Основы защиты информации

Петров Сергей Николаевич
к.т.н., доцент кафедры защиты информации
petrov@bsuir.by

16 ЛК 12ПЗ **зачет**

Информационная безопасность. Важность проблемы. Основные понятия.

Лекция 1

Информация

Информация от латинского informatio – ознакомление, разъяснение

Информация – сведения

(о лицах, предметах, фактах, событиях, явлениях и процессах)

независимо от формы их представления

- Закон Республики Беларусь от 10.11.2008 N455-З «Об информации, информатизации и защите информации»

Свойства информации

- Информация доступна человеку, если она содержится на материальном носителе
- Информация имеет ценность
- Ценность информации изменяется со временем
- Информация покупается и продается
- Количество информации сложно оценить

Изменение информации во времени

$$C(t) = C_0 e^{-2.3t/\tau}$$

Co - ценность информации в момент ее возникновения

t - время от момента возникновения информации до момента определения ее стоимости;

τ - время от момента возникновения информации до момента ее устаревания.

Информация

- Электронные носители

- Поля и волны

- Бумажные носители

- **База данных** - совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях

- **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

- **Информационная сеть** - совокупность информационных систем, взаимодействующих посредством сетей электросвязи;

Проблемы информационной безопасности

- Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности, конфиденциальности, доступности и сохранности информации

Закон Республики Беларусь от 10.11.2008 N455-З
«Об информации, информатизации и защите информации»

Направления кибербезопасности

- Network security
- Application Security
- Mobile Security
- Malware/Spyware Analysis
- Risk Audit/Management
- Cyber Forensics
- Penetration Tester
- Network security analyst
- Security analyst
- OS secuirty
- System security (user level)
- System security (kernel level
- Encryption explicitly
- Decryption explicitly

Свойства информационных ресурсов

Integrity

- **Целостность –** неизменность информации в процессе ее передачи или хранения

- данные не были изменены при выполнении какой-либо операции над ними

Свойства информационных ресурсов

Availability

- **Доступность** – свойство информационных ресурсов, определяющее возможность их беспрепятственного получения и использования по требованию уполномоченных лиц

24/7 service

Свойства информационных ресурсов

Confidentiality

- **Конфиденциальность** – свойство информационных ресурсов, связанное с тем, что они не станут доступными для неуполномоченных лиц
- Обязательное для лица, получившего доступ к информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

ОСНОВНЫЕ ТЕРМИНЫ

Угроза threat

возможность возникновения такой ситуации, следствием которой может стать нарушение безопасности информации.

Связанные понятия

- **источник угрозы** - субъект, являющийся непосредственной причиной возникновения угрозы
- **модель угроз** - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации

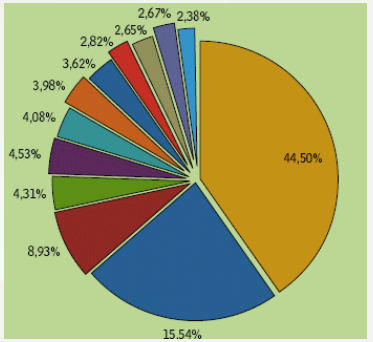
Классификация угроз

- по цели реализации угрозы, нарушение **доступности, целостности, конфиденциальности**

- по компонентам информационных систем, на которые угрозы нацелены **(данные, программы, аппаратура, поддерживающая инфраструктура)**;

- по характеру **(случайные/преднамеренные, природные/техногенного характера)**;

- по расположению источника угроз **(внутренние/внешние)**.



ОСНОВНЫЕ ТЕРМИНЫ

Уязвимость vulnerability

свойство (недостаток или слабое место) информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Если уязвимость соответствует угрозе, то существует риск.

ОСНОВНЫЕ ТЕРМИНЫ

Риск risk

- вероятный ущерб, который понесет компания при раскрытии, модификации, утрате или недоступности своей информации.

- **анализ информационного риска**: выявление угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз.

ОСНОВНЫЕ ТЕРМИНЫ

Атака attack, intrusion

попытка реализации угроз информации называются.

