Анализ инцидентов.

Вопросы

- 1. Основные понятия.
- 2. Классификация инцидентов ИБ.
- 3. Основные предпосылки возникновения инцидентов.
- 4. Управление инцидентами ИБ.
- 5. Расследование инцидентов ИБ.
- 6. Примеры расследования и анализа инцидентов ИБ.

Вопросы

- 1. Основные понятия

Основные понятия

- **Уязвимость** — это недостаток в программном обеспечении, оборудовании или процедуре, который может предоставить атакующему возможность доступа к компьютеру или сети и получения несанкционированного доступа к информационным ресурсам.
- **Угроза** — это потенциальная опасность эксплуатации уязвимости для информации или системы.

Основные понятия

- **Риск** — вероятностная оценка реализации угрозы, описывающая вероятность наступления события и размер ожидаемого ущерба, который может понести владелец информационного ресурса, в случае успешной реализации угрозы.
- **Воздействие** (атака) — реализованная угроза, приводящая к нанесению ущерба в связи с действиями источника угрозы.
- **Контрмеры** (или защитные меры) — это меры, внедрение которых позволяет снизить уровень потенциального риска.

Основные понятия

- **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.

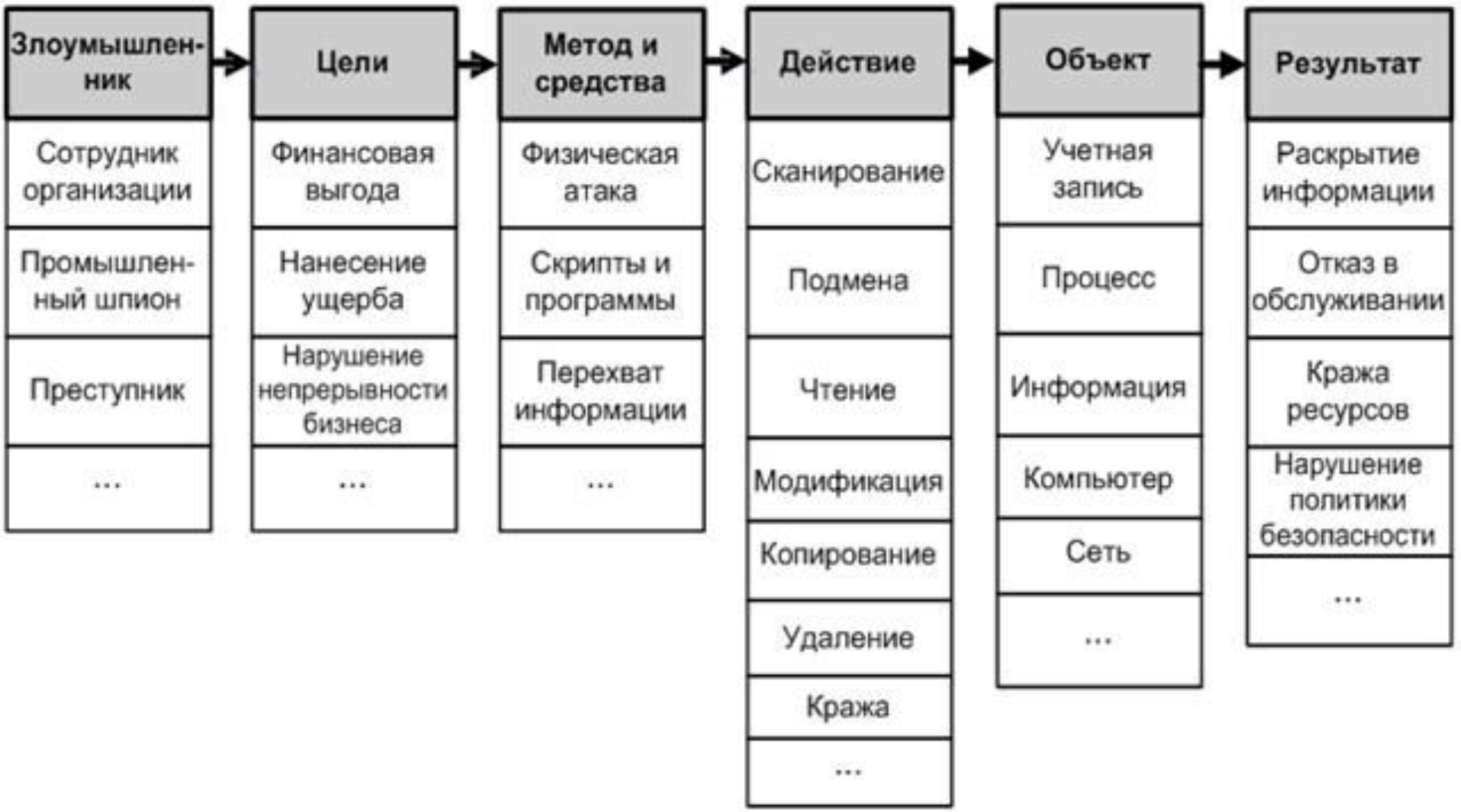
Основные понятия

- **Киберинцидент** — событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.
- **Кибератака** — целенаправленное воздействие программных и (или) программно- аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Вопросы

- 2. Классификация инцидентов ИБ.

Классификация инцидентов ИБ



Классификация инцидентов ИБ

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Классификация инцидентов ИБ

- Блокирование доступа к информации
- Распространение вредоносного программного обеспечения
- Несанкционированный доступ, модификация, похищение информации
- Сетевые атаки

Вопросы

- 3. Основные предпосылки возникновения инцидентов.

Основные предпосылки возникновения инцидентов

- 1. **Слабые** парольные политики, **отсутствие** защиты от подбора пароля (капчи, двухуровневая аутентификация, установка правил сложности пароля).
- 2. **Установка** логинов и паролей (особенно администраторы) на рабочие учетные записи отличные от учеток для **личного** пользования любых сервисов и сайтов.
- 3. **Несменяемые** пароли.
- 4. Использование **нешифрованных** протоколов передачи данных.
