МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт информационных технологий, машиностроения и автотранспорта

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: институт информационных технологий, машиностроения и автотранспорта
Должность: директор института
Дата: 05.04.2023 03:57:14

Стенин Дмитрий Владимирович

Рабочая программа дисциплины

Методы и средства защиты информационных систем

Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация / направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация
"Специалист по защите информации"

Формы обучения
очная

Кемерово 2023 г.

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 03.04.2023 07:19:04

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 4 от 04.04.2023

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 04.04.2023 03:34:07

Прокопенко Евгения Викторовна

Согласовано учебно-методической комиссией по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Протокол № 4 от 04.04.2023

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 04.04.2023 03:35:42

Прокопенко Евгения Викторовна

1 Перечень планируемых результатов обучения по дисциплине "Методы и средства защиты информационных систем", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-4 - Способен определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем.

Результаты обучения по дисциплине:

Знать способы реализации угроз безопасности в автоматизированных системах.

Уметь выявлять известные уязвимости информационных систем.

Владеть правилами, процедурами, практическими приемами, руководящими принципами, методами, средствами) для защиты информации автоматизированных систем.

2 Место дисциплины "Методы и средства защиты информационных систем" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Языки программирования, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Технологии и методы программирования, Нормативные требования по защите информации, Информационные угрозы, Классификация защищаемой информации и информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Методы и средства защиты информационных систем" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Методы и средства защиты информационных систем" составляет 4 зачетных единицы, 144 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 3/Семестр 5			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	16		
Самостоятельная работа	80		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Методы и средства защиты информационных систем", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	**Трудоемкость в часах**
	ОФ
1. Методы криптографической защиты информации. Основные понятия и классификация средств криптографической защиты информации. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства идентификации и аутентификации пользователей; средства аутентификации электронных данных и средства управления ключевой информацией.	2
2. Симметричные алгоритмы шифрования. Основные свойства симметричных криптосистем. Классическая сеть Фейстеля. Блочные алгоритмы шифрования данных. Алгоритм шифрования DES и его модификации. Шифрование в режимах ESB, CBC, CFB и OFB.	1
3. Асимметричные алгоритмы шифрования. Основные свойства асимметричных криптосистем. Однонаправленные функции. Алгоритм шифрования RSA. Криптосистема Эль Гамаля. Комбинированные криптосистемы.	1
4. Функции хэширования. Основные свойства хэш-функций. Функция хэширования SHA, MD5. Функция хэширования. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Ключевые и бесключевые функции хэширования.	2
5. Электронная цифровая подпись. Основные свойства цифровой подписи. Алгоритмы цифровой подписи. Отечественный стандарт цифровой подписи. Схемы слепой подписи. Схемы неоспоримой подписи.	2
6. Идентификация и аутентификация. Основные понятия и классификация. Аутентификация на основе одноразовых и многоразовых паролей. Биометрическая идентификация и аутентификация пользователя. Аутентификация, основанная на симметричных и асимметричных алгоритмах.	2
7. Управление криптографическими ключами. Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом.	2
8. Практика сетевой защиты Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.	2
9. Защита в вычислительных сетях . Общие вопросы безопасности в ЛВС. Защита информации при межсетевом взаимодействии. Криптографические протоколы, используемые для защиты технологии клиент-сервер. Защита информации в Web-технологиях. Основные схемы сетевой защиты на базе межсетевых экранов. Защита электронной почты. Принципы и средства защиты электронной почты.	2

Итого	**16**

4.2. Практические занятия

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
1. Исследование криптоалгоритма шифрования RSA.	8
2. Исследование электронной цифровой подписи RSA .	8
3. Исследование криптоалгоритма шифрования Эль Гамаля.	8
4. Исследование электронной цифровой подписи Эль Гамаля.	8
Итого	**32**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	30
Оформление отчетов по практическим и(или) лабораторным работам	44
Подготовка к промежуточной аттестации	6
Итого	**80**
Самостоятельная работа под руководством преподавателя	16

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Методы и средства защиты информационных систем"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ПК-4	Определяет комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем	**Знать** способы реализации угроз безопасности в автоматизированных системах. **Уметь** выявлять известные уязвимости информационных систем. **Владеть** правилами, процедурами, практическими приемами, руководящими принципами, методами, средствами) для защиты информации автоматизированных систем.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100

Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

Тема 1. Методы криптографической защиты информации.

