Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Basics of Information Security in Financial Organizations/Основы информационной безопасности в финансовых организациях

Цель дисциплины:

Дать студентам основные понятия об организации деятельности по защите информации в финансовых организациях.

Задачи дисциплины:

- освоение студентами подходов, методов по управлению рисками информационной безопасности;

- приобретение практических навыков инвентаризации информационных активов, анализа бизнес-процессов обработки информации, определения угроз и рисков в этих бизнес-процессах;

- приобретение умения разрабатывать компенсирующие меры для рисков информационной безопасности.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- порядок организации деятельности по защите информации в финансовых организациях;

- типовые информационные инфраструктуры финансовых организаций;

- типы данных, обрабатываемых финансовыми организациями и типовые бизнес-процессы.

уметь:

- проводить инвентаризацию информационных активов;

- проводить анализ бизнес-процессов обработки информации;

- выявлять угрозы информационной безопасности;

- определять уровень риска информационной безопасности;

- разрабатывать эффективные компенсирующие меры для рисков информационной безопасности.

владеть:

- навыками освоения большого объема информации;

- навыками представления результатов деятельности подразделения информационной безопасности;

- навыками расследования инцидентов.

Темы и разделы курса:

1. Basics of information security and description of the infrastructure of financial institutions.

Информация. Свойства информации. Законодательство по информационной безопасности. Финансовые организации, их процессы и инфраструктура.

2. Analysis of business processes of financial organizations and identification of threats. Determination of the level of risks. Development of compensatory measures

Определение бизнес-процессов и их анализ, выявление угроз и расчет уровня риска. Определение наиболее эффективных компенсирующих мер и создание программы по внедрению данных мер.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Basics of Network Technologies/Основы сетевых технологий

Цель дисциплины:

изучение фундаментальных основ построения сетей передачи данных, описание роли компьютерных сетей в телекоммуникационном мире, типы и виды сетей, методы мультиплексирования, коммутация пакетов и каналов, открытые системы и модель OSI.

Задачи дисциплины:

 Предоставить студентам глубокие знания и понимание основ сетевых технологий в отношении приложений для решения задач кибербезопасности.

 Развить инженерные навыки при реализации сетевых технологий на практике.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

 Основные концепции построения локальных и глобальных сетей

 Область применимости традиционных и современных сетевых технологий

 Многообразии сетевых протоколов и стандартов

 Принципы работы различных типов коммуникационного оборудования

 Основы протокола TCP/IP, маршрутизация и IP-адресация, метод CIDR (Classless Inter-Domain Routing - бесклассовая междоменная маршрутизация)

 Представление о круге проблем, связанных с защитой данных в сетях

уметь:

 использовать преимущества и недостатки различных сетевых технологий для решения разнообразных прикладных задач

 объяснять отличия разных типов сетевых архитектур

 описывать типичные компоненты оборудования, используемые для передачи данных в сети

 описывать принципы и протоколы удаленной связи

владеть:

 навыками построения структурных схем локальных сетей и сетей, включающих глобальные связи

 применением различных моделей обмена данными в сети связи

 навыками применения изученных сетевых технологий для решения прикладных задач обработки данных в области кибербезопасности

Темы и разделы курса:

1. Introduction to network technology

Теоретические основы, принципы и систематическое введение в сетевую проблематику, что дает базовые знания, необходимые для решения прикладных задач обработки данных в области кибербезопасности..

2. The basic foundation of network technology

Изучение принципов работы сети как единого целого рассматриваются основные понятия и наиболее важные характеристики программных и аппаратных компонентов, образующих сеть: компьютеров, коммуникационной аппаратуры и операционных систем.

3. Decision Trees Algorithms

Приводятся типовые структуры вычислительных сетей. Поясняется функциональное назначение основных элементов сетевой операционной системы - сервера, редиректора и коммуникационных драйверов. Дается характеристика наиболее известных сетевых ОС. Рассматриваются принципы межсетевого взаимодействия. Приводятся основные понятия из области сетевой безопасности

4. The most popular communication protocol stacks

Рассматривается наиболее популярные стеки коммуникационных протоколов их соответствие семиуровневой модели ISO/OSI. Изучаются принципы работы коммуникационной аппаратуры различных типов: повторителей, мостов, коммутаторов, маршрутизаторов

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Critical Infrastructure Security and Management System Security/Безопасность критически важной инфраструктуры и системы управления

Цель дисциплины:

Изучение теоретических и практических основ кибербезопасности критических информационных инфраструктур, а также подготовка слушателей к дальнейшей самостоятельной работе в области защиты критических информационных инфраструктур.

Задачи дисциплины:

1. Предоставить студентам глубокие знания и понимание подходов и способов защиты объектов КИИ для решения задач кибербезопасности инфраструктуры;

2. Изучить передовые практик защиты критических информационных инфраструктур;

3. Развить практические навыки применения технологии защиты объектов КИИ от компьютерных атак.

4. Обучить методам мониторинга событий информационной безопасности и умению проводить оценки инцидентов на объектах КИИ.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- Теоретические и нормативно-правовые основы защиты КИИ;

- основные концепции построения локальных и глобальных сетей;

- область применимости традиционных и современных сетевых технологий;

- содержание и предназначение основных сетевых протоколов и стандартов;

- принципы работы различных типов коммуникационного оборудования;

- применение протокола TCP/IP, маршрутизацию и IP-адресацию;

- представление о круге проблем, связанных с защитой данных в сетях ;

- основные требования к защите КИИ;

- методы и подходы к созданию системы защиты объектов КИИ;

- технологии реагирования события информационной безопасности и правила реагирование на инциденты компьютерной безопасности;

- интеллектуальные технологии обеспечения информационной безопасности на основе по¬токовой обработки данных;

- технологии доверенной сетки устройств и безопасной системной архитектуры;

- технологии программно-конфигурируемых сетей и виртуализации сетевых функций;

- основы технологии криптографических модулей;

- основы функционирования доверенных «облачных» вычисления;

- основы создания безопасных мобильных технологии поколений 4G+ и 5G;

- основы анализа программ и аналитической верификации;

- основы квантовых технологии передачи данных.

уметь:

- использовать различные сетевые технологии для решения разных прикладных задач;

- использовать отличия разных типов сетевых архитектур;

- описывать типичные компоненты оборудования, используемые для передачи данных в сети;

- применять принципы и протоколы удаленной связи;

- планировать работы для создания открытого сегмента системы раннего обнаружения компьютерных атак на критическую инфраструктуру.

владеть:

- навыками построения структурных схем локальных сетей и сетей, включающих глобальные связи;

- навыками применения различных моделей обмена данными в сети связи;

- навыками применения сетевых технологий для решения прикладных задач обработки данных в области кибербезопасности;

- навыками работы с данными, используемыми в системах обнаружения и предотвращения компьютерных атак кии.

Темы и разделы курса:

1. National critical infrastructures

КИИ Великобритании, Европейского сообщества, Германии и Российской Федерации. Основные объекты КИИ.

Основные национальные технические стандарты по информационной инфраструктуре. Обзор исследований и разработок технологий кибербезопасности агентства DARPA США. Развитие стандартов функциональной безопасности КИИ РФ.

2. Typical compositions of information objects of critical information infrastructures

Стандартная модель взаимодействия открытых систем- OSI модель. Модель стека протоколов TCP/IP. Основные протоколы сети. Среда передачи данных и цифровое кодирование. Характеристики физической среды сетевых технологий. Основы цифрового кодирования. Иерархическая структура ЛВС. Кабельная система ЛВС. Технология коммутации в СКС. Протоколы доступа в сети ЛВС. Протоколы Ethernet.Сетевая адресация. Виртуальные ЛВС. Сети с беспроводным доступом. Обнаружение ошибок и неисправностей на канальном уровне.

