Законы, стандартизация

Teach
Me
Skills

Собираемся и отмечаемся

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Teach Me Skills

Mini-quize по прошлым темам:

1. **В чем отличие между GET и POST запросами?**
2. **Какие достоинства можно выделить по отношению к правилам YARA?**
3. **Что такое ИБ?**
4. **В чем отличие кибер- и информационной безопасности?**
5. **Какие типы атак проводятся чаще всего и на что они нацелены?**

Teach Me Skills

Mini-quize по новой теме:

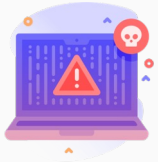
1. **Как вы понимаете что такое Playbook?**
2. **Какие цели у расселдования киберинцедента?**
3. **Что по вашему выгоднее и лучше, создать и поддерживать идеально защищенную систему или восстанавливаться после инцидентов не имея соответсвующей защиты?**
4. **Как можно охарактеризовать защищенную систему?**
5. **Что такое КВОИ?**
6. **Какие бывают виды инцидентов?**

Teach Me Skills

План занятия

1. Изучим основные опредления, пристуствующие в ИБ
2. Рассмотрим основные атаки, инфорграфику
3. Познакомимся с логикой работы злоумышленников
4. Разберемся в общих чертах с реагированием на инциденты
5. Постараемся разобраться в НПА в области ИБ

Основные понятия в сфере ИБ



Уязвимость — это недостаток в программном обеспечении, оборудовании или процедуре, который может предоставить атакующему возможность доступа к инфраструктуре.

Атака — реализованная угроза, приводящая к нанесению ущерба в связи с действиями злоумышленника.

Риск — вероятностная оценка реализации угрозы, описывающая вероятность наступления события и размер ожидаемого ущерба, который может понести владелец информационного ресурса, в случае успешной реализации угрозы.

Угроза — это потенциальная опасность эксплуатации уязвимости для информации или системы.

Контрмеры (или защитные меры) — это меры, внедрение которых позволяет снизить уровень потенциального риска.

Информационная безопасность, направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) и места хранения.

Кибербезопасность защищает **цифровые** данные от компрометации или атак.

Основные понятия в сфере ИБ

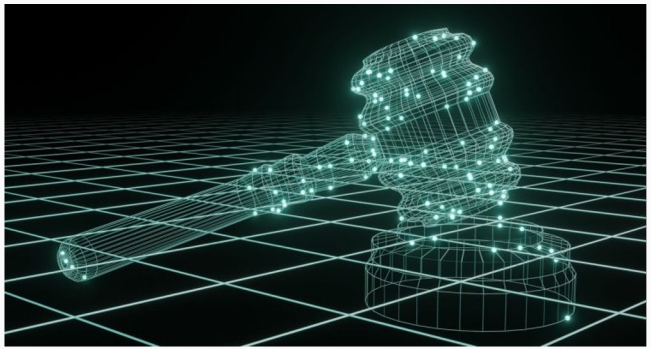
Teach Me Skills

Событие ИБ — идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент ИБ — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или ИБ.

Кибератака - это преднамеренное использование компьютерных систем, сетей и технологий для нанесения ущерба, проникновения, разрушения или получения несанкционированного доступа к информации или ресурсам.

Киберинцидент — событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.



Статистические данные

Индекс развития информационно-коммуникационных технологий (ICT Development Index) — это комбинированный показатель, характеризующий достижения стран мира с точки зрения развития информационно-коммуникационных технологий. Оценивается доступ к ИКТ, использование ИКТ, а также навыки, то есть практические знания этих технологий населением стран, охваченных исследованием.

Индекс развития ИКТ в мире

1	Исландия	8.98
2	Южная Корея	8.85
3	Швейцария	8.74
4	Дания	8.71
5	Великобритания	8.65
6	Гонконг	8.61
7	Нидерланды	8.49
8	Норвегия	8.47
9	Люксембург	8.47
10	Япония	8.43
32	Беларусь	7.55
45	Россия	7.07

2017 г

Глобальный индекс кибребезопасности

1	США	100
2	Великобритания	99.54
3	Саудовская Аравия	99.54
4	Эстония	99.48
5	Южная Корея	98.52
6	Сингапур	98.52
7	Испания	98.52
8	Россия	98.06
9	ОАЭ	98.06
10	Малайзия	98.06
97	Беларусь	50.57

