Технологии информационной безопасности - Темы лекций курса

Продолжительность курса: 3 месяца, 2 часа/неделю (24-30 часов всего)

Тема 1: Основы информационной безопасности

1.1 Базовые концепции и терминология

- Определение информационной безопасности и кибербезопасности
- Триада КЦД: Конфиденциальность, Целостность, Доступность
- Дополнительные свойства безопасности: Аутентификация, Неотрекаемость, Подотчётность
- Активы, угрозы, уязвимости и риски
- Инциденты безопасности и нарушения безопасности
- Принцип эшелонированной защиты
- Безопасность на этапе проектирования и безопасность по умолчанию

1.2 Ландшафт угроз и векторы атак

- Классификация субъектов угроз: национальные государства, киберпреступники, хактивисты, инсайдеры
- Характеристики продвинутых постоянных угроз (APT)
- Векторы атак: сетевые, прикладные, физические, социальные
- Жизненный цикл уязвимостей и ответственное раскрытие
- Общие уязвимости и экспозиции (CVE) и система оценки CVSS
- Фреймворк MITRE ATT&CK для анализа угроз
- Атаки с использованием ИИ и автоматизированное обнаружение уязвимостей
- Угрозы квантовых вычислений: атаки "собирай сейчас, расшифруй позже"
- Атаки на цепь поставок и перечень компонентов программного обеспечения (SBOM)

Тема 2: Вредоносное ПО и социальная инженерия

2.1 Вредоносное программное обеспечение

- Таксономия вредоносного ПО: вирусы, черви, трояны, программы-вымогатели, шпионское ПО, руткиты, буткиты
- Бесфайловое вредоносное ПО и техники "использования подручных средств" (living-off-the-land)
- Векторы заражения и методы распространения
- Бизнес-модели программ-вымогателей: RaaS (программы-вымогатели как услуга), двойное вымогательство
- Основы статического и динамического анализа вредоносного ПО
- Антивирусные технологии: сигнатурное, эвристическое, поведенческое обнаружение, обнаружение на базе ML
- Техники обхода песочниц (sandbox)

2.2 Социальная инженерия и человеческий фактор

- Психология атак социальной инженерии
- Варианты фишинга: целевой фишинг, уэйлинг (на руководителей), вишинг, смишинг, квишинг (фишинг через QR-код)
- Претекстинг, приманка и "хвост" (tailgating)
- Компрометация деловой переписки (BEC) и мошенничество от лица руководителей
- Фишинг-контент, генерируемый ИИ с использованием больших языковых моделей
- Deepfake-атаки: клонирование голоса, подстановка видео
- Состязательный ИИ: атаки на системы безопасности на базе ML
- Обучение осведомлённости о безопасности и симуляции фишинга

Тема 3: Управление доступом и управление учётными данными

3.1 Модели управления доступом

- Фреймворк управления идентификацией и доступом (IAM)
- Дискреционное управление доступом (DAC) и мандатное управление доступом (MAC)
- Управление доступом на основе ролей (RBAC) и современные ограничения
- Управление доступом на основе отношений (ReBAC) (Google Zanzibar)
- Управление доступом на основе атрибутов (ABAC) и на основе политик (PBAC)
- Современные модели "политика как код": OPA/Rego, AWS Cedar
- Идентификация машин: идентификация рабочих нагрузок, SPIFFE/SPIRE
- Облачный доступ: авторизация на уровне плоскости управления и плоскости данных
- Принцип минимальных привилегий и разделение обязанностей

3.2 Аутентификация и управление учётными записями

- Факторы аутентификации: знание, владение, свойственность, контекст
- Многофакторная аутентификация (MFA) и стандарт FIDO2/WebAuthn
- Современные протоколы: OIDC, OAuth 2.0, SAML (и устаревшие RADIUS/Diameter)
- Беспарольная аутентификация, ключи доступа (passkeys), защита от перебора учётных данных
- Непрерывное адаптивное доверие (CAT) и непрерывная оценка доступа (CAE)
- Управление привилегированным доступом (PAM) и доступ "точно в срок"
- Управление и администрирование идентификации (IGA)
- Обнаружение и реагирование на угрозы идентификации (ITDR)
- Архитектура нулевого доверия: сигналы и политики на основе рисков
- Децентрализованная идентификация и проверяемые учётные данные