1. Основные понятия и классификация средств криптографической защиты

1. информации.
2. Аппаратно-программные средства защиты информации:
3. Средства обеспечения конфиденциальности данных;
4. средства идентификации и аутентификации пользователей;
5. средства аутентификации электронных данных и средства управления ключевой
6. информацией.

Тема 2. Симметричные алгоритмы шифрования.

1. Основные свойства симметричных криптосистем.
2. Что представляет собой Классическая сеть Фейстеля.
3. Блочные алгоритмы шифрования данных.
4. Алгоритм шифрования DES и его модификации.
5. Шифрование в режимах ESB, CBC, CFB и OFB.

Тема 3. Асимметричные алгоритмы шифрования.

1. Основные свойства асимметричных криптосистем.
2. Однонаправленные функции.
3. Алгоритм шифрования RSA.
4. Криптосистема Эль Гамаля.
5. Комбинированные криптосистемы.

Тема 4. Функции хэширования.

1. Основные свойства хэш-функций.
2. Функция хэширования SHA, MD5.
3. Понятие функции хэширования.
4. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
5. Ключевые и бесключевые функции хэширования.

Тема 5. Электронная цифровая подпись.

1. Основные свойства цифровой подписи.
2. Алгоритмы цифровой подписи.
3. Отечественный стандарт цифровой подписи.
4. Схемы слепой подписи.
5. Схемы неоспоримой подписи.

Тема 6. Идентификация и аутентификация.

1. Основные понятия идентификации и аутентификации
2. Классификация методов идентификации и аутентификации.
3. Аутентификация на основе одноразовых и многоразовых паролей.
4. Биометрическая идентификация и аутентификация пользователя.
5. Аутентификация, основанная на симметричных и асимметричных алгоритмах.

Тема 7. Управление криптографическими ключами.

1. Генерация и хранение ключей.
2. Распределение ключей.
3. Управление ключами в системах с открытым ключом.
4. Понятие и принцип действия криптографического ключа
5. Классификация криптографических ключей в зависимости от алгоритмов использования

Тема 8. Практика сетевой защиты

1. Концепция построения защищённых виртуальных частных сетей VPN.
2. Функции и компоненты сети VPN.
3. VPN-решения для построения защищённых корпоративных сетей.
4. Какие протоколы используются для защиты и безопасной передачи данных в VPN-сетях?
5. Отличаются ли методы защиты VPN-сетей от реальных корпоративных сетей?

Тема 9. Защита в вычислительных сетях .

1. Общие вопросы безопасности в ЛВС.
2. Криптографические протоколы, используемые для защиты технологии клиент-сервер.
3. Защита информации в Web-технологиях.
4. Основные схемы сетевой защиты на базе межсетевых экранов.
5. Защита электронной почты. Принципы и средства защиты электронной почты.

Примерный перечень тестовых заданий:

Тема 1. Методы криптографической защиты информации.

1. Какие из сервисов реализуются при использовании криптографических преобразований {несколько верных ответов):

контроль целостности;
аутентификация;
шифрование;
алгоритм.

2. Что позволяют обеспечивать криптографические методы защиты:

целостность сообщений;
конфиденциальность сообщений;
определять подлинность источников сообщений;
гарантировать невозможность отказа от совершенных действий.

3. Чем определяется уровень надежности применяемых криптографических преобразований:

значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;
сложностью комбинации символов, выбранных случайным образом;
использованием большого числа ключей для шифрования;
отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

Тема 2. Симметричные алгоритмы шифрования.

