Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средствах защиты
сборник учебно-методических материалов специальности

10.02.04 - Обеспечение информационной безопасности телекоммуникационных систем.

Благовещенск 2023

Печатается по решению
редакционно-издательского совета
факультета СПО
Амурского государственного
Университета

Составитель: Мельников Д.В.
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средствах защиты: сборник учебно-методических материалов специальностей 10.02.04 – Обеспечение информационной безопасности телекоммуникационных систем / Амур. Гос. Ун-т, Факультет среднего профессионального образования; сост. Д.В. Мельников – Благовещенск: АмГУ, 2023. – 12 с.

Лекция – одна из базовых форм обучения обучающихся. Углубляясь в значение термина, можно сказать, что лекцией следует называть такой способ изложения информации, который имеет стройную логическую структуру, выстроен с позиций системности, а также глубоко и ясно раскрывает предмет.

1. Краткое содержание курса лекций

МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	
Тема 1.1. Обеспечение безопасности операционных систем	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. Windows 7. Windows8. Linux. QNX и другие операционные системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации Пароли. PIN-коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи. Программно-аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон –Замок системный администратор. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог.
Тема 1.2. Технологии разграничения доступа	Архитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Server2016. Возможности администратора. Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда. Способы организации. Методы применения. ActiveDirectory. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов.

	Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP.Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.
Тема 1.4. Технологии обнаружения вторжений	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях.Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусовЖизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.
Тема 1.5. Методы управления средствами защиты	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.
МДК 02.02.Криптографическая защита информации	
Раздел 2.Криптографическая защита информации	

Тема 2.1. Основы криптографических методов защиты информации	Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста . Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.
Тема 2.2. Современные стандарты шифрования	Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. Российские стандарты симметричного шифрования . Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.

Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	Целостность сообщения. Случайная модель Orac1e. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции. Электронная цифровая подпись. Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012. Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/M1ME . Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети Защита информации в сетях организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. Защита информации в сетях сотовой связи. A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.

2.Методические рекомендации (указания) к практическим занятиям

Важной составной частью учебного процесса являются практические занятия.

Задачей преподавателя при проведении практических работ является грамотное и доступное разъяснение принципов и правил проведения работ, побуждение обучающихся к самостоятельной работе, определения места изучаемой дисциплины в дальнейшей профессиональной работе будущего выпускника.

Практическое занятие - форма организации обучения, когда обучающиеся по заданию и под руководством преподавателя выполняют одну или несколько практических работ.

Организация и проведение практических работ.

Выполнение обучающимися практических работ направлено:

- на обобщение, систематизацию, углубление и закрепления полученных теоретических занятий;

- на формирование умений применять полученные знания на практике;

- на выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Продолжительность - не менее двух академических часов. Необходимыми структурными элементами практической работы являются:

- самостоятельная деятельности обучающихся,
- инструктаж, проводимый преподавателем,
- организация обсуждения итогов выполнения лабораторной работы.

Перед началом выполнения лабораторной или практической работы проводится проверка знаний обучающихся - их теоретической готовности к выполнению задания.

Форма организации обучающихся на лабораторных или практических работах - индивидуальная.

При индивидуальной форме организации занятий каждый обучающийся выполняет индивидуальное задание.

Темы практических работ

1. Стеганографические методы скрытия информации
2. Бинарная арифметика. Модульная арифметика
3. Применение методов шифрования перестановкой
4. Применение методов шифрования заменой
5. Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа
6. Разработка хэш-функции
7. Разработка схемы простого пароля
8. Разработка схемы динамического пароля
9. Сертификаты открытого ключа
10. Настройка и администрирование токена
11. Настройка сервисов Рутокен-PinPad
12. Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя
13. Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита
14. Настройка изолированной среды
15. АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды
16. Программы надежного удаления информации
17. Архивирование информации
18. Основные действия с виртуальной машиной
19. Работа с контрольными точками
20. Использование внешних устройств
21. Работа с локальным хранилищем сертификатов в ОС WINDOWS
22. Установка и настройка ПО eTokenPKIClient
23. Настройка ПО eTokenPKIClient с помощью групповых политик
24. Развертывание TMS в среде Active Directory
25. Настройка TMS всреде Active Directory
26. Настройкаполитик TMS
27. Изучение средств обнаружения атак