Тема 4: Технологии безопасности и защита инфраструктуры

4.1 Технологии сетевой безопасности

- Типы межсетевых экранов: пакетный фильтр, с сохранением состояния, уровня приложений, нового поколения (NGFW)
- Межсетевые экраны веб-приложений (WAF)
- Виртуальные частные сети: IPSec, SSL/TLS VPN, OpenVPN
- WireGuard: современный VPN с использованием ChaCha20-Poly1305, Curve25519, BLAKE2
- Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS)
- Сегментация сети, VLAN и архитектура DMZ
- Микросегментация для сетей нулевого доверия
- Управление информацией и событиями безопасности (SIEM)
- Расширенное обнаружение и реагирование (XDR)
- Оркестровка, автоматизация и реагирование в сфере безопасности (SOAR)

4.2 Защита конечных точек и систем

- Обнаружение и реагирование на конечных точках (EDR)
- Обнаружение вторжений на основе хоста (HIDS) и предотвращение (HIPS)
- Укрепление операционной системы и базовые конфигурации безопасности
- Стратегии управления обновлениями и управление уязвимостями
- Безопасность мобильных устройств и управление мобильными устройствами (MDM)
- Предотвращение утечки данных (DLP)
- Сервис безопасного доступа на грани (SASE)
- Инструменты безопасности на базе ИИ/ML и поведенческая аналитика
- Белый список приложений и изоляция (sandboxing)

Тема 5: Криптография - симметричная и асимметричная

5.1 Симметричная криптография

- Принципы симметричного шифрования, перемешивание и рассеивание
- Блочные шифры и потоковые шифры
- Стандарт шифрования данных (DES) и Тройной DES (устаревшие, историческое значение)
- Усовершенствованный стандарт шифрования (AES-128, AES-192, AES-256)
- Режимы работы AES: ECB (небезопасный), CBC, CTR, OFB, CFB
- Аутентифицированное шифрование с ассоциированными данными (AEAD): AES-GCM, AES-CCM
- AES-GCM-SIV: режим, устойчивый к повторному использованию nonce
- ChaCha20: потоковый шифр как альтернатива AES
- ChaCha20-Poly1305: шифр AEAD, используемый в TLS 1.3 (RFC 8439)
- XChaCha20: вариант с расширенным nonce для крупномасштабного шифрования
- Ascon: стандарт NIST для легковесной криптографии (2023) для IoT/ встроенных систем
- Проблемы управления ключами и функции выработки ключей (HKDF, PBKDF2)

5.2 Асимметричная криптография

- Принципы криптографии с открытым ключом и математические основы
- Алгоритм RSA: генерация ключей, шифрование, подпись (RSA-2048, RSA-4096)
- Схемы дополнения RSA: OAEP для шифрования, PSS для подписей
- Криптография на эллиптических кривых (ECC): кривые NIST (P-256, P-384, P-521)
- Curve25519/X25519: высокоскоростная эллиптическая кривая для обмена ключами
- Ed25519/EdDSA: быстрые детерминистические цифровые подписи
- X448/Ed448: варианты кривых с повышенной безопасностью (224-битная безопасность)
- Обмен ключами Диффи-Хеллмана: классический DH, ECDH, X25519

- Гибридные схемы шифрования, сочетающие симметричное и асимметричное
- Постквантовая криптография (PQC) и угрозы квантовых вычислений
- Угроза алгоритма Шора для RSA/ECC, влияние алгоритма Гровера на симметричную криптографию
- Стандарты NIST PQC (FIPS 203, 204, 205 - 2024):
- ML-KEM (CRYSTALS-Kyber): инкапсуляция ключей на основе решёток
- ML-DSA (CRYSTALS-Dilithium): цифровые подписи на основе решёток
- SLH-DSA (SPHINCS+): подписи на основе хеш-функций без сохранения состояния
- Дополнительные алгоритмы PQC: FALCON, BIKE, HQC, Classic McEliece
- Криптогибкость: проектирование систем для миграции алгоритмов
- Гибридные классические/PQC схемы: X25519+ML-KEM для переходной безопасности

Тема 6: Целостность данных, цифровые подписи и PKI

6.1 Хеширование и целостность данных

- Свойства криптографических хеш-функций: устойчивость к коллизиям, устойчивость к преобразу, лавинный эффект
- Атака дня рождения и вероятность коллизий хеш-функций
- Устаревшие хеши: MD5, SHA-1 (не рекомендуются, продемонстрированы атаки коллизий)
- Семейство SHA-2: SHA-256, SHA-384, SHA-512, SHA-512/256
- SHA-3 (Keccak): SHA3-256, SHA3-512, конструкция губки (sponge)
- Функции с расширяемым выводом SHA-3 (XOF): SHAKE128, SHAKE256
- BLAKE2 (BLAKE2b, BLAKE2s): быстрее SHA-3, широко используется
- BLAKE3: параллелизируемый, единый алгоритм для хеширования/MAC/KDF/XOF
- Коды аутентификации сообщений: HMAC-SHA256, HMAC-SHA3, KMAC, Poly1305
- Проверка целостности на основе хешей и контрольные суммы
- Хеширование паролей: bcrypt, scrypt, Argon2id (функции с высоким потреблением памяти)