1. Какой алгоритм не используется при симметричном шифровании:

поточное шифрование;
побитовое шифрование;
блочное шифрование;
алгоритм Эль-Гамаля.

2. Что является преимуществом симметричного шифрования:

скорость выполнения криптографических преобразований;
легкость внесения изменений в алгоритм шифрования;
секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
применение в системах аутентификации (электронная подпись).

3. Какой размер ключа в отечественном стандарте симметричного шифрования:

56 бит;
124 бит;
256 бит.

Тема 3. Асимметричные алгоритмы шифрования.

1. Асимметричные алгоритмы шифрования по-другому называются


1678907003

алгоритмами шифрования с открытым ключом
симметричными алгоритмами шифрования
односторонними алгоритмами шифрования
помехоустойчивыми алгоритмами шифрования

2. Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования передаваемых данных?

отправитель шифрует сообщение открытым ключом получателя, а получатель расшифровывает сообщение своим закрытым ключом
отправитель шифрует сообщение закрытым ключом получателя, а получатель расшифровывает сообщение своим открытым ключом
отправитель шифрует сообщение своим открытым ключом, а получатель расшифровывает сообщение закрытым ключом отправителя
отправитель шифрует сообщение своим закрытым ключом, а получатель расшифровывает сообщение открытым ключом отправителя

3. Преимуществами асимметричных криптографических алгоритмов являются {несколько верных ответов):

скорость выполнения криптографических преобразований;
легкость внесения изменений в алгоритм шифрования;
секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
применение в системах аутентификации (электронная цифровая подпись).

Тема 4. Функции хэширования.

1. Как называется значение хеш-функции?

хеш-код
хеш-блок
прообраз
сумма

2. Какие требования предъявляются к криптографическим хеш-функциям?

хеш-функция должна быть применима к сообщению фиксированного размера
при известном значении хеш-функции H(M)=m должно быть трудно (практически невозможно) найти подходящий прообраз M
при известном сообщении M должно быть трудно найти другое сообщение M’ с таким же значением хеш-функции, как у исходного сообщения
для сообщений одинакового размера хеш-код должен получаться одинаковым

3. Что называется хеш-функцией?

функция, позволяющая создать комбинацию бит, служащую для контроля изменений в зашифрованном сообщении
функция, которая позволяет создать электронную цифровую подпись
функция, позволяющая создать контрольную комбинацию бит, служащую для обнаружения искажений в передаваемом сообщении
функция, которая для строки произвольной длины вычисляет некоторое характерное целое значение или некоторую другую строку фиксированной длины

Тема 5. Электронная цифровая подпись.

1. Электронные цифровые подписи, созданные с использованием стандарта ГОСТ Р3410-94, являются рандомизированными, так как …

для одинаковых сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи
для одинаковых сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи
для разных сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи

для разных сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи

2. Каким требованиям должна удовлетворять электронная цифровая подпись?

подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими
подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ

3. Отметьте все верные утверждения относительно электронной цифровой подписи:

подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
От поставленной подписи невозможно отказаться, то есть лицо, подписавшее документ, не сможет потом утверждать, что не ставило подпись
подпись не связывается с конкретным сообщением и может быть перенесена на другой документ
подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ

Тема 6. Идентификация и аутентификация.

1. В качестве аутентификатора в сетевой среде могут использоваться:

год рождения субъекта
фамилия субъекта
секретный криптографический ключ

2. Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от: выбрать все верные

перехвата
воспроизведения
атак на доступность

3. При использовании сервера аутентификации Kerberos пароли по сети:

не передаются
передаются в зашифрованном виде
передаются в открытом виде

Тема 7. Управление криптографическими ключами.

1. При замене ключей методом RSA сревер получает ___

половину ключа в исходном тексте
(2) 48-байтовое случайное число
ключ Диффи-Хеллмана, подписанный своим секретным ключом
фиксированную половину ключа (gx)

2. Сколько различных ключей криптографических объектов извлекаются из материала для ключей в протоколе SSL ?

