2	Session hijacking from Web server	Malicious System administrator	User's web session	Stealing session directly from Web server filesystem	Follow least privilege principle. Capture logs.	Implement PAM (R)
3	Account fraud	Malicious external user	Client data	Use bugs or vulnerabilities of the service to manipulate with the data.	Follow least privilege principle. Capture logs.	Implement VM tool (R) Continue using Fraud detection system.(M)
4	Client's data snooping internally	Malicious System administrator	Client data	Sniffing traffic between Financial transaction and Messaging bus	Encrypt traffic. Capture logs.	Implement PAM (R)
5	External DDOS attack	Hired hacker	Web server availability	Using tools, bot-net, etc., ruined the service	Enable default system protection (fail to ban, etc.).	Implement anti-DDOS system (M)
6	Web server damaging from internal network	Malicious System administrator	Web server availability	Utilizing access to web server, damaging OS or applications	Follow least privilege principle. Capture logs.	Implement HA hot reserving.(M) Implement PAM (R)

VALIDATE


0. Subject
1. Model System
2. Find Threats
3. Address Threats
4. Validate

ЗАЧЕМ ПРОВЕРЯТЬ

1. Все найденные угрозы могут (должны) быть продемонстрированы, а эмуляция атак – хороший способ проверить защитные меры.
2. Модель угроз – хороший источник тестов для инженеров (Test-Driven Development).
3. Многие тесты могут (должны) быть автоматизированы в рамках разработки/приемки системы.
4. Попробуйте обойти защитные меры (пентест).
5. Хороший способ обнаружить новые угрозы.

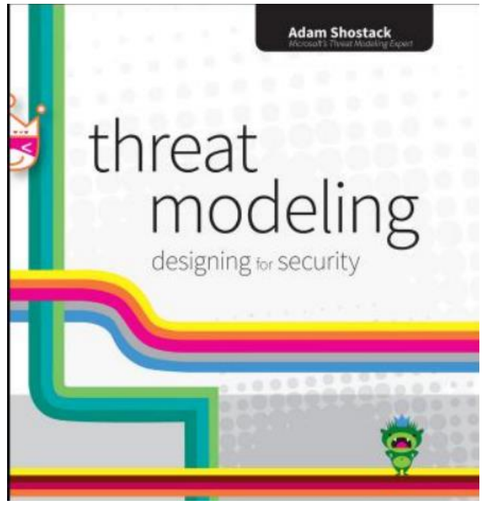


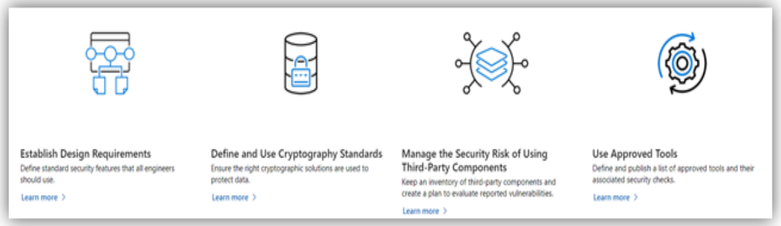
ВСЕ ЛИ МЫ СДЕЛАЛИ ПРАВИЛЬНО?

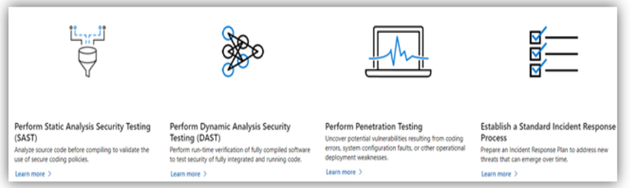
- ✓ У нас было достаточно времени?
- ✓ Все необходимые ресурсы задействованы или было бы хорошо вовлечь кого-то еще?
- ✓ Насколько сложно было приступить (орг. или иные проблемы)?
- ✓ Задачи и скоуп были понятны всем?
- ✓ Мы верим, что наш перечень угроз хорош?
- ✓ Готовы ли мы объяснить понятным языком инженерам?
- ✓ А остальным?
- ✓ Готовы ли мы конвертировать угрозы в риски?

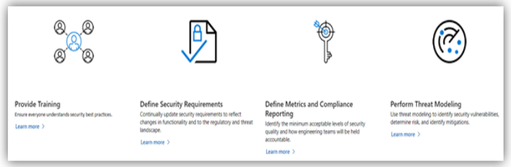
ПОЛЕЗНЫЕ ССЫЛКИ

- ✓ https://www.microsoft.com/en-us/securityengineering/sdl – Microsoft SDL and Threat Modeling tools
- ✓ https://owasp.org/www-community/Threat_Modeling - OWASP TM approach and links
- ✓ https://github.com/mozilla/seasponge - TM tool
- ✓ https://owasp.org/www-project-threat-dragon/ - OWASP TM tool
- ✓ “Threat Modeling. Design for Security”, book by Adam Shostack
- ✓ https://www.nist.gov/cyberframework - NIST CSF
- ✓ https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat/ - CIS Controls and Assessment tool
- ✓ https://attack.mitre.org/matrices/enterprise/# and https://d3fend.mitre.org/









#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

Connect me:

FACEBOOK.COM/R.O.ZHUKOV

ROZHUKOV.BLOGSPOT.COM

LINKEDIN.COM/IN/ROZHUKOV