Основы протоколов IPv4 и IPv6. Статистические маршруты. Таблицы маршрутизации. Протоколы управляющих сообщений Internet. Внешний межшлюзовый протокол маршрутизации.

3. Organization and management of network services at the facilities of critical information infrastructures in ensuring national and international security

Базовые сетевые службы Internet и прикладные протоколы. Классификация служб. Протоколы транспортного уровня. Система доменных имен. Протоколы: удаленного вызова процедур, терминала, передачи гипертекстовых данных, передачи файлов. Служба электронной почты. Организация сетевых файловых систем. Архитектура систем управления. Анализ потоков данных.

Анализ содержания трафика данных в сети.

4. National approaches to the protection of critical information infrastructures

Киберпространство как потенциальный источник угроз критически важных объектов инфраструктуры и инфраструктуры государства.

Основные виды угроз на объекты КИИ.

5. Security of critical information infrastructures

Стратегические цели и основные направления обеспечения информационной безопасности. Технические приемы проведения компьютерных атак на TCP-сети объектов КИИ:

Прослушивание сети. Сканирование сети. Генерация пакетов. Перехват данных. Ложные ARP-ответы. Навязывание ложного маршрутизатора. Имперсонация TCP соединения без обратной связи. Десинхронизация TCP соединения. Несанкционированное подключение к сети. Несанкционированный обмен данными. Туннелирование. Принуждение к ускоренной передаче данных. Отказ в обслуживании.

6. Methods and measures to ensure the security of critical information infrastructures

Фильтрация данных на маршрутизаторе. Защита Хоста. Защита маршрутизатора Превентивное сканирование. Потенциальные возможности защиты шифрованием. Схемы шифрования.

Уязвимость схем шифрования в беспроводных сетях Wireless LAN.

7. Objects of protection of critical information infrastructures

Защита речевой информации в цифровых телефонных сетях. Угрозы нарушения конфиденциальности информации в IP телефонии. Угрозы безопасности IP трафика в сети.

8. Vulnerabilities of critical information infrastructures

Классификация уязвимостей. Оценка угроз компьютерных атак на информационные ресурсы.

9. CII defense model

Возможные нарушители безопасности критических информационных инфраструктур. Модель угроз. Модель нарушителя. Схема категорирования объектов КИИ. Задание на выполнение требований информационной безопасности КИИ. Мероприятия по защите КИИ.

10. Certification of CII facilities for compliance with information security requirements

Порядок проведения аттестации объектов КИИ. Аккредитованные лаборатории. Требования к проведению аттестации объектов КИИ.

11. Threats to the security of critical information infrastructures

События и инциденты безопасности КИИ. Оценка угроз компьютерных атак на информационные ресурсы КИИ. Источники угроз компьютерных атак. Методика вероятностной оценки актуальных угроз безопасности информации.

12. Monitoring the security of critical information infrastructures

Проблемы обнаружения и предупреждения компьютерных атак. Системы мониторинга сообщений информационной безопасности и выявления инцидентов на объектах КИИ. Обзор методов обнаружения. Системы IPS, IDS. Классификация систем обнаружения атак. Системы SIEM. Сравнительные анализ систем SIEM. Мониторинг угроз безопасности.

13. System of detection and prevention and prevention of computer attacks of the CII object

Модели и методы упреждения компьютерной атаки на КИИ

Модификация «архитектуры фон Неймана» для выбора аппаратной платформы. Сетевые средства информационной безопасности для АСУ.

14. Principles of security of critical information infrastructures

Устойчивость объектов КИИ. Метод оценки устойчивости объектов КИИ к угрозам ИБ.

15. Security management of critical information infrastructure

Подходы к созданию системы управления ИБ объектов КИИ. Риск-ориентированный подход оценки показателей качества управления КИИ.

16. Technologies for ensuring the safety of software and equipment of information systems of objects of critical information infrastructure

Модели оценки безопасности КИИ. Основные подходы к модели КИИ. Метод Вейлет-анализа. Условие устойчивости модели прогнозирования.

17. Organization of national systems for the protection of critical information infrastructures

Обнаружение компьютерных атак с использованием нейронных сетей. Практические задачи обнаружения атак.

18. Technical methods and technologies for protecting critical information infrastructures

Рекомендации и требования регуляторов. Методика категорирования объектов КИИ. Меры защиты объектов КИИ. Межсетевой экран. VPN. Защита периметра. Сегментирование системы. Защита линий связи и коммуникаций. Мониторинг системы средствами обнаружения вторжений. Эшелонирование защиты. Идентификация и аутентификация. Антивирусная защита. Доверенная загрузка. Обновление средств защиты. Доверенное конфигурирование. Организация демилитаризованной зоны сети. Управление сетевыми потоками. Сокрытие адресов и архитектуры сети. Антиспуффинг. NAT. Раздельная фильтрация открытого IP-трафика и шифруемого.

19. Organizational methods of protecting critical information infrastructures

Создание комиссии по категорированию. Категорирование объектов КИИ. Сбор данных для категорирования объектов КИИ. Оценка критичности процессов. Формирование перечня объектов КИИ. Оценка масштабов последствий и соотнесение со значениями показателей категорий КИИ. Метод оценки категории значимости объекта КИИ. Определение объектов КИИ, связанных с критическими процессами. Акт категорирования объектов КИИ. Внесение изменений в результаты категорирования объектов.

20. Responsibility for violation of security requirements of critical information infrastructures

Права и обязанности субъектов КИИ. Ответственность должностных лиц субъекта КИИ согласно 187-ФЗ и КоАП РФ.

21. Advanced technologies for the development of critical information infrastructures

Безопасность функционирования доверенных «облачных» и «туманных» вычисления, виртуальные среды; Проблемы создания безопасных мобильных технологии поколений 4G+ и 5G;

Возможные подходы в технологии автоматизированного моделирования обстановки. Прогнозная аналитика. Системный облик BI-платформы безопасности.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Cyber Defense/Киберзащита

Цель дисциплины:

1.Привить студентам навыки разработки методов синтеза защищённых распределенных компьютерных сетей (РКС), являющихся ос-новой для построения ведомственных и корпоративных сетей.

2.Приобретение навыков анализа применимости технологий обеспечения безопасности РКС в условиях деструктивных воздействий со стороны и внутренних, и внешних проникновений, с комплексным применением криптографических алгоритмов и многоуровневой и эшелонированной защитой информации.

Задачи дисциплины:

Формирование у студентов практических навыков применения изученных методов и схем в условиях комплекса деструктивных воздействий.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

Овладение студентами навыков создания подходов, методов и моделей анализа динамики процессов противостояния комплексу деструктивных воздействий различного характера на объекты риска РКС.

уметь:

Студенты приобретут практические навыки разработки и применения моделей и методов с комплексным применением криптографических алгоритмов и многоуровневой и эшелонированной защитой информации в РКС.

владеть:

Приобретение умения создания технологий синтеза алгоритмического и программно-аппаратного обеспечения, обеспечивающих необходимый уровень ИБ в РКС.

Темы и разделы курса:

1. Methodology for system analysis of the risk of an attack on DCN objects. The concept of separation of information security solutions.

Вариант формирования многоконтурной зональной системы защиты компьютерной сети. Использование межсетевых экранов (МЭ), систем обнаружения атак и протоколов, обеспечивающих аутентификацию, шифрование и установление сеансов защищенного информационного обмена на верхних уровнях ЭМВОС.

Примеры программирования протоколов аутентификации в среде Matlab.

