ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование
дисциплины (модуля): **Криптографические протоколы**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Никишова А. В., кандидат технических наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - Целью освоения дисциплины является формирование теоретическа и практическая подготовка выпускника в области защиты информации с помощью криптографических протоколов.

Задачи дисциплины:

- изучение теоретических основ криптографических протоколов;
- изучение теоретических основ решения задач аутентификации пользователей, распределения ключей, обеспечения неотрекаемости и анонимности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Криптографические протоколы» относится к обязательной части учебного плана.

Дисциплина изучается на 5 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Студент должен уметь:

использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Студент должен владеть навыками:

навыками и методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Девятый семестр
Контактная работа (всего)	**80**	**80**
Лабораторные	32	32
Лекции	32	32
Практические	16	16
Самостоятельная работа (всего)	**64**	**64**
Виды промежуточной аттестации	**36**	**36**
Экзамен	36	36
Общая трудоемкость часы	**180**	**180**
Общая трудоемкость зачетные единицы	**5**	**5**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (32 ч.)

Девятый семестр. (32 ч.)

Тема 1. Криптографические протоколы (2 ч.)

Понятие протокола и его основные характеристики. Понятие криптографического протокола. Свойства безопасных криптографических протоколов. Применение криптографических протоколов для обеспечения информационной безопасности. Классификация криптографических протоколов.

Тема 2. Безопасность криптографических протоколов (2 ч.)

Основные виды уязвимостей и атак на криптографические протоколы, защитные меры. Подходы к оценке безопасности криптографических протоколов.

Тема 3. Протоколы передачи сообщений (2 ч.)

Криптографический протокол передачи сообщений с обеспечением свойства целостности. Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности. Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.

Тема 4. Протоколы передачи сообщений (2 ч.)

Криптографический протокол передачи сообщений с обеспечением свойства целостности. Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности. Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.

Тема 5. Протоколы аутентификации. (2 ч.)

Понятия идентификации и аутентификации. Слабая и сильная аутентификация. Односторонняя и двухсторонняя аутентификация.

Тема 6. Протоколы аутентификации. (2 ч.)

Слабая аутентификация на основе фиксированных паролей. Атаки на фиксированные пароли. Правила составления паролей. Методы хранения паролей в системах. Схемы использования паролей.

Тема 7. Протоколы аутентификации. (2 ч.)

Сильная аутентификация типа «запрос-ответ» и «рукопожатия». «Запрос-ответ» на основе симметричных и асимметричных алгоритмов шифрования.

Тема 8. Протоколы аутентификации. (2 ч.)

Протоколы аутентификации, использующие цифровую подпись. Протоколы идентификации, использующие технику доказательства знания.

Тема 9. Протоколы распределения ключей. (2 ч.)

Типы протоколов распределения ключей: протоколы обмена ключей, протоколы открытого распределения ключей и схемы предварительного распределения ключей.

Тема 10. Протоколы передачи ключей с использованием симметричного шифрования. (2 ч.)

Двусторонние протоколы передачи ключей с использованием симметричного шифрования. Протоколы типа «запрос-ответ» и его модификации.

Тема 11. Использование односторонней функции. (2 ч.)

«Бесключевой» протокол Шамира и его модификации.

Тема 12. Трехсторонние протоколы. (2 ч.)

Виды и атаки. Протоколы широкоротой лягушки, Yahalom, Нидхейма-Шредера, Отвей-Риса, Kerberos и их модификации.

Тема 13. Использование асимметричного шифрования. (2 ч.)

Использование асимметричного шифрования для передачи ключей симметричных криптосистем.

Тема 14. Протоколы без использования цифровой подписи. (2 ч.)

Одношаговый протокол, протокол NSPK, протокол Woo-Lam. Смешанные протоколы.

Тема 15. Использование цифровой подписи. (2 ч.)

Сертификаты открытых ключей. Открытое распределение ключей и его отличие от распределения открытых ключей.

Тема 16. Понятие безопасного аутентификационного протокола обмена ключами. (2 ч.)

Протокол Диффи-Хеллмана, его достоинства и недостатки. Атака «человек посередине» и методы защиты от неё.

5.2. Содержание дисциплины: Лабораторные (32 ч.)

Девятый семестр. (32 ч.)

Тема 1. Протоколы идентификации, использующие пароли. (2 ч.)

Тема 2. Протоколы идентификации, использующие пароли. (2 ч.)

Тема 3. Протоколы сильной аутентификации. (2 ч.)

Тема 4. Протоколы сильной аутентификации. (2 ч.)

Тема 5. Протоколы идентификации, использующие технику доказательства знания. (2 ч.)

Тема 6. Протоколы идентификации, использующие технику доказательства знания. (2 ч.)

Тема 7. Протоколы передачи ключей с использованием симметричного шифрования. (2 ч.)

Тема 8. Протоколы передачи ключей с использованием симметричного шифрования. (2 ч.)

Тема 9. Протоколы передачи ключей с использованием асимметричного шифрования. (2 ч.)

Тема 10. Протоколы передачи ключей с использованием асимметричного шифрования. (2 ч.)

Тема 11. Схемы предварительного распределения ключей. (2 ч.)

Тема 12. Схемы предварительного распределения ключей. (2 ч.)

Тема 13. Протокол распределения ключей Диффи-Хеллмана. (2 ч.)

Тема 14. Протокол распределения ключей Диффи-Хеллмана. (2 ч.)

Тема 15. Изучение средств настройки протокола IPSEC. (2 ч.)

Тема 16. Изучение средств настройки протокола IPSEC. (2 ч.)

5.3. Содержание дисциплины: Практические (16 ч.)

Девятый семестр. (16 ч.)

Тема 1. Аутентифицированные протоколы. (2 ч.)

Предварительное распределение ключей. Проблема предварительного распределения ключей.

Тема 2. Схемы разделения секрета. (2 ч.)

Свойства схем предварительного распределения ключей. Примеры схем предварительного распределения ключей между n абонентами. Схемы разделения секрета.

Тема 3. Модели криптографических протоколов. (2 ч.)

Сложность криптографических алгоритмов (теорема Кука, NP-полнота).

Тема 4. Криптографические протоколы. (2 ч.)

Протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы.

Тема 5. Протоколы установления подлинности. (2 ч.)

Парольные системы разграничения доступа и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и ЭЦП.

Тема 6. Протоколы управления ключами. (2 ч.)

Протоколы сертификации ключей. Протоколы распределения ключей. Протоколы Oakley, ISAKMP.

Тема 7. Удостоверяющие центры. (2 ч.)

Основные понятия. Виды удостоверяющих центров. Типовая схема построения многоуровневых удостоверяющих центров.

Тема 8. Криптографические протоколы электронных платёжных систем. (2 ч.)

Свойства