Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Введение в компьютерную безопасность

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2 Способен совершенствовать и реализовывать новые математические методы решения прикладных задач.

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-2.1 Использует результаты прикладной математики для освоения, адаптации новых методов решения задач в области своих профессиональных интересов.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;

– рефераты.

Пример типового теста (ИОПК-2.1). Защита информации. Основные термины и определения. Термины, относящиеся к способам защиты информации.

1. Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации разведками и другими заинтересованными субъектами это:

а) защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

2. Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации это:

а) защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

3. Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации это

а) информации защита информации от разглашения

б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

4. Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

а) информации защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

5. Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

а) информации защита информации от разглашения
б) защита информации от утечки
в) защита информации от несанкционированного доступа
г) защита информации от несанкционированного воздействия
д) защита информации от непреднамеренного воздействия

Ключи: 1 б), 2 а), 3 в), 4 г), 5 д).

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно более, чем на половину вопросов.

Примеры тем рефератов (ИОПК-4.2):

- Криптографические протоколы идентификации на основе техники “запрос-ответ”.
- Протоколы идентификации на основе техники доказательства знания.
- Криптографические протоколы открытого распределения ключей
- Криптографические протоколы предварительного распределения ключей
- Криптографические протоколы электронного голосования.
- Криптографические протоколы безопасных совместных вычислений.
- Криптографические протоколы электронного аукциона.
- Атаки на протоколы идентификации.
- Атаки на протоколы распределения ключей.

Критерии оценки реферата.

«Отлично»: тема полностью раскрыта, работа оформлена на высоком уровне, в работе проведен широкий и последовательный обзор научно/технической литературы по

исследуемой проблеме, автор свободно ориентируется в материале, оперирует терминологией по рассматриваемой проблеме, может аргументировано отстаивать свою точку зрения и ответить на возникающие вопросы.

«Хорошо»: тема работы в целом достаточно полно раскрыта, использованы соответствующая основная и дополнительная литература и другие источники, автор достаточно уверенно ориентируется в материале, имеются замечания или неточности в части изложения и отдельные недостатки по оформлению работы.
«Удовлетворительно»: тема работы раскрыта недостаточно полно, использовались только основные источники, материал изложен непоследовательно, имеются недостатки в оформлении.

«Неудовлетворительно»: тема работы не раскрыта, материал изложен непоследовательно, отсутствуют ссылки на литературные источники и другие источники, имеются недостатки в оформлении работы, автор плохо ориентируется в представленном материале, содержание работы заимствовано из какого-либо источника.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Промежуточная аттестация осуществляется на основе выполнения студентом контрольного задания, которое выявляют все запланированные индикаторы достижения компетенций.

Примеры контрольных заданий.

Задание 1 .Требуется изучить и программно реализовать какой – либо криптографический протокол из предложенного списка:

- S/KEY (One-Time Password System), RFC 1760, https://datatracker.ietf.org/doc/html/rfc1760
- TOTP (Time-based One-Time Password Algorithm), RFC 6238, https://datatracker.ietf.org/doc/html/rfc6238
- CHAP (Challenge Handshake Authentication Protocol), RFC 1994, https://datatracker.ietf.org/doc/html/rfc1994
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), RFC 2433, https://www.rfc-editor.org/rfc/rfc2433
- Diffie-Hellman, RFC 2631, https://datatracker.ietf.org/doc/html/rfc2631
- Oakley (any example), RFC 2412, https://datatracker.ietf.org/doc/html/rfc2412

При реализации возможны модификации и упрощения оригинала, которые не затрагивают базовые принципы работы протокола.

Отчет о проделанном контрольном задании необходимо загрузить среду электронного обучения ТГУ. Отчет должен включать в себя: название дисциплины и название задания, ФИО и номер группы исполнителя работы, краткое описание спецификации протокола, детали и особенности программной реализации (используемые классы и методы, структуры данных, формат сообщений протокола, а также выборочные примеры кода программы), скриншоты (снимки экрана), демонстрирующие проходы (шаги) и типовые сценарии работы протокола, например случай с правильным/ложным паролем или штатный/нештатный режим работы.