2. Fundamentals of building a public key management infrastructure.

Архитектура криптографической подсистемы Windows, алгоритм электронной подписи, алгоритм обмена сеансовыми ключами симметричного шифрования, схема генерации сеансового ключа из хеш-значения, модуль открытого ключа.

Примеры программирования алгоритмов шифрования в среде Matlab.

3. General provisions on certification and certificates.

Сертификат ключа. Сертификаты оконечных пользователей. Сертификаты издателей.

4. Complex application of cryptographic algorithms and systems in computer networks. Cryptographic interface (CryptoaAPI).

Задачи и процедуры управления открытыми ключами. Жизненный цикл криптографического ключа. Примеры программирования стадий и фаз жизненного цикла криптографических ключей в Матлаб.

5. Sources of information about the attacks.

Журнал регистрации операционной системы (журналы системных событий, приложений и безопасности). Журнал регистрации коммуникационного оборудования. Журнал регистрации межсетевого экрана. Примеры программ анализа журнальных событий в Matlab.

6. Hiding the source and fact of the attack.

Подмена адреса источника атаки. Создание фальшивых пакетов. Использование чужих компьютеров для атаки. Фрагментация атаки. Примеры программирования фальшивых пакетов в Matlab.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Fundamentals of Intelligent Cyber Security Management/Основы систем управления информационной безопасностью

Цель дисциплины:

1.Развивать у студентов способность оценивать текущую ситуацию в области безопасности, включая общее состояние распространенных уязвимостей и вероятные последствия сбоев в системе безопасности;

2.Развивать у студентов критическое оценивание сильных и слабых сторон общих моделей кибербезопасности, включая триаду ЦРУ.

Задачи дисциплины:

1. Развивать у студентов оценку взаимосвязей между элементами системы безопасности, включая аппаратное обеспечение, программное обеспечение, политику и людей.

2. Развивать у студентов понимание того, как организации управляют проблемой кибербезопасности, проектируя и разрабатывая решения по кибербезопасности для организации, компонентных устройств, формируя интегрирующие технологии для решения вопросов кибербезопасности. Существующие методы, применяемые для получения эффективных решений кибербезопасности.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

1. Студенты смогут глубоко изучить широкий круг вопросов кибербезопасности и принципов, лежащих в основе теории рисков.

2.Студенты изучат концептуальные аспекты внедрения решений кибербезопасности в организации.

уметь:

студенты смогут оценить риск, связанный с ландшафтом угроз киберпространства.

владеть:

1.Студенты смогут изучить анатомию кибератаки, и это поможет им в будущем разрабатывать новые решения.

2.Студенты смогут изучить технологию защиты от киберугроз и разобраться, как она работает.

Темы и разделы курса:

1. The concept of risk cyber-attacks

Постановка задачи оценки риска атаки. Структура риска. Инварианты, функции защиты. Примеры программирования функций защиты с помощью нейронных сетей в Матлаб.

2. Logical-probabilistic approach to risk assessment

ЛВ-полиномы. Сравнительный анализ защищенности объекта риска. Примеры программирования ЛВ-полиномов в Матлаб.

3. Destabilizing factors and security functions

Полнота и содержательная природа системы функций защиты для любой атаки. Причинно-следственная диаграмма функций защиты. Примеры программирования причинно-следственной диаграммы функций защиты объекта риска в Матлаб.

4. Criteria for the security of the cyber-attack object. Risk Assessment

Условие защищенности объекта риска. Оценка защищенности объекта риска. Примеры программирования алгоритма оценки защищенности объекта риска в Матлаб.

5. Risks evaluation

Уточнённое условие защищённости объекта риска. Новые градации функций защиты. Примеры программирования новых градаций функций защиты объекта риска в Матлаб.

6. Enterprise Role and Structure

Платформа как сервис: современное состояние, возможности. Инструменты отслеживания кибератаки. Примеры программирования инструментов отслеживания кибератаки в Матлаб.

7. Security Metrics and Measurements

Оценка риска DDoS-атаки. Оценка риска спама. Примеры программирования оценки риска конкретной кибератаки в Матлаб.

8. Cyber Security Anatomy

Модели безопасных частных и публичных облаков. Требования к безопасным Гипервизорам в облачных технологиях. Примеры программирования сенсоров фиксации вредоносного трафика в публичных облаках в Матлаб.

9. Cyber Security Controls

Модели безопасного управления облачными системами. Примеры программирования алгоритмов анализа событий в управляющих процедурах облачных систем в Матлаб.

10. Testing and Validation of Security Devices

Отражение кибератак. Обеспечение гарантированного качества обслуживания (QoS) в облачных инфраструктурах. Информационная безопасность как качество сервиса. Примеры программирования алгоритмов отражения кибератак в облачных инфраструктурах в Матлаб.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

History, Philosophy and Methodology of Natural Science/История, философия и методология естествознания

Цель дисциплины:

приобщить студентов к историческому опыту мировой философской мысли, дать ясное представление об основных этапах, направлениях и проблемах истории и философии науки, способствовать формированию навыков работы с предельными вопросами, связанными с границами и основаниями различных наук и научной рациональности, овладению принципами рационального философского подхода к процессам и тенденциям развития современной науки.

Задачи дисциплины:

– систематизированное изучение философских и методологических проблем естествознания с учетом историко-философского контекста и современного состояния науки;

– приобретение студентами теоретических представлений о многообразии форм человеческого опыта и знания, природе мышления, соотношении истины и заблуждения;

— понимание роль науки в развитии цивилизации, соотношение науки и техники и связанные с ними современные социальные и этические проблемы, умение различать исторические типы научной рациональности, знать структуру, формы и методы научного познания в их историческом генезисе, современные философские модели научного знания;

— знакомство с основными научными школами, направлениями, концепциями, с ролью новейших информационных технологий в мире современной культуры и в области гуманитарных и естественных наук;

— понимание смысла соотношения биологического и социального в человеке, отношения человека к природе, дискуссий о характере изменений, происходящих с человеком и человечеством на рубеже третьего тысячелетия;

— знание и понимание диалектики формирования личности, ее свободы и ответственности, своеобразия интеллектуального, нравственного и эстетического опыта разных исторических эпох.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

– структуру естественных и социо-гуманитарных наук, специфику их методологического аппарата;

– соотношение принципов и гипотез в построении научных систем и теорий;

– основы современной научной картины мира, базовые принципы научного познания и ключевые направления междисциплинарных исследований;

– концепции развития науки и разные подходы к проблеме когнитивного статуса научного знания;

– проблему материи и движения;

– понятия энергии и энтропии;

– проблемы пространства–времени;

– современные проблемы физики, химии, математики, биологии, экологии;

– великие научные открытия XX и XXI веков;

– ключевые события истории развития науки с древнейших времён до наших дней;

– взаимосвязь мировоззрения и науки;

– проблему формирования мировоззрения;

– систему интердисциплинарных отношений в науке, проблему редукционизма в науке;

– теоретические модели фундаментальных процессов и явлений в физике и ее приложениях к естественным наукам;

– о Вселенной в целом как физическом объекте и ее эволюции;

– о соотношении порядка и беспорядка в природе, о проблемах нелинейных процессов и самоорганизующихся систем;

– динамические и статистические закономерности в природе;

– о роли вероятностных описаний в научной картине мира;

– принципы симметрии и законы сохранения;

– новейшие открытия естествознания для создания технических устройств;

– особенности биологической формы организации материи, принципы воспроизводства и развития живых систем;

– о биосфере и направлении ее эволюции.