Связанные понятия

- **Злоумышленник** - лицо предпринявшее такую попытку
- **Вектор атаки** - последовательность действий (способ) для получения неавторизованного доступа к защищённой информационной системе

например, URL сайта с get-параметрами в нем или форма ввода информации

ОСНОВНЫЕ ТЕРМИНЫ

Несанкционированный доступ

unauthorized access

Доступ с нарушением установленных прав доступа и правил разграничения доступа

Иначе – неправомерный или нелегитимный

ОСНОВНЫЕ ТЕРМИНЫ

Утечка информации

information leakage

Неконтролируемое распространение защищаемой информации в результате разглашения или НСД

- Преднамеренная
- Непреднамеренная

В результате чего обладатель информации ограниченного доступа утрачивает контроль над этой информацией

ОСНОВНЫЕ ТЕРМИНЫ

Канал утечки информации

information leakage channel

Способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

Канал утечки информации

примеры

- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).
- «Сеть» – утечка через браузер (отправка данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
- «Бумажные документы» – утечка вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).

ОСНОВНЫЕ ТЕРМИНЫ

Канал утечки информации

Отличается от более конкретного понятия

Технический канал утечки информации

Технический канал утечки информации – совокупность источника информации, линии связи (физической среды), шумов и технических средств перехвата информации

Компрометация данных

compromise

Факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Например, компрометация банковской карты — ситуация, при которой данные банковской карты (пароль и логин от интернет-банка, ПИН-код, одноразовый пароль, данные паспорта владельца карты и секретное слово) стали известны другому лицу,

в результате чего ее дальнейшее использование представляется небезопасным

ОСНОВНЫЕ ТЕРМИНЫ

Инцидент информационной безопасности
Information security incident

Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность

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

Решения для инфраструктурной безопасности

Защищаемый компонент ИТ-инфраструктуры	Тип решения
ИТ-инфраструктура	Управление сетевой безопасностью (Firewall Management)
	Межсетевые экраны (Firewalls)
	Обнаружение/предотвращение вторжений (Intrusion Detection System – IDS, Intrusion Prevention System – IPS)
	Системы противодействия целевым атакам (Advanced Persistent Threat) – Anti-APT
	Системы мониторинга трафика
	Системы класса Deception
	Защита каналов связи
	Защита виртуальных сред
	Средства перенаправления web-трафика (Web-proxy)
	Защита от спама
	Защита от 0-Day атак
	Система сканирования уязвимостей
	Системы резервного копирования и восстановления информации

Решения для инфраструктурной безопасности

Защищаемый компонент ИТ-инфраструктуры	Тип решения
Конечные точки	Антивирусная защита (Anti-Virus Protection - AVP)
	Системы обнаружения атак и реагирования на них (Endpoint, Detect & Response - EDR)
	Защита банкоматов
	Контроль подключения внешних устройств
Доступ	Системы управления корпоративной мобильностью (Enterprise Mobile Management - EMM)
	Идентификация и контроль доступа к сети (Network Access Control - NAC)
	Системы управления многофакторной (расширенной) аутентификацией (Multi-Factor Authentication – MFA или Advanced Authentication – AA)
Web	Защита web-приложений и сайтов (Web Application Firewall - WAF)
	Защита от DDoS атак

Решения для People-Centric Security

Название системы	Класс	Функции
Автоматизированная система управления учетными записями и правами пользователей (создается на базе продуктов класса Identity Management)	IDM	Автоматизирует управление учетными записями и правами пользователей в информационных системах заказчика, построения ролевых моделей, аудита имеющихся доступов
Автоматизированная система контроля за действиями привилегированных пользователей (создается на базе продуктов класса Privileged Account Management)	PAM	Обеспечивает контроль за действиями системных администраторов, специалистов подрядчиков, аудиторов и других пользователей с расширенными правами
Автоматизированная система защиты от утечек конфиденциальной информации (создается на базе продуктов класса Data Loss Prevention)	DLP	В режиме реального времени анализирует все информационные потоки для контроля переписки по эл. почте, голосовых и текстовых сообщений, переданных файлов, информации, отправляемой на облачные сервисы или принимаемой с них, внешних устройств, документов, отправляемых на печать и т.д. и сообщает о возможных инци-дентах
Автоматизированная система противодействия мошенничеству (создается на базе продуктов класса Anti-fraud)	AFR	Автоматизирует контроли для борьбы с: • внутренним мошенничеством; • клиентским и/или платежным мошенничеством в системах дистанционного банковского обслуживания; • неплатежным мошенничеством (закупки, склад, учет и т. д.)