- Варианты Argon2 и настройка параметров (стоимость памяти, временная стоимость, параллелизм)

6.2 Цифровые подписи и сертификаты

- Схемы цифровой подписи и их свойства безопасности
- Подписи RSA: PKCS#1 v1.5 (устаревший), RSA-PSS (рекомендуемый)
- DSA и ECDSA (P-256, P-384)
- EdDSA (Ed25519, Ed448): детерминистический, быстрая проверка
- Подписи Шнорра и подписи BLS (агрегируемые, применения в блокчейне)
- Пороговые подписи и мультиподписи
- Постквантовые подписи: ML-DSA (Dilithium), SLH-DSA (SPHINCS+), FALCON
- Компоненты инфраструктуры открытых ключей (PKI) и модели доверия
- Иерархия удостоверяющих центров (CA) и кросс-сертификация
- Структура сертификатов X.509, расширения и валидация
- Жизненный цикл сертификатов: выпуск, продление, отзыв (CRL, OCSP)
- Журналы прозрачности сертификатов (CT) для обнаружения ошибочного выпуска
- Автоматизированное управление сертификатами: протокол ACME, Let's Encrypt
- Протокол TLS 1.3: улучшенное рукопожатие, обязательная прямая секретность
- Аутентификация на основе DNS (DANE) и записи TLSA
- Подписание кода, целостность программного обеспечения и безопасность цепи поставок (Sigstore, SLSA)
- Возникающие криптографические технологии: гомоморфное шифрование, MPC, доказательства с нулевым разглашением

Тема 7: Безопасность облака и защита инфраструктуры

7.1 Основы облачной безопасности

- Модели облачных сервисов: обязанности по безопасности IaaS, PaaS, SaaS
- Модель разделённой ответственности по облачным провайдерам
- Матрица контролей облака от Cloud Security Alliance (CSA)

- Управление идентификацией и доступом в облаке: политики IAM, сервисные аккаунты
- Шифрование данных при передаче (TLS) и в покое (конвертное шифрование)
- Сервисы управления ключами и ключи под управлением клиента
- Сертификации соответствия в облаке: SOC 2, ISO 27001, FedRAMP
- Безопасность в мультиоблаке: согласованные политики на AWS, Azure, GCP
- Безопасность контейнеров: укрепление Docker, сканирование образов, защита во время выполнения
- Безопасность Kubernetes: RBAC, сетевые политики, стандарты безопасности подов
- Безопасность serverless: разрешения функций, уязвимости холодного старта
- Сканирование безопасности Инфраструктуры как Кода (IaC): Terraform, CloudFormation
- Платформа защиты cloud-native приложений (CNAPP)
- Безопасность API: API-шлюзы, ограничение скорости, OAuth 2.0, защита от угроз API

7.2 Отказоустойчивость сети и инфраструктуры

- Концепции доступности: время безотказной работы, SLA, "девятки доступности"
- Шаблоны избыточности: активный-пассивный, активный-активный, N+1
- Восстановление после катастроф: RTO, RPO, горячий/тёплый/холодный резервные сайты
- Планирование непрерывности бизнеса и тестирование
- Стратегии резервного копирования: правило 3-2-1, неизменяемые резервные копии, изолированные резервные копии
- Архитектуры высокой доступности и балансировка нагрузки
- Типы DDoS-атак и смягчение: волюметрические, протокольные, уровня приложений
- Сети доставки контента (CDN) для защиты и производительности
- Реагирование на инциденты в облачных средах
- Инженерия хаоса и тестирование отказоустойчивости

Тема 8: Управление рисками, политики и соответствие

8.1 Управление рисками безопасности

- Жизненный цикл управления рисками: идентификация, оценка, обработка, мониторинг
- Методологии оценки рисков: количественные и качественные
- Идентификация и классификация активов
- Моделирование угроз: STRIDE, PASTA, деревья атак
- Инструменты оценки уязвимостей и тестирование на проникновение
- Расчёт риска: матрицы вероятность x воздействие
- Варианты обработки риска: принятие, смягчение, передача (страхование), избежание
- Аппетит к риску и толерантность к риску
- Метрики безопасности, KPI и KRI
- Фреймворк управления рисками ISO 27005
- Управление рисками третьих сторон и оценка поставщиков
- Непрерывный мониторинг рисков и автоматизированное сканирование
- Киберстрахование: типы покрытия, требования, ограничения