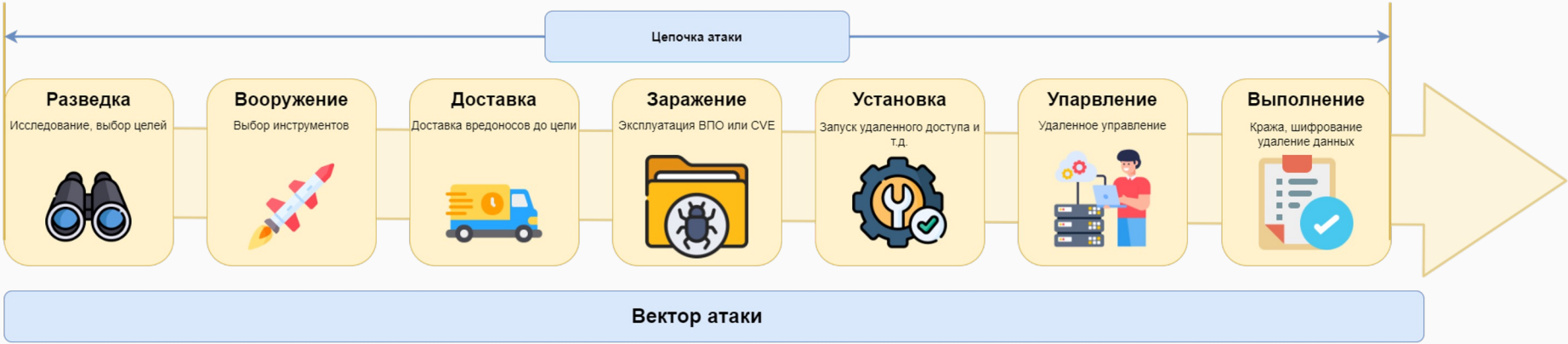
39-е место, 2017 ↓
69-е место, 2018 ↓
97-е место, 2020 ↓

Оценивается юридический, технический, организационная подготовленность, готовность к сотрудничеству, развитие образовательного и исследовательского потенциала страны.

Как действуют злоумышленники

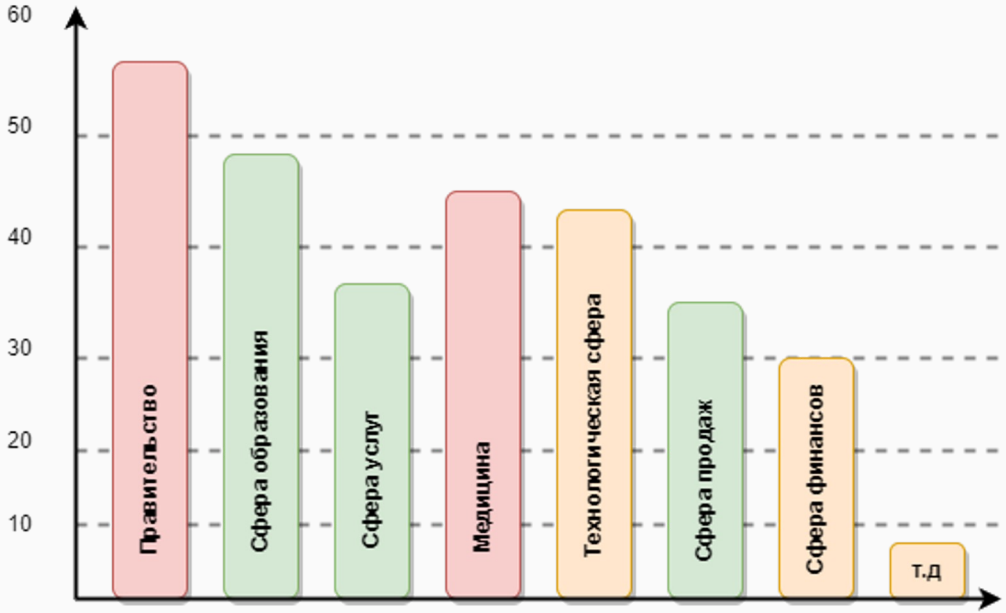
Что мы будем использовать для профилирования действий злоумышленников?

Матрицы MITTRE



Инциденты ИБ

Инцидент ИБ — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или ИБ.



В зависимости от цвета – сложность атак

Предпосылки и реагирование на инциденты

Процесс ИБ

Основные игроки с «темной» стороны

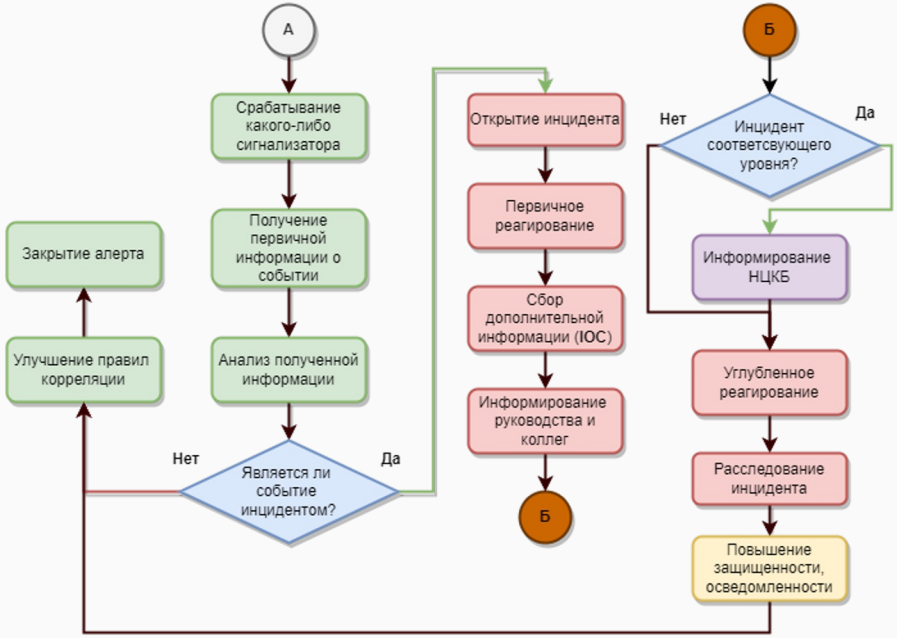
Каким будет результат реагироваия на инцидент?