уметь:

- эффективно использовать на практике теоретические компоненты науки: понятия, суждения, умозаключения, гипотезы, доказательства, законы;

– применять методологию естествознания при организации конкретных исследований;

– дать панораму наиболее универсальных методов и законов современного естествознания.

владеть:

– научной методологией как исходным принципом познания объективного мира;

– принципами выбора адекватной методологии исследования конкретных научных проблем;

– системным анализом;

– знанием научной картины мира;

– понятийным и методологическим аппаратом междисциплинарных подходов в науке.

Темы и разделы курса:

1. The formation of science and philosophy in the West and in the East.

Проблема возникновения науки в древности. Рецептурный и прикладной характер знания на Древнем Востоке. Рождение философии. Научные программы Платона, Аристотеля и Демокрита. Зарождение античной науки: математика, физика, астрономия и биология. Проблема социальной организации античной науки. «Мусический» культ и научно-философские школы. Александрийский Мусейон и дальнейшее развитие эллинистической науки. Наука Древнего Рима. Арабская средневековая наука.

Наука в Европе в Средние века. Христианство и наука Спор веры и разума. Переосмысление античного наследия. Средневековый эмпиризм. Николай Кузанский и понятие бесконечности. Мировоззренческий поворот эпохи Возрождения.

2. The main periods and basic forms of the development of science

Возникновение науки Нового времени: основные концепции и ключевые персоналии. Ключевые исследовательские программы новоевропейской науки. Триумф нью-тоновской физики и становление математического естествознания. Центральные теоре-тические постулаты и методы классического естествознания.

3. Rationalistic and empiricist traditions in the philosophy of the Modern Times

Рационалистическое направление: метод дедукции и понятие интеллектуальной интуиции в философии Декарта и Спинозы. Декартовский пробабилизм. Теория врожденных идей. Учение Лейбница об „истинах факта“ и „истинах разума“, о видах знания, об анализе и синтезе. Рационалистическая трактовка тезиса о соответствии бытия и мыш-ления.

Традиция английского эмпиризма: бэконовское учение об опыте, о роли индукции, об „идолах“ познания. Локковская модель научного познания. Тезис Беркли: быть — зна-чит быть воспринимаемым. Юмовский скептицизм и психологизм, критика понятия при-чинности.

4. Kant’s solution of the problem of knowledge

Постановка вопроса о возможности познания. Пространство и время как формы чувственности. Конструирование предметности в процессе познания. Разум как

законодатель. Специфика кантовского понимания мышления. Критика возможности сверхчувственного познания. Понятие „вещи в себе“. Антиномии разума.

5. The approach to knowledge in neokantian philosophy

Марбургская и баденская школы неокантианства. Неокантианская разработка теории познания. Деление наук на номотетические и идиографические. Проблема ценностей в Баденской школе.

6. Positivism

Первый и второй позитивизм XIX в. Аналитическая философия Б. Рассела и Л. Витгенштейна. Логический позитивизм и «лингвистический поворот». Постпозитивизм К. Поппера, Т. Куна и И. Лакатоса.

7. Critique of positivism from the point of view of logic. Critical rationalism of Karl Popper

Логическая критика позитивизма К. Поппером: проблемы индукции и демаркации; принцип фальсификации; отношение к истине. Концепция роста науки К. Поппера: фаллибилизм и теория правдоподобия. Развитие современной космологии и физики элементарных частиц.

8. Historical criticism of positivism. Historical approach in the philosophy of science.

Существуют ли “решающие эксперименты”? Тезис о “несоизмеримости теорий”. Куновская модель развития науки: научное сообщество и научная парадигма, “нормальная” и “аномальная” фазы в истории науки. Модель исследовательских программ И. Лакатоса: “жесткое ядро” и “защитный пояс гипотез”; “прогрессивный сдвиг проблем” как критерий отброса исследовательских программ. Исторический релятивизм П. Фейерабенда. Спор реализма и антиреализма в современной философии науки. Социологизация современной философии науки. Спор о модели «внешней» и «внутренней» истории Лакатоса. Место лаборатории в науке. Взаимоотношения науки и техники во второй половине XX – начале XXI в.

9. The structure of scientific knowledge

Место математики и измерений. Место оснований и теорий явлений. Место методологических принципов.

10. Philosophical problems of natural sciences

Понятие динамических и статистических закономерностей и вероятности как объективной характеристики природных объектов. Место принципов симметрии и законов сохранения.

Синергетика, самоорганизация и соотношение порядка и беспорядка. Модель глобального эволюционизма.

Особенности наук о живом. Вопрос о редукции биологии и химии к физике. Противоречия между природой и человеком в наши дни. Глобальные проблемы современной цивилизации, возможности экологической катастрофы. Биосфера, ноосфера, экология и проблема устойчивого развития.

Междисциплинарные подходы в современной науке.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Information Security in the Cloud/Информационная безопасность в облаке

Цель дисциплины:

Дать студентам знания и понятия о кибербезопасности облака.

Изучить и научиться применять классические методы безопасности к сегодняшним проблемам облачной безопасности.

Задачи дисциплины:

-освоение студентами подходов, методов поиска уязвимости облачной безопасности, используя стандартные систематические методы.

- приобретение практических навыков в создании собственных реализаций облачной инфраструктуры и веб-сервисов, разрабатывать для них решения безопасности.

- приобретение умения использовать классические концепции безопасности, такие как минимальные привилегии и разделение обязанностей, а также более технические методы криптографии и контроля доступа.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- как защитить сеть, инфраструктуру, данные и приложения в облаке

- как создать и защитить частную сеть в облаке

- способы мониторинга, регистрации и аудита в облаке

- определить риски на основе моделей развертывания и моделей предоставления услуг различных продуктов, предлагаемых поставщиками облачных услуг (CSP).

- как обнаруживать и реагировать на инциденты безопасности в облаке и принимать соответствующие меры.

уметь:

- создавать учетные записи и пользуйтесь услугами любого из ведущих CSP

- обеспечивать безопасный доступ к консолям, используемым для доступа к средам CSP.

- оценивать службы ведения журналов различных CSP и использовать эти журналы для обеспечения необходимой отчетности для событий, происходящих в облачной среде.

- внедрять, настройка и безопасность аутентификации SSH на основе сертификатов для виртуальных машин, запущенных в облаке.

- конфигурировать интерфейс командной строки и должным образом защитить ключи доступа, чтобы минимизировать риск взлома учетных данных.

- использовать базовые сценарии Bash и Python для автоматизации задач в облаке.

- внедрять элементы управления сетевой безопасностью, встроенные как в AWS, так и в Azure.

- использовать архитектурный шаблон для автоматического создания и предоставления исправленных и защищенных образов виртуальных машин для нескольких учетных записей AWS.

- использовать лучшие практики AWS и Azure для обеспечения безопасности.

- развернуть полную среду «инфраструктура как код» для нескольких облачных провайдеров.

владеть:

- инструментами мониторинга и аудита облачных ресурсов для непрерывной безопасности в облаке

- методами использования управляемых сервисов безопасности AWS для автоматизации безопасности,

- инструментами безопасности приложений и моделирование угроз для оценки безопасности облачных веб-приложений.

- автоматическим созданием и предоставлением исправленных и защищенных образов виртуальных машин.

Темы и разделы курса:

1. Accessing the web management consoles of cloud infrastructure.

Доступ к веб-консолям AWS, Azure, GCP и запуск виртуальных машин в выбранной среде. Веб-консоли. Практические задания по запуску виртуальных машин в AWS и Azure. VPC. Обеспечение защищенного образа.

2. AWS Security Center and Azure

Безопасность предложения «программное обеспечение как услуга». Платформа как услуга AWS и Azure.