Решения для People-Centric Security

Название системы	Класс	Функции
Автоматизированная система тестирования и обучения сотрудников практической кибербезопасности	APH	Имитирует фишинговые атаки, выявляет сотрудников с недостаточным уровнем знаний и/или навыков в области ИБ и предоставляет инструменты для обучения
Автоматизированная система защиты баз данных	DAM	Обеспечивает безопасность СУБД и независимый аудит операций с базами данных и бизнес-приложениями
Автоматизированный анализатор исходного кода приложений	SAST	Позволяет анализировать код приложений на наличие уязвимостей

Решения для центров управления ИБ

Название системы	Класс	Функции
Автоматизированная система мониторинга, корреляции и анализа событий ИБ (создается на базе решений класса Security Information and Event Management)	SIEM	Обеспечивает получение информации о событиях ИБ из различных источников (межсетевые экраны, средства защиты баз данных и приложений, средства контроля за работой пользователей, операционные системы и др.), анализирует их, в результате чего определяет и сигнализирует о появлении инцидентов
Автоматизированная система мониторинга и управления инцидентами ИБ (создается на базе решений класса Incident Response Platform)	IRP	Обеспечивает инвентаризацию ИТ-активов, регистрацию инцидентов ИБ, назначение и контроль задач по работе с инцидентами, запуск преднастроенных алгоритмов и автоматизированных сценариев, которые обеспечивают быстроту реакции и слаженность действий команды реагирования, помогая свести к минимуму возможные негативные последствия от инцидента
Автоматизированная система управления данными кибер-разведки (создается на базе решений класса Threat Intelligence Platform – TIP)	TIP	Обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре заказчика с помощью сенсоров
Автоматизированная система управления информационной безопасностью (создается на базе решений класса Security Governance, Risk, Compliance)	SGRC	Обеспечивает автоматизацию таких процессов, как: • управление рисками ИБ; • моделирование угроз; • аудит ИБ; • контроль и управление ИТ-активами; • планирование и контроль задач специалистов по ИБ
Автоматизированная система инвентаризации активов (создается на базе решений класса (Asset Control Platform - ACP)	ACP	Позволяет автоматизированно: • вести единый, полный и актуальный реестр активов; • осуществлять контроль изменений ИТ-инфраструктуры; • выполнять инвентаризацию несколькими способами;

АНАЛИТИКА InfoWatch

InfoWatch - разработчик решений для анализа и предотвращения утечек корпоративных данных

КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

КЛАССИФИКАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

- Правовые
- Технические
  - Криптографические
  - Физические
- Организационные

- **ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ**: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

- **ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
- ----------

- **КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**: Защита информации с помощью ее криптографического преобразования.

- **ФИЗИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**: Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

итоги

- **Информация и формы ее представления**

Документы
Физические поля и волны
Электронные носители

Базы данных
Информационные системы

итоги

- **Основные концепции и подходы ИБ**

Конфиденциальность
Доступность
Целостность

Правовые
Организационные
Технические

- № 455-З РБ «Об информации, информатизации и защите информации»

итоги

- **Основные понятия области ИБ** (угроза, уязвимость, утечка, атака, риск…)
  - СТБ 1596-2009 РБ «Информационная безопасность сети электросвязи»
  - № 455-З РБ «Об информации, информатизации и защите информации»
  - 149-ФЗ Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»
  - Словарь терминов по информационной безопасности (энциклопедия безопасника)
    - https://ib-bank.ru/glossary/