Повышение осведомленности и защиты инфраструктуры

Какая основная цель злоумышленников?

Получение финансовой выгоды

Расследование инцидентов



Примерный playbook для раегирования на инцидент

Какие IOC вы считаете важными?

Сетевые IOC’s:
URL, DOMAIN, IP_DEST, PORT_DEST

Локальные IOC’s:
HASH, SSDEEP

Документы в отношении ИБ

Teach Me Skills

О кибербезопасности Указ № 40 от 14 февраля 2023 г. → Документ устанавливает правовую основу для создания национальной системы кибербезопасности. Документ подробно определяет функции и задачи по обеспечению кибербезопасности, указывает на владельцев КВОИ, которые обязаны создавать центры кибербезопасности.

Приказ ОАЦ №130 от 25.07.2023. Требования к Центрам кибербезопасности (SOC) → ТРЕБОВАНИЯ к центрам обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций

Указ № 69 "О развитии республиканской системы мониторинга общественной безопасности". Указ № 69 от 25 февраля 2022 г. → Документ предусматривает переход от компании "24x7 Паноптес" к РУП "Белтелеком" в качестве оператора системы мониторинга общественной безопасности. РУП "Белтелеком" становится ответственным за создание и поддержание системы мониторинга, а также за хранение информации, также говорится о добавлении специальных технических средств в систему для автоматической фиксации административных правонарушений.

Регуляторы в сфере ИБ

Teach Me Skills

Национальные Агентства по Информационной Безопасности:

1. *Национальное агентство по кибербезопасности (**CISA**) США:* Занимается координацией и реагированием на киберугрозы в Соединенных Штатах.

2. *Национальный центр кибербезопасности (**NCSC**) Великобритания:* Ответственен за укрепление национальной кибербезопасности и предоставление советов и ресурсов.

3. *Федеральная служба по техническому и экспортному контролю* (**ФСТЭК**) Россия. Реализует и поддерживает политику государства в сфере ИБ, осуществляет взаимодействие между другими ведомствами.

4. *Оперативно аналитический центр при президенте* (**ОАЦ**) Республика Беларусь. Осуществляет регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь.

Международные Организации:

1. *Интерпол:* Сотрудничает с государствами-членами для борьбы с киберпреступностью и обеспечения кибербезопасности.

2. *Европейское Агентство по кибербезопасности (**ENISA**):* Предоставляет рекомендации и ресурсы для улучшения кибербезопасности в Европейском союзе.

Стандартизационные Организации:

1. *Международная организация по стандартизации (**ISO**):* Разрабатывает стандарты, включая стандарты по управлению информационной безопасностью (ISO/IEC 27001).

2. *Национальный институт стандартов и технологий (**NIST**) (США):* Создает руководства и стандарты, такие как NIST SP 800, связанные с ИБ.

ЦК и НЦКБ

Teach Me Skills

История **CERT** тесно связана с борьбой против сетевых червей.
Первый червь «червь Морриса» парализовал работу узлов интернета. Для борьбы с червём была сформирована первая команда «Computer emergency response team» или «**CERT**».
В дальнейшем команды во всём мире стали называть себя «**CERT**». В англоязычных странах некоторые группы называли себя аббревиатурой «**CSIRT**».

CERT.BY осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Республики Беларусь, а также реагирование на сами инциденты как в информационных системах государственных органов и организаций, так и у самостоятельно обратившихся субъектов национального сегмента сети Интернет.

BC-CERT.BY Основная задача команды реагирования - снижение уровня угроз информационной безопасности в зоне ответственности сетей и сервисов ООО "Белорусские облачные технологии“. И имеет дело с инцидентами, происходящими или направленными на зону ответственности сетей и сервисов .

Team	Official Team Name	Country
BC-CERT.BY (Suspended)	BeCloud CERT TEAM	BY
CERT.BY (Suspended)	National CERT of Belarus	BY

Teach
Me
Skills

Спасибо за внимание!