3. Hardening and securing cloud environments and applications.

Применение инструментов и сервисов безопасности. Обеспечение доступа к консоли. Усиление защиты, исправление и защита образов виртуальных машин, включая SSH.

4. Command line interface (CLI)

Применение простых скрипты для автоматизации работы

5. Logs and security services to detect malware on a cloud virtual machine.

Утечка секретов в коде, развернутом в облаке. Получение и анализ облачного журнала. Инструмент с открытым исходным кодом для аудита учетной записи AWS

6. Government Clouds.

Рассмотрение основных проблем применения облачных технологий в правительственных учреждения, отвечающих государственным требованиям безопасности.

7. Implementation enterprise governance strategies

Контроль доступа на основе ролей, политики Azure и блокировки ресурсов.

8. Azure AD infrastructure, users, groups, and multi-factor authentication.

Защита идентификации Azure AD, политики рисков, условный доступ и проверки доступа. Управление привилегированной идентификацией Azure AD, роли Azure AD и ресурсы Azure. Azure AD Connect, включая методы аутентификации и локальную синхронизацию каталогов.

9. Perimeter security strategies,

Стратегии сетевой безопасности, группы безопасности сети и группы безопасности приложений.Стратегии безопасности хоста, защита конечных точек, управление удаленным доступом, управление обновлениями и шифрование диска.

10. Container security strategies

Экземпляры контейнеров Azure, реестр контейнеров Azure и Azure Kubernetes. Хранилище ключей Azure, включая сертификаты, ключи и секреты. Стратегии безопасности приложений, регистрация приложений, управляемые удостоверения и конечные точки служб.

11. Storage security strategies.

Подписи общего доступа, политики хранения больших двоичных объектов и проверку подлинности файлов Azure. Стратегии безопасности баз данных, аутентификация, классификация данных, динамическое маскирование данных и всегда зашифрованные

12. Azure Security Center.

Политики, рекомендации и своевременный доступ к виртуальной машине. Azure Monitor, подключенные источники, аналитика журналов и оповещения.

13. Azure Data Lake enterprise-class security features.

Шифрование транспортного уровня с HTTPS. Расширенная защита от угроз. Контроль доступа к сети. Центр безопасности Azure. Key Vault.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Intelligent Technology for Information Security/Интеллектуальные технологии в информационной безопасности

Цель дисциплины:

1.Привить студентам навыки разработки методов генерации гипотез о риск-моделях веб-атак в высокодинамичных веб-системах.

2.Приобретение навыков анализа применимости нейро-нечеткого и байесовского подходов (объединение априорных и наблюдаемых данных) к синтезу интеллектуальных систем принятия решений по инцидентам информационной безопасности и разработке механизмов веб-программирования в Hadoop.

Задачи дисциплины:

Формирование у студентов практических навыков применения изученных методов и схем и аргументации при принятии решений по противодействию веб-атакам в условиях множественного выбора.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

Овладение студентами навыков создания подходов, методов и моделей анализа динамики процессов информационного противоборства различного характера

уметь:

Студенты приобретут практические навыки применения риск-моделей и методов, учитывающих многомерность данных для идентификации параметров веб-атак, а также извлечения знаний в информационном противоборстве

владеть:

Приобретение умения интерпретировать полученные результаты для построения сценариев, прогнозов, принятия решений с целью противодействия веб-инъекционным атакам и объяснения характера возникающих в информационно-коммуникационных системах инцидентов информационной безопасности.

Темы и разделы курса:

1. The methodology of a systematic risk analysis of Infocommunications.

Исторические сведения о становлении научной дисциплины – системный анализ рисков инфокоммуникаций. Основные понятия информационной войны в Интернете.

Примеры программирования информационной войны в среде Matlab.

2. Examples of information warfare. The formal statement of the research problem.

Характеристика особенностей сложных систем: уникальность, слабая структурированность теоретических и фактических знаний о системах, композиционный характер

(мультипротокольность), неоднородность подсистем и элементов, случайность и неопределенность факторов, действующих в системах, многокритериальность процессов оценки (игры с конфликтующими интересами), большая размерность, непрерывность переменных и немонотонность в динамике, субъективность в описании сложных систем. Интегральные характеристики. Общие свойства.

Примеры программирования информационных мультипротокольных систем в среде Matlab.

3. Overviev: globalism and the case of Azia and Africa blocs.

Пределы применимости вероятностных подходов оценки риска атак. Полнота, инвариантность случайной диаграммы риска атаки. Примеры программирования значения риска объекта риска в Matlab.

4. Criteria for the security of the cyber-attack object. Risk Assessment.

Условие защищенности объекта риска. Оценка защищенности объекта риска. Примеры программирования алгоритма оценки защищенности объекта риска в Матлаб.

5. Risks evaluation.

Уточнённое условие защищённости объекта риска. Новые градации функций защиты. Примеры программирования новых градаций функций защиты объекта риска в Матлаб.

6. Risks analysis methods and mathematical techniques used in intelligent systems information security.

Оценка экстремальных рисков. Метрики для оценки рисков. Максимизация, экстремальные задачи, мультиэкстремальные задачи.

7. Modeling web-based attacks

Класс моделей. Процесс идентификации в системно-ориентированном моделировании в облаке. Примеры программирования бот-атак в Matlab, Hadoop.

8. Premodernity analysis: goal setting.

Моделирование этапов, постановка целей, построение информационной структурно-функциональной среды, построение логической среды СУБД. верификация. Примеры программирования логических сред СУБД, в среде MATLAB, Hadoop.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Machine Learning Techniques for Cybersecurity/Методы машинного обучения применительно к кибербезопасности

Цель дисциплины:

Изучить методы машинного обучения в приложении для решения задач кибербезопасности, а также подготовить студентов к дальнейшей самостоятельной работе, используя практические навыки алгоритмов машинного обучения.

Задачи дисциплины:

1. Предоставить студентам глубокие знания и понимание методов машинного обучения в отношении приложений для решения задач кибербезопасности;

2. Развить практические навыки использования алгоритмов машинного обучения.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

теоретические основы и принципы машинного обучения;

классы моделей и метрики качества;

подходы к подготовке и предобработке данных;

основные подходы генерации и выбора признаков;

основные понятия, применяемые при описании алгоритмов обучения;

основные понятия для описания деревьев решений, операции с деревьями;

многослойный персептрон, сверточные, рекуррентные и генеративно-состязательные сети;

методы расширения набора данных;

особенности применения предобученных моделей (перенос обучения);

алгоритмы с адаптивными темпами обучения;

меры расстояний, иерархические и плоские, четкие и нечеткие алгоритмы кластеризации.

уметь:

использовать алгоритмы машинного обучения для решения задач классификации;

использовать алгоритмы машинного обучения для решения задач кластеризации;

использовать алгоритмы машинного обучения для прогнозирования временных рядов;

использовать нейросетевые алгоритмы для обнаружения вторжений;

использовать деревья решений;

использовать алгоритмы обнаружения

владеть:

навыками работы с данными, используемыми в системах обнаружения вторжений.

навыками применения изученных алгоритмов машинного обучения для решения прикладных задач обработки данных в области кибербезопасности.

Темы и разделы курса:

1. Introduction to Learning Systems.

Теоретические основы и принципы машинного обучения, классы моделей (линейные, логические, нейросетевые), метрики качества, подходы к подготовке данных, предобработка данных, генерация и выбор признаков, разведочный анализ данных, методы интерпретации данных и моделей.