Задание 2. С помощью свободно распространяемого эмулятора сети (PNETLab, Cisco Packet Tracer, Boson NetSim, GNS3, VIRL, EVE-NG) требуется спроектировать произвольную простую сетевую топологию и произвести настройку сетевых устройств, промоделировать какую-либо компьютерную атаку, а далее в реализованную сетевую топологию добавить и настроить средство защиты информации или перенастроить сетевые устройства и убедиться, что компьютерная атака нейтрализована. Моделировать компьютерную атаку из одного из следующих классов:

- ARP-spoofing attack
- VLAN-hopping attack
- CAM Overflow attack
- DHCP Starvation attack
- STP L2 attack
- DDOS attack
- ICMP redirect man-in-the-middle attack
- OSPF route spoofing
- BGP route spoofing

Отчет о проделанном контрольном задании выкладывается в среду электронного обучения ТГУ и включает в себя: название дисциплины и название задания; ФИО и номер группы исполнителя работы; краткое описание компьютерной атаки; рисунок сетевой топологи для моделирования атаки; скриншоты (снимки экрана), демонстрирующие шаги атаки с комментариями; скриншоты, демонстрирующие меры противодействия атаке с комментариями.

Критерии оценивания промежуточной аттестации:

Зачет по дисциплине – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении контрольного задания.

Незачет по дисциплине – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении контрольного задания.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Тест (ИОПК-2.1). Термины, относящиеся к способам защиты информации.

1. Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации разведками и другими заинтересованными субъектами это:

е) защита информации от разглашения
ж) защита информации от утечки
з) защита информации от несанкционированного доступа
и) защита информации от несанкционированного воздействия
к) защита информации от непреднамеренного воздействия

2. Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации это:

е) защита информации от разглашения
ж) защита информации от утечки
з) защита информации от несанкционированного доступа
и) защита информации от несанкционированного воздействия
к) защита информации от непреднамеренного воздействия

3. Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации это

е) информации защита информации от разглашения
ж) защита информации от утечки
з) защита информации от несанкционированного доступа
и) защита информации от несанкционированного воздействия
к) защита информации от непреднамеренного воздействия

4. Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

е) информации защита информации от разглашения
ж) защита информации от утечки
з) защита информации от несанкционированного доступа
и) защита информации от несанкционированного воздействия
к) защита информации от непреднамеренного воздействия

5. Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации это:

е) информации защита информации от разглашения
ж) защита информации от утечки
з) защита информации от несанкционированного доступа
и) защита информации от несанкционированного воздействия
к) защита информации от непреднамеренного воздействия

Ключи: 1 б), 2 а), 3 в), 4 г), 5 д).

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

1. Классификация криптографических протоколов.
2. Классификация компьютерных атак.

3. Основные механизмы защиты компьютерной сети.
4. Основные средства защиты компьютерной сети.
5. Типовые атаки на криптографические протоколы.
6. Пример криптографического протокола идентификации.
7. Пример криптографического протокола распределения ключей
8. Пример атаки на протокол идентификации.
9. Пример атаки на протокол распределения ключей.
10. Несанкционированные операции с информацией.
11. Источники и классификация угроз безопасности информации.
12. Типовые непреднамеренные искусственные угрозы.
13. Типовые преднамеренные искусственные угрозы.
14. Классификация способов несанкционированного доступа.
15. Типовые атаки на коммуникационные протоколы.
16. Законодательные меры противодействия угрозам безопасности.
17. Организационные меры противодействия угрозам безопасности.
18. Физические и технические меры противодействия угрозам безопасности.
19. Идентификация, аутентификация, авторизация.
20. Протоколирование и аудит (активный аудит).
21. Логическое управление доступом.
22. Защита межсетевого взаимодействия.

Информация о разработчиках

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, кафедра компьютерной безопасности, доцент