8.2 Политики и стандарты безопасности

- Иерархия политик безопасности: политики, стандарты, процедуры, руководства
- ISO/IEC 27001 Система менеджмента информационной безопасности (СМИБ)
- Фреймворк кибербезопасности NIST 2.0 и его шесть функций
- Контроли CIS и стандарты конфигурации безопасности
- Управление безопасностью: роли (CISO, DPO), комитеты, отчётность
- Типы аудита безопасности: внутренний, внешний, сертификационный
- Проверка соответствия и сбор доказательств
- Планирование реагирования на инциденты: подготовка, обнаружение, локализация, устранение, восстановление, извлечённые уроки
- Модели и зрелость Центра операций безопасности (SOC)
- Регламенты ЕС: Директива NIS2, DORA (финансовый сектор), Закон о киберустойчивости

- Последствия Закона ЕС об ИИ для систем безопасности
- GDPR и регулирование конфиденциальности: трансграничный трансфер данных, уведомление о нарушениях
- Отраслевое соответствие: PCI DSS, HIPAA, SOX

Соответствие лабораторных работ

Лаб	Тема	Часы
ЛР1	Анализ инцидентов безопасности, кейсы крупных нарушений	2
ЛР2	Изучение техник социальной инженерии	2
ЛР3	Конфигурация безопасной среды, укрепление	2
ЛР4	Локальные политики безопасности в Windows/Linux	2
ЛР5	Конфигурация межсетевого экрана, настройка VPN	4
ЛР6	Аутентификация, авторизация, учёт (AAA)	2
ЛР7	Инструменты шифрования файлов и данных	2
ЛР8	Реализация симметричного шифрования	2
ЛР9	Проверка целостности данных, хеширование	2
ЛР10	Реализация цифровых подписей	2
ЛР11	Идентификация информационных активов, сканирование уязвимостей	2
ЛР12	Оценка рисков, планирование обработки рисков	2
ЛР13	Разработка СМИБ для организации	2
ЛР14	Создание политик безопасности	2

Стандарты и справочники (2024-2026)

Стандарты ISO/IEC

- ISO/IEC 27001:2022 - Системы менеджмента информационной безопасности
- ISO/IEC 27002:2022 - Контроли информационной безопасности
- ISO/IEC 27005:2022 - Управление рисками информационной безопасности
- ISO/IEC 27017:2023 - Контроли облачной безопасности

- ISO/IEC 27701:2019 - Управление конфиденциальной информацией

Публикации NIST

- NIST FIPS 203 (2024) - ML-KEM (Механизм инкапсуляции ключей на основе модулярных решёток)
- NIST FIPS 204 (2024) - ML-DSA (Алгоритм цифровой подписи на основе модулярных решёток)
- NIST FIPS 205 (2024) - SLH-DSA (Алгоритм цифровой подписи на основе хеш-функций без сохранения состояния)
- NIST SP 800-207 - Архитектура нулевого доверия
- Фреймворк кибербезопасности NIST 2.0 (2024)
- NIST SP 800-63B - Руководства по цифровой идентификации (Аутентификация)

Регламенты и директивы ЕС (2024-2026)

- Директива NIS2 (ЕС 2022/2555) - Безопасность сетей и информации
- DORA (ЕС 2022/2554) - Закон о цифровой операционной устойчивости
- Закон ЕС об ИИ (2024) - Регулирование искусственного интеллекта
- Закон ЕС о киберустойчивости (2024)

Отраслевые фреймворки и отчёты

- Фреймворк MITRE ATT&CK (обновляется ежеквартально)
- Отчёт ENISA о ландшафте угроз (ежегодный)
- Cloud Security Alliance (CSA) - Матрица контролей облака v4
- OWASP Top 10 (2021, обновление ожидается в 2025)
- Контроли CIS v8.1

Криптографические стандарты

- RFC 8446 - TLS 1.3
- RFC 8439 - ChaCha20-Poly1305
- RFC 7748 - Эллиптические кривые для безопасности (X25519, X448)
- RFC 8032 - EdDSA (Ed25519, Ed448)
- RFC 9180 - Гибридное шифрование с открытым ключом (HPKE)

Структура оценивания

Компонент	Вес
Периодическая оценка 1 (Темы 1-4)	15%
Периодическая оценка 2 (Темы 5-8)	15%
Лабораторные работы	15%
Самостоятельное обучение (интеллект-карты, политики безопасности)	15%
Итоговый экзамен	40%

Курс подготовлен для Технического университета Молдовы, Факультет вычислительной техники, информатики и микроэлектроники, преподаватель Масютин Максим