2. Machine Learning Theory

Алгоритмы обучения (задача, показатель эффективности, неконтролируемый / контролируемый опыт), пропускная способность, переоценка и недооценка, регуляризация, гиперпараметры и наборы для проверки, оптимизация, перекрестная проверка, оценки, смещение и дисперсия, оценка максимального правдоподобия, байесовская статистика, контролируемые алгоритмы обучения, неконтролируемое обучение, алгоритмы стохастического градиентного спуска.

3. Decision Trees Algorithms

Сложность выборки, деревья классификации и регрессии, индекс Джини, алгоритм ID3, функция энтропии и получение информации, автоматическое обнаружение взаимодействия по хи-квадрату, реализации меры усиления, обрезка, правила расщепления на основе порогов, повышение градиентного дерева, алгоритм AdaBoost, случайные леса.

4. Deep Learning (Practice, Programming).

Многослойный персептрон. Сверточные нейронные сети. Рекуррентные нейронные сети. Генеративно-состязательные сети. Функции активации. Функционал оптимизации. Функция потерь. Проблема переобучения и обобщающая способность нейросети. Обратное распространение ошибки. Вычислительный граф. Проблема затухающих градиентов и нормализация. Регуляризация. Расширение набора данных. Перенос обучения (предобученные модели). Шумоустойчивость. Стохастический градиентный спуск. Стратегии инициализации параметров. Алгоритмы с адаптивными темпами обучения

AdaGrad, RMSProp, Adam. Алгоритмы автоматической оптимизации гиперпараметров. Поиск по сетке и случайный.

5. Machine Learning for Classification Tasks.

Практические задачи классификации в области кибербезопасности. Классификация спам-рассылки. Классификация интернет ресурсов. Классификация зловредных программ. Классификация сетевых атак.

6. Machine Learning for Clustering Tasks

Практические задачи кластеризации. Понятие кластеризации, Меры расстояний, Иерархические и плоские алгоритмы, Четкие и нечеткие алгоритмы, Объединение кластеров, Алгоритм DBSCAN

7. Machine Learning for Time Series Prediction.

Модели экспоненциального сглаживания, Модели скользящего среднего, Трендовые модели, Bootstrapping, Авторегрессионные модели, ARMA, ARIMA, GARCH, Адаптивная авторегрессия, Прогнозирование плотности распределения

8. Intrusion Detection Using Neural Networks.

Практические задачи обнаружения вторжений.

9. Anomaly Detection

Практические задачи обнаружения аномалий. детектирование выбросов, детектирование новизны, Статистические тесты, Итерационные методы, Метрические методы, Методы подмены задачи, Изолирующий лес, Ансамбли алгоритмов

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Neural Network Based Intrusion Detection System/Нейросетевые системы обнаружения компьютерных атак

Цель дисциплины:

Предоставить студентам навыки разработки методов для генерации гипотез о моделях риска веб-атак в высокодинамичных веб-системах.

Задачи дисциплины:

1. Формирование практических навыков применения изученных методов и схем рассуждений при принятии решений о противодействии веб-атакам в условиях множественного выбора.

2. Приобретение навыков анализа применимости нейронечеткого и байесовского подходов (объединение априорных и наблюдаемых данных) к синтезу интеллектуальных систем принятия решений по инцидентам информационной безопасности и разработке механизмов веб-программирования в Hadoop.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

Студенты осваивают подходы, методы и модели для анализа динамики процессов информационного противодействия различного характера.

уметь:

Приобретать практические навыки применения моделей риска и методов системного анализа с точки зрения многомерности данных для определения параметров сетевых атак и извлечения знаний в области информационного противодействияОптимизировать код, используя возможности и методы системного анализа с точки зрения многомерности данных для определения параметров веб-атак.

владеть:

- умениями интерпретировать полученные результаты для построения сценариев, прогнозов, принятия решений с целью противодействия атакам веб-инъекций и объяснять

характер возникающих в информационно-коммуникационных системах инцидентов информационной безопасности.

Темы и разделы курса:

1. Own risk analysis methods and mathematical techniques used in intelligent systems information security

Оценка экстремальных рисков. Метрики для оценки риска. Традиционные методы системного анализа сложных систем: матрица, систематизации, граф, стохастические модели. Максимизация, экстремальные задачи, многоэкстремальные задачи. Методы поиска локальных и глобальных экстремумов функций. Линейное программирование - постановка задачи. Алгоритм симплекс-метода. Понятие о методе эллипсоидов. Алгоритм - это внутренняя точка. Линеаризация задач математического программирования. Другие методы системного анализа: 1) кластерный анализ; 2) минимаксная, многокритериальная оптимизация; 3) исследование операций; 4) процессы принятия решений, поддержка принятия решений (dss), критерии сравнения и выбора, сравнение альтернатив; 5) математическая теория планирования эксперимента; 6) задача сетевого планирования и анализа графического дизайна.

2. Practical examples of the applicability of the models.

Практические примеры применимости моделей.

3. Modeling web-based attacks

Основные задачи и методы. Системное моделирование атак ботнета. Компоненты системного моделирования: математическое моделирование, компьютерное моделирование, информационное моделирование, моделирование принятия решений, имитационное моделирование, оптимизационные модели, вероятностное (стохастическое) моделирование. Системно-интегрированное моделирование. Принципы. Класс моделей. Процесс идентификации в системно-интегрированном моделировании в облаке. Среда веб-программирования, Hadoop.

4. The use of ITU experience.

Практическое использование опыта ITU.

5. Premodernity analysis: goal setting.

Этапы моделирования: постановка целей, построение информационной структурно-функциональной среды, построение логической среды СУБД, верификация. Цели и задачи в зависимости от назначения модели: общая модель, глобальная и локальная модель. Точность, временной горизонт, объекты, функциональная связность, описания видов (логические и вероятностные уравнения, нейронечеткий дизайн принятия решений по инцидентам безопасности).

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Russian as a Foreign Language/Русский язык как иностранный

Цель дисциплины:

Целью дисциплины «Русский язык как иностранный (уровень А2)» является формирование межкультурной профессионально ориентированной коммуникативной компетенции на начальном уровне А2 (по Общеевропейской шкале уровней владения иностранными языками) для решения социально-коммуникативных задач в различных областях бытовой, культурной, профессиональной и научной деятельности на русском языке, а также для дальнейшего самообразования

Задачи дисциплины:

Задачи формирования межкультурной профессионально ориентированной коммуникативной компетенции состоят в последовательном овладении студентами совокупностью субкомпетенций, основными из которых являются:

– лингвистическая компетенция, т.е. умение адекватно воспринимать и корректно использовать языковые единицы на основе знаний о фонологических, грамматических, лексических, стилистических особенностях изучаемого языка;

– социолингвистическая компетенция, т.е. умение адекватно использовать реалии, фоновые знания, ситуативно обусловленные формы общения;

– социокультурная компетенция, т.е. умение учитывать в общении речевые и поведенческие модели, принятые в соответствующей культуре;

– социальная компетенция, т.е. умение взаимодействовать с партнерами по общению, вступать в контакт и поддерживать его, владея необходимыми стратегиями;

– стратегическая компетенция, т.е. умение применять разные стратегии для поддержания успешного взаимодействия при устном / письменном общении;

– дискурсивная компетенция, т.е. умение понимать и порождать иноязычный дискурс с учетом культурно обусловленных различий;

– общая компетенция, включающая наряду со знаниями о стране и мире, об особенностях языковой системы также и способность расширять и совершенствовать собственную картину мира, ориентироваться в медийных источниках информации;

– межкультурная компетенция, т.е. способность достичь взаимопонимания в межкультурных контактах, используя весь арсенал умений для реализации коммуникативного намерения;

– компенсаторная компетенция, т.е. способность избежать недопонимания, преодолеть коммуникативный барьер за счет использования известных речевых и метаязыковых средств.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- Основные факты, реалии, имена, достопримечательности, традиции России;
- некоторые достижения, открытия, события из области русской науки, культуры, политики, социальной жизни;
- основные фонетические, лексико-грамматические, стилистические особенности русского языка и его отличие от родного языка;
- основные различия письменной и устной речи.