Темы лабораторных работ

1. Применение методов шифрования многоалфавитной замены
2. Криптоанализ методов перестановки
3. Криптоанализ методов замены
4. Компьютерное шифрование
5. Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители
6. Настройка сервисов Рутокен-ЭЦП
7. Настройка сервисов Рутокен–Bluetooth
8. Настройка сервисов Рутокен–S
9. Разработка алгоритма PGP
10. Изучение протоколов SSL, TLS, IPSec

11. Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2
12. Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация
13. Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование
14. Восстановление информации типовыми средствами Программы восстановление информации
15. Программные средства резервного копирования. Настройка RAID-массивов
16. Инсайдерская информация. Программы сбора информации о ПК
17. Настройка межсетевого экрана.
18. Настройка использования виртуального токена
19. Использование токена на рабочем месте администратора
20. Установка и настройка СКЗИ «КриптоПроCSP»
21. Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP
22. Применение SecretDisk4
23. Применение SecretDisk Server NG
24. Изучение основных возможностей ПО VipNetClient
25. Изучение настроекПОVipNetClient
26. Изучение возможностей ПО Деловая почта
27. Изучение антивирусных продуктов

3.Методические рекомендации по составлению информационных сообщений (докладов)

Информационное сообщение (доклад) – есть результат процессов преобразования формы и содержания документов с целью их изучения, извлечения необходимых сведений, а также их оценки, сопоставления, обобщения и представления в устной форме (защиты)

Требования к оформлению

Объем информационных сообщений (докладов) – до 5 полных страниц текста, набранного в текстовом редакторе Word, шрифтом – TimesNewRoman, 14 шрифтом с одинарным межстрочным интервалом, параметры страницы – поля со всех сторон по 20 мм.

Ссылки на литературу концевые, 10 шрифтом. В названии следует использовать заглавные буквы, полужирный шрифт, при этом не следует использовать переносы; выравнивание осуществлять по центру страницы. Данные об авторе указываются 14 шрифтом (курсивом) в правом верхнем углу листа.

4.Методически рекомендации по составлению мультимедийной презентации

Общие требования к презентации

Мультимедийные презентации используются для того, чтобы выступающий смог на большом экране или мониторе наглядно продемонстрировать дополнительные материалы к своему сообщению, эти материалы могут также быть подкреплены соответствующими звукозаписями.

Общие нормы:

- презентация не должна быть меньше 10 слайдов.
- первый лист – это титульный лист, на котором обязательно должны быть представлены: название; фамилия, имя, отчество автора.
- следующим (2-ой) слайдом может быть содержание, где представлены основные этапы (моменты) презентации. Желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание.
- дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста.
- в презентации необходимы импортированные объекты из существующих цифровых образовательных ресурсов. (Наиболее приемлемым и удобным в работе является «Использование Microsoft Office»);

– последним слайдом презентации должен быть список литературы.

Практические рекомендации по созданию презентаций:

Создание презентации состоит из трех этапов:

I. Планирование презентации – это многошаговая процедура, включающая определение целей, изучение аудитории, формирование структуры и логики подачи материала. Планирование презентации включает в себя:

– определение целей,
– определение основной идеи презентации,
– подбор дополнительной информации,
– планирование выступления,
– создание структуры презентации,
– проверка логики подачи материала,
– подготовка заключения.

II. Разработка презентации – методологические особенности подготовки слайдов презентации, включая вертикальную и горизонтальную логику, содержание и соотношение текстовой и графической информации.

III. Репетиция презентации – это проверка и отладка созданной презентации.

Требования к оформлению презентаций

В оформлении презентаций выделяют два блока:

– оформление слайдов;
– представление информации на них.

Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

Оформление слайдов:

Стиль	- соблюдайте единый стиль оформления, - избегайте стилей, которые будут отвлекать от самой презентации.
Использование цвета	- в слайдах необходимо использовать цветовую схему, - для фона и текста используйте контрастные цвета, - обратите внимание на цвет гиперссылок (до и после использования).
Анимационные эффекты	- используйте возможности компьютерной анимации для представления информации на слайде. - не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.

Представление информации:

Содержание информации	- используйте короткие слова и предложения, - минимизируйте количество предлогов, наречий, прилагательных, - заголовки должны привлекать внимание аудитории.
Расположение информации на странице	- старайтесь использовать возможности схематического, а не текстового представления информации, - наиболее важная информация должна располагаться в центре экрана.
Шрифты	- размер для заголовков – не менее 36 пунктов. - размер для информации – не менее 20 пунктов. - шрифты без засечек легче читать с большого расстояния, - нельзя смешивать разные типы шрифтов в одной презентации, - для выделения информации следует использовать

	жирный шрифт, курсив или подчеркивание, - нельзя злоупотреблять прописными буквами (они читаются хуже строчных).
Способы выделения информации	следует использовать: - рамки; границы, заливку; - штриховку, стрелки; - рисунки, диаграммы, схемы для иллюстрации наиболее важных фактов.
Объем информации	- не стоит заполнять один слайд слишком большим объемом информации: люди могут единовременно запомнить не более трех фактов, выводов, определений. - наибольшая эффективность достигается тогда, когда ключевые пункты отображаются по одному на каждом отдельном слайде.
Виды слайдов	Для обеспечения разнообразия следует использовать разные виды слайдов: - с текстом; - со схемами; - с диаграммами.

5.Методические рекомендации к проведению занятий с использованием активных и интерактивных форм

Федеральный государственный образовательный стандарт среднего профессионального образования (ФГОС СПО) одним из требований к условиям реализации основных образовательных программ обязывает использовать в учебном процессе активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Внедрение активных и интерактивных форм обучения – одно из важнейших направлений совершенствования подготовки обучающихся.

Активные методы обучения – формы обучения, направленные на развитие у обучаемых самостоятельного мышления и способности квалифицированно решать нестандартные профессиональные задачи. Цель обучения – развивать мышление обучаемых, вовлечение их в решение проблем, расширение и углубление знаний и одновременное развитие практических навыков и умения мыслить, размышлять, осмысливать свои действия.

Интерактивное обучение – это специальная форма организации познавательной деятельности. Она имеет в виду вполне конкретные и прогнозируемые цели:

- повышение эффективности образовательного процесса, достижение высоких результатов;
- усиление мотивации к изучению дисциплины;
- формирование и развитие профессиональных навыков обучающихся;
- формирование коммуникативных навыков;
- развитие навыков анализа и рефлексивных проявлений;
- развитие навыков владения современными техническими средствами и технологиями восприятия и обработки информации;
- формирование и развитие умения самостоятельно находить информацию и определять ее достоверность;
- окращение доли аудиторной работы и увеличение объема самостоятельной работы студентов.

Интерактивные формы применяются при проведении аудиторных занятий, при самостоятельной работе обучающихся и других видах учебных занятий, а также при повышении квалификации.

6.Уроки с применением активных и интерактивных форм проведения занятий

Метод основан на анализе конкретных ситуаций.

Поэтому концентрирование внимания обучаемых на этих случаях, происшедших в области их будущей деятельности, полезно для выработки обобщенных точек зрения на поведение в экстремальных условиях.

Метод разбора конкретных ситуаций способствует формированию профессиональной интуиции, чутья, умения разбираться в нестандартных ситуациях, а также предвидеть возможные последствия тех или иных решений.

Особенностью метода является необходимость в опытном наставнике, обладающем большим тактом, позволяющем ему, не задевая излишне самолюбия слушателей, обсуждать время от времени и случаи из их практики.

СОДЕРЖАНИЕ