6
4
2
7

3. В PGP при передаче открытого ключа по электронной почте для подтверждения подлинности применяют ___

дайджест
открытый ключ приемника
секретный ключ передатчика
ключ сеанса

Тема 8. Практика сетевой защиты

1. Как называют средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству.

экран
шлюз
файервол
мост

2. Какие задачи решают сетевые сканеры безопасности?

идентификация и анализ уязвимостей
инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети
формирование отчетов, содержащих описание уязвимостей и варианты их устранения
поиск и идентификация угроз в сети интернет

3. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется

брандмауэром
браузером
маршрутизатором
фильтром

Тема 9. Защита в вычислительных сетях.

1. Какой стандарт рассматривает вопросы сетевой безопасности?

оранжевая книга
зеленая книга
черная книга
красная книга

2. Какой криптографический метод преобразования информации применяется в информационных сетях для повышения достоверности передаваемой информации?

шифрование
стеганография
кодирование
сжатие

3. Какие сетевые протоколы обмена позволят защититься от атаки «анализ сетевого трафика»?

TELNET
SSL
SSH
TLS
FTP
HTTP

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном

объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации является зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:
- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:
- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.
2. Политика безопасности информационных систем и ее основные элементы
3. Дискреционный и мандатный доступ к ресурсам информационных систем.
4. Основные методы обеспечения безопасности информационных систем
5. Основные услуги безопасности, предоставляемые информационными системами
6. Механизмы реализации услуг безопасности в информационных системах
7. Классификация криптографических алгоритмов
8. Структурная схема симметричной криптосистемы
9. Структурная схема асимметричной криптосистемы
10. Математические определения шифра, процедур шифрования и дешифрации
11. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы
12. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля
13. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования
14. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB
15. Алгоритм шифрования TEA: структура, достоинства и недостатки

16. Алгоритм шифрования DES: структура, достоинства и недостатки
17. Линейный криптоанализ блочных шифров
18. Дифференциальный криптоанализ блочных шифров
19. Поточные шифры: принципы функционирования, структура
20. Методы построения нелинейных поточных шифров
21. Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов
22. RSA: математические основы криптоалгоритма
23. RSA: структура криптоалгоритма
24. Алгоритм асимметричного шифрования Рабина
25. Криптосистема ЭльГемаля: структура, криптостойкость
26. Метод ключевого обмена Диффи-Хелмана
27. Системы управления ключами: разновидности ключей, схемы обмена ключами
28. Сертификация открытых ключей асимметричных алгоритмов. Инфраструктура PKI
29. Хэш-функции: назначение и основные свойства
30. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров
31. Система ЭЦП на основе алгоритма ЭльГемаля
32. Система ЭЦП на основе эллиптических кривых
33. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA
34. Генерация криптостойких случайных чисел.
35. Вероятностная генерация простых чисел для криптоалгоритмов.
36. Аутентификация в информационных системах: назначение, разновидности, угрозы подсистемам аутентификации
37. Биометрические методы аутентификации пользователей
38. Системы аутентификации с защищенными паролями и с проверкой на стороне сервера
39. Система аутентификации по схеме «запрос-ответ»
40. Протокол аутентификации пользователей Kerberos
41. Угрозы безопасности в глобальных сетях
42. Межсетевые экраны: назначение, основные функции, состав
43. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки
44. Proxy-сервера : назначение, основные функции, достоинства и недостатки
45. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона
46. Обзор криптографических протоколов: SSL, TLS, IPSecurity, SSH, PPTP, L2TP
47. Обзор аутентификационных протоколов : PAP, CHAP, EAP, RADIUS.
48. Средства аудита ОС семейства Windows
49. Модель безопасности ОС семейства Windows
50. Подсистема аудита ОС семейства Unix
51. Модель безопасности ОС Unix
52. Эксплойты: определение. Атаки на переполнение буфера и методы защиты от них.
53. Эксплойты: определение. SQL-инъекции и методы. защиты от них
54. Компьютерные вирусы: определение, методы заражения и маскировки. Методы защиты от вирусов.