уметь:

- Порождать адекватные устные и письменные тексты в условиях конкретной ситуации общения;
- реализовывать коммуникативное намерение с целью воздействия на партнера по общению;
- адекватно понимать и интерпретировать смысл и намерение автора при восприятии устных и письменных аутентичных текстов;
- выявлять сходство и различия в системах родного и иностранного языков;
- проявлять толерантность, эмпатию, открытость и дружелюбие при общении с представителями другой культуры.

владеть:

- Межкультурной профессионально ориентированной коммуникативной компетенцией в разных видах речевой деятельности на уровне А2;
- социокультурной компетенцией для успешного взаимопонимания в условиях общения с представителями другой культуры;
- различными коммуникативными стратегиями;
- учебными стратегиями для организации своей учебной деятельности;
- стратегиями рефлексии и самооценки в целях самосовершенствования личных качеств и достижений;
- разными приемами запоминания и структурирования усваиваемого материала;
- интернет-технологиями для выбора оптимального режима получения информации.

Темы и разделы курса:

1. My World

Коммуникативные задачи. Рассказать о своей повседневной деятельности. Говорить о времени. Назначать встречу. Рассказать о своей семье. Заполнять форму регистрации. Спросить email.

Лексика. Глаголы для описания повседневной деятельности. Поздно – рано. Время. Время суток. Числа 10 – 100. Мероприятия. Семья. Форма регистрации.

Грамматика. Глаголы (первое спряжение). Время: 1 час, 2 - 4 часа, 5 – 20 часов. Время суток при ответе на вопрос «Когда». Притяжательные местоимения (мужской и женский род) мой / моя, твой / твоя и т.д.

Фонетика. Произношение т, ть. Произношение [ц], безударные «я», «е». Произношение [ж], [ш], оглушение «ж» на конце слов.

2. Our Lesson

Коммуникативные задачи. Понимать инструкции преподавателя на уроке и задания в учебнике. Спрашивать о наличии предмета, используя конструкцию «у вас есть?». Указывать на предмет. Назначать встречу. Рассказывать о своих планах на неделе.

Лексика. Императив (формальный вариант и мн. ч.) – читайте, слушайте и т.д. Личные вещи. Числа 100 – 1000. У меня + событие. Множественное число. Дни недели (когда?).

Грамматика. Глаголы, обозначающие деятельность на уроке (читать, писать и др.). Наречия. Конструкция «у меня есть / нет». Род имен существительных. Дни недели. Мероприятия.

Фонетика. Произношение «о» в безударной позиции. [ж], [ш]. Оглушение [ж] на конце слов. Произношение у,г.

3. In the City

Коммуникативные задачи. Рассказывать о своем городе. Спрашивать дорогу. Понимать вывески в городе. Говорить о принадлежности предметов. Просить счет в ресторане. Делать заказ в ресторане. Объяснять, на какой неделе (этой, прошлой, следующей). Рассказывать о том, где они были (какие места посетили).

Лексика. Объекты города (парки, рестораны, музеи и т.д.). «К сожалению». Слова: меню, счёт, билет. Некоторые названия еды и напитков. «На этой неделе / на прошлой неделе / на следующей неделе».

Грамматика. Окончания прилагательных. Притяжательные местоимения. Предложный падеж при выражении локации. Глагол «быть» в прошедшем времени.

Фонетика. Оглушение «д» на конце слов и перед глухими согласными. Отработка фразы «к сожалению». Слова, где «ч» произносится как [ш].

4. My Home

Коммуникативные задачи. Говорить о доме, рассказать, какая мебель там есть, что люди делают обычно дома. Вызвать мастера и рассказать о проблеме в доме. Объяснять, где что находится. Выражать испуг или удивление при помощи слова «Ой!». Демонстрировать удивление. Говорить о вкусах и предпочтениях, о стиле жизни.

Лексика. Комнаты. Мебель. Глаголы (видеть, ненавидеть, смотреть, хотеть, спать). Части дома (стена, пол, потолок, угол) и вокруг дома (сад, лес). Занятия в свободное время.

Грамматика. Глаголы-исключения. Существительные среднего рода во множественном числе. Исключения во множественном числе. Существительные-исключения в предложном падеже (на полу, в саду, и др.). Прошедшее время. Существительные в винительном падеже при выражении прямого объекта.

Фонетика: Произношение названий комнат. Произношение слов со сменой ударения в предложном падеже (в лесу, на полу и т.д.). Произношение [х]. Удивляться при помощи слова «ух ты!».

5. Tasty Food

Коммуникативные задачи. Рассказывать о своем режиме питания. Покупать фрукты и овощи в магазине. Заказывать еду в ресторане. Понимать официанта. Вносить уточнения в заказ. Общаться за ужином; спросить рецепт. Восхищаться или критиковать разные вещи. Приглашать друзей куда-либо и принимать их приглашения.

Лексика. Продукты. Слова: «нравится», «нужно», «надо». Продукты и блюда. Фразы для ресторанов. Блюда. Фразы, чтобы приглашать и принимать приглашение.

Грамматика. Личные местоимения в дательном падеже. Творительный падеж после предлога «с». Будущее время.

Фонетика. Произношение [ы], [и]. Оглушение звонких согласных на конце (б, д, в, з, ж, г). Интонация восхищения: «Как хорошо!».

6. Health

Коммуникативные задачи. Объяснять, какая часть тела болит. Общаться с доктором. Говорить и спрашивать о самочувствии. Давать рекомендации. Говорить о здоровом образе жизни, давать рекомендации, говорить, что можно делать, а что нельзя. Говорить о возрасте.

Лексика. Части тела. Фразы для общения с доктором. Можно / нельзя. Фразы для общения с доктором.

Грамматика. Конструкция «у меня был (а/о/и). Местоимения в дательном падеже со словами «можно», «нельзя» и с возрастом.

Фонетика: Интонация междометия «Ай!» при выражении боли. Произношение ь, ъ.

7. People

Коммуникативные задачи. Говорить об оптимизме и пессимизме. Выражать эмоции. Соглашаться / не соглашаться. Описывать характер человека. Конструкция «Кто это такой?». Описывать внешность человека. Сравнивать. Спрашивать нужный размер, цвет в магазине одежды. Покупать одежду.

Лексика. Эмоции (счастлив, рад, расстроен). Прилагательные, описывающие черты характера. Внешность. Одежда. Цвета.

Грамматика. Краткая форма прилагательных (счастливый – счастлив). Окончания прилагательных (мягкий вариант). Сравнительная и превосходная степени прилагательных (более, самый). Родительный падеж в конструкции «у меня есть». Сравнительная и превосходная степень прилагательных (исключения).

Фонетика. Произношение [ш], [щ]. Комбинация «дж». Интонация восхищения / удивления с использованием слова «так». Произношение «ё» после шипящих.

8. Transport

Коммуникативные задачи. Заказывать такси. Описывать поездку: на каком транспорте, сколько нужно ехать. Говорить о датах. Назначать, отменять, переносить или подтверждать встречи. Рассказывать о поездках. Рассказать о местоположении стран и городов.

Лексика. Виды транспорта. Порядковые числительные. Глаголы организации встреч: перенести, отменить, подтвердить, прийти/приехать, уйти/уехать. Части света. Слова для путешествий.

Грамматика. Предложный падеж для транспорта после предлога «на» (на машине). Окончания порядковых числительных. Родительный падеж при выражении месяца после конкретной даты (5 марта). Винительный падеж при выражении направления (куда?). Глаголы движения с приставками (начальный этап). Родительный падеж после предлогов из / с. Родительный падеж при выражении определения.

Фонетика. Отработка разницы произношения между «е» и «ё» в спряжении глаголов «идти», «ехать». Слова, где буква «г» произносится как «в» (его, сегодня). Оглушение «з» в предлоге «из».

9. My Family

Коммуникативные задачи. Спрашивать и рассказывать о своей семье, называть, кто кому кем приходится. Приглашать на вечеринку. Уточнять время. Спрашивать и рассказывать о своих увлечениях, о проведении свободного времени. Отказываться от приглашения. Поддержать разговор на тему «семья», рассказать о себе, когда родились, женились и т.д.

Лексика. Семья. Фразы-клише, чтобы пригласить, принять приглашение. Глаголы, обозначающие активность в свободное время (кататься, заниматься). Семейное положение. Глаголы: жениться, родиться, познакомиться, случиться.

Грамматика. Родительный падеж при выражении принадлежности. Возвратные глаголы в настоящем времени. Творительный падеж с глаголом «заниматься». Возвратные глаголы в прошедшем времени.

Фонетика. Оглушение «ж» на конце слов. Произношение тс, тьс = [ц]. Произношение и = [ы] после ш, ж, ц.

10. Holidays

Коммуникативные задачи. Поздравлять с праздниками. Рассказывать о традициях. Демонстрировать собеседнику, что вы знали что-то, но забыли. Подписывать поздравительную открытку, пожелать хорошего дня, приятного аппетита, спокойной ночи и т.д. Предлагать идеи подарков, соглашаться или опровергать идеи собеседника. Выражать удивление или недоверие при помощи фразы «Да ладно?!».

Лексика. Названия праздников. Глаголы: праздновать, поздравлять, прощаться. Пожелания (счастье, радость, любовь, удача, здоровье, богатство). Подарки. Предлоги.

Грамматика. Творительный падеж после предлога «с» с глаголом «поздравлять». Родительный падеж (существительные, прилагательные и местоимения) при выражении пожеланий. Родительный падеж после предлогов: из, от, для, без, до, после, около, у.

Фонетика. Слова с непроизносимой буквой «д». Слова, где г = [в]. Интонация фразы «Да ладно?!».

11. Shopping

Коммуникативные задачи. Общаться с продавцом в магазине, покупать косметику, выражать свои бизнес идеи. Спрашивать и называть время. Покупать фрукты и овощи на рынке. Обменять товар, спросить о наличии большого размера или примерочной комнаты, объяснить проблемные ситуации.

Лексика. Виды магазинов. Части тела. Косметика. Числа. Фрукты. Овощи. Одежда. Фразы для магазина.

Грамматика. Существительные, прилагательные и притяжательные местоимения (ед. и мн. ч.) с числами. Родительный падеж (ед. и мн. ч.) с числами. Родительный падеж (существительные, прилагательные, притяжательные местоимения) при выражении отсутствия.

Фонетика. Оглушение «в» на конце слов. Оглушение парных звонких согласных перед глухими согласными. Разница в произношении между «большой» и «больше».

12. Countries and Nationalities

Коммуникативные задачи. Узнавать, откуда собеседник и рассказывать о себе. Говорить о месте проживания и посещенных местах. Разговаривать о погоде. Обсуждать погоду в разное время года в разных странах. Говорить о стереотипах. Называть национальности.

Лексика. Страны. Месяцы. Времена года. Погода. Страны. Национальности.

Грамматика. Месяцы в предложном падеже при ответе на вопрос «когда?». Глаголы 2-го спряжения. Времена года при ответе на вопрос «когда». Образование существительных, называющих национальности.

Фонетика. Произношение р, рь, ю. Произношение названий национальностей.

Аннотации к рабочим программам дисциплин.

Направление: 03.04.01 Прикладные математика и физика

Направленность: Cyber Security/Кибер-безопасность

Vulnerabilities and Attacks/Уязвимости и атаки

Цель дисциплины:

изучение актуальности проблемы защиты информационных технологий в современных условиях и создание стройной и непротиворечивой защитной системы в сфере накопления, использования и защиты информации

Задачи дисциплины:

1. Предоставить студентам глубокие знания и понимание по созданию и администрированию инфраструктуры с точки зрения киберзащиты.

2.Развить у студентов инженерные навыки по защите от кибер-атак с применением информационных и сетевых технологий на практике.

Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные концепции построения защищённых локальных и глобальных сетей,

- область применимости традиционных и современных сетевых технологий,

- многообразие сетевых протоколов и стандартов,

- принципы работы различных типов коммуникационного оборудования и оборудования информационной безопасности,

- основы протокола TCP/IP, маршрутизация и IP-адресация, метод CIDR (Classless Inter-Domain Routing - бесклассовая междоменная маршрутизация). Методы обнаружения уязвимостей и идентификации кибер-атак,

- представление о круге проблем, связанных с защитой данных в сетях,

уметь:

- использовать преимущества и недостатки различных сетевых технологий для решения разнообразных прикладных задач обеспечения безопасности,

- объяснять отличия разных типов сетевых архитектур и их влияние на информационную безопасность,

- описывать типичные компоненты оборудования, используемые для передачи данных в сети. Подходы к синтезу новых безопасных технологий,

- описывать принципы и протоколы удаленной связи с решением задач обеспечения информационной безопасности «из конца в конец»,

владеть:

навыками построения структурных схем безопасных локальных сетей и сетей, включающих глобальные связи,

применением различных моделей безопасного обмена данными в сети связи,

навыками применения изученных информационных сетевых технологий для решения прикладных задач обеспечения информационной безопасности различных объектов риска.

Темы и разделы курса:

1. Model of the offender information safety of computer networks and systems.

Модель угроз информационной безопасности программных и программно-аппаратных средств различных объектов риска.

Методика формирования профиля защиты объектов риска различного назначения.

Примеры программирования выбранного профиля защиты среде Matlab.

2. Checking the functionality of protected fragments of Infocommunications.

Структура программно-аппаратного комплекса для проведения исследований характеристик защищённых инфокоммуникаций.

Облачный мониторинговый кластер безопасности.

Примеры программирования фрагментов мониторингового кластера безопасности систем в среде Matlab.

3. General provisions for the organization of network protection.

Формирование политики межсетевого взаимодействия.

Основные схемы подключения межсетевых экранов.

Примеры программирования схемы подключения межсетевого экрана объекта риска в Matlab.

4. Criteria for the security of the cyber attack object.

Условие защищенности объекта риска. Оценка защищенности объекта риска. Примеры программирования алгоритма оценки защищенности объекта риска в Матлаб.

Примеры программирования новых градаций функций защиты объекта риска в Матлаб.

5. Risk analysis methods and mathematical techniques used in intelligent systems for information security.

Оценка экстремальных рисков. Метрики для оценки рисков. Максимизация, экстремальные задачи, мультиэкстремальные задачи.

Примеры программных средств для оценки рисков в Matlab.

6. Modeling web-based attacks.

Класс моделей. Процесс идентификации в системно-ориентированном моделировании в облаке. Примеры программирования бот-атак в Matlab, Hadoop.

7. Premodernity analyses: goal settings.

Моделирование этапов, постановка целей, построение информационной структурно-функциональной среды, построение логической среды СУБД. верификация. Примеры программирования логических сред СУБД, в среде MATLAB, Hadoop.