- 5. Использование **устаревших** и неподдерживаемых протоколов и сервисов.

Основные предпосылки возникновения инцидентов

- 6. Несвоевременная **установка обновлений**, патчей и фиксов.
- 7. Не проводится **замена оборудования**, которое больше не поддерживается поставщиком, и на которое, соответственно, больше не выпускаются обновления ПО и патчи безопасности. Лучше всего менять оборудование до того как закончится поддержка производителя.
- 8. Оставляют **стандартные настройки** и пути (особенно к админке) движков, платформ, устройств.
- 9. Не проводится **инвентаризация** технических средств, ПО и активов.

Основные предпосылки возникновения инцидентов

- Рекомендации по соблюдению «цифровой гигиены» и организации безопасной работы в удаленном режиме
- https://cert.by/?p=1572
- Распространенные проблемы и ошибки, приводящие к компрометации интернет-ресурсов
- https://cert.by/?p=1897
- https://cert.by/?p=1942

Вопросы

- 4. Управление инцидентами ИБ.

Управление инцидентами ИБ

- ISO/IEC 27035-1:2016
- ISO/IEC 27035-2:2016
- ISO/IEC 27035:2011

Управление инцидентами ИБ

- **ЦЕЛИ** (один из возможных вариантов списка)**:**
- гарантировать **целостность** критически важных систем;
- сохранить и восстановить **данные**;
- сохранить и восстановить **сервисы**;
- выяснить, **почему** инцидент ИБ стал возможен;
- предотвратить **развитие** атак и **будущие** инциденты ИБ;
- избежать нежелательной **огласки** информации об инциденте ИБ;
- найти **виновников** инцидента ИБ;
- наказать **нарушителей** ПИБ организации.

Управление инцидентами ИБ

- **Виды деятельности:**
- Обнаружение и регистрация
- Оценка, классификация и приоритезация
- Сохранение информации
- Всестороннее исследование
- Разрешение и закрытие
- Извлечение уроков
- Подготовка к усовершенствованию процесса управления

Вопросы

- 5. Расследование инцидентов ИБ.

Расследование инцидентов ИБ

- **Основные цели:**
- локализация и ликвидация последствий инцидентов ИБ;
- установление виновных лиц и их мотивации, обеспечение возможности привлечения их к ответственности.

Расследование инцидентов ИБ

- **Виды деятельности:**
- сбор свидетельств и их анализ;
- выявление виновных;
- установление причин, давших возможность инциденту произойти;
- вынесение рекомендаций по принятию мер по предотвращению инцидентов;
- хранение и защита материалов расследования.

Вопросы

- 6. Примеры инцидентов.

- СПАСИБО ЗА ВНИМАНИЕ!