Примерный перечень тестовых заданий на экзамен:

1. Какие из сервисов реализуются при использовании криптографических преобразований {несколько верных ответов):

контроль целостности;
аутентификация;
шифрование;
алгоритм.

2. Что позволяют обеспечивать криптографические методы защиты:

целостность сообщений;
конфиденциальность сообщений;
определять подлинность источников сообщений;


1678907003

гарантировать невозможность отказа от совершенных действий.

3. Чем определяется уровень надежности применяемых криптографических преобразований:

значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;
сложностью комбинации символов, выбранных случайным образом;
использованием большого числа ключей для шифрования;
отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

4. Какой алгоритм не используется при симметричном шифровании:

поточное шифрование;
побитовое шифрование;
блочное шифрование;
алгоритм Эль-Гамаля.

5. Что является преимуществом симметричного шифрования:

скорость выполнения криптографических преобразований;
легкость внесения изменений в алгоритм шифрования;
секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
применение в системах аутентификации (электронная подпись).

6. Какой размер ключа в отечественном стандарте симметричного шифрования:

56 бит;
124 бит;
256 бит.

7. Асимметричные алгоритмы шифрования по-другому называются

алгоритмами шифрования с открытым ключом
симметричными алгоритмами шифрования
односторонними алгоритмами шифрования
помехоустойчивыми алгоритмами шифрования

8. Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования передаваемых данных?

отправитель шифрует сообщение открытым ключом получателя, а получатель расшифровывает сообщение своим закрытым ключом
отправитель шифрует сообщение закрытым ключом получателя, а получатель расшифровывает сообщение своим открытым ключом
отправитель шифрует сообщение своим открытым ключом, а получатель расшифровывает сообщение закрытым ключом отправителя
отправитель шифрует сообщение своим закрытым ключом, а получатель расшифровывает сообщение открытым ключом отправителя

9. Преимуществами асимметричных криптографических алгоритмов являются {несколько верных ответов):

скорость выполнения криптографических преобразований;
легкость внесения изменений в алгоритм шифрования;
секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
применение в системах аутентификации (электронная цифровая подпись).

10. Как называется значение хеш-функции?

хеш-код
хеш-блок

прообраз
сумма

11. Какие требования предъявляются к криптографическим хеш-функциям?

хеш-функция должна быть применима к сообщению фиксированного размера
при известном значении хеш-функции H(M)=m должно быть трудно (практически невозможно) найти подходящий прообраз M
при известном сообщении M должно быть трудно найти другое сообщение M’ с таким же значением хеш-функции, как у исходного сообщения
для сообщений одинакового размера хеш-код должен получаться одинаковым

12. Что называется хеш-функцией?

функция, позволяющая создать комбинацию бит, служащую для контроля изменений в зашифрованном сообщении
функция, которая позволяет создать электронную цифровую подпись
функция, позволяющая создать контрольную комбинацию бит, служащую для обнаружения искажений в передаваемом сообщении
функция, которая для строки произвольной длины вычисляет некоторое характерное целое значение или некоторую другую строку фиксированной длины

13. Электронные цифровые подписи, созданные с использованием стандарта ГОСТ Р3410-94, являются рандомизированными, так как …

для одинаковых сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи
для одинаковых сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи
для разных сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи
для разных сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи

14. Каким требованиям должна удовлетворять электронная цифровая подпись?

подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими
подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ

15. Отметьте все верные утверждения относительно электронной цифровой подписи:

подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
От поставленной подписи невозможно отказаться, то есть лицо, подписавшее документ, не сможет потом утверждать, что не ставило подпись
подпись не связывается с конкретным сообщением и может быть перенесена на другой документ
подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ

16. В качестве аутентификатора в сетевой среде могут использоваться:

год рождения субъекта
фамилия субъекта
секретный криптографический ключ

17. Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от: выбрать все верные

перехвата
воспроизведения

атак на доступность

18. При использовании сервера аутентификации Kerberos пароли по сети:

не передаются
передаются в зашифрованном виде
передаются в открытом виде

19. При замене ключей методом RSA сревер получает ___

половину ключа в исходном тексте
(2) 48-байтовое случайное число
ключ Диффи-Хеллмана, подписанный своим секретным ключом
фиксированную половину ключа (gx)

20. Сколько различных ключей криптографических объектов извлекаются из материала для ключей в протоколе SSL ?

6
4
2
7

21. В PGP при передаче открытого ключа по электронной почте для подтверждения подлинности применяют ___

дайджест
открытый ключ приемника
секретный ключ передатчика
ключ сеанса

22. Как называют средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству.

экран
шлюз
файервол
мост

23. Какие задачи решают сетевые сканеры безопасности?

идентификация и анализ уязвимостей
инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети
формирование отчетов, содержащих описание уязвимостей и варианты их устранения
поиск и идентификация угроз в сети интернет

24. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется

брандмауэром
браузером
маршрутизатором
фильтром

25. Какой стандарт рассматривает вопросы сетевой безопасности?

оранжевая книга
зеленая книга
черная книга
красная книга

26. Какой криптографический метод преобразования информации применяется в информационных сетях для повышения достоверности передаваемой информации?

шифрование
стеганография
кодирование
сжатие

27. Какие сетевые протоколы обмена позволят защититься от атаки «анализ сетевого трафика»?

TELNET
SSL
SSH
TLS
FTP
HTTP

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;

2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885 (дата обращения: 01.04.2022). — Режим доступа: для авториз. пользователей.

2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 96 с. — ISBN 978-5-8114-6527-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148474 (дата обращения: 01.04.2022). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Туманов, С. А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. – Новосибирск : Изд-во НГТУ, 2016. – 54, [1] с. – URL: http://library.kuzstu.ru/meto.php?n=227592.pdf&type=nstu:common (дата обращения: 18.11.2023). – Текст : электронный.

2. Туманов, С. А. Система защиты информации от несанкционированного доступа на основе "SecretNet 7" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. – Новосибирск : Изд-во НГТУ, 2016. – 89, [2] с. – URL: http://library.kuzstu.ru/meto.php?n=226348.pdf&type=nstu:common (дата обращения: 18.11.2023). – Текст : электронный.

3. Нестандартные методы защиты информации ; Северо-Кавказский федеральный университет; Автор-составитель: Пашинцев Владимир Петрович; Автор-составитель: Ляхов Алексей Владимирович. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 196 с. – URL: http://biblioclub.ru/index.php?page=book_red&id=458132 (дата обращения: 26.04.2023). – Текст : электронный.

4. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699 (дата обращения: 01.04.2022). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Защита информации : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 56 с. – URL: http://library.kuzstu.ru/meto.php?n=4637 (дата обращения: 18.11.2023). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Электронная библиотечная система «Юрайт» https://urait.ru/
6. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Информационные системы и технологии : научно-технический журнал (электронный) https://elibrary.ru/contents.asp?titleid=28336
2. Информационные технологии и вычислительные системы : журнал (печатный/электронный) https://elibrary.ru/contents.asp?titleid=8746
3. Информация и безопасность : научный журнал (печатный)
4. Открытые системы. СУБД : журнал (печатный/электронный) https://elibrary.ru/contents.asp?titleid=9826
5. Программные продукты и системы : международный научно-практический журнал (печатный)

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Методы и средства защиты информационных систем"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в

следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Методы и средства защиты информационных систем", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Libre Office
2. Mozilla Firefox
3. Google Chrome
4. 7-zip
5. Microsoft Windows
6. ESET NOD32 Smart Security Business Edition
7. Kaspersky Endpoint Security
8. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Методы и средства защиты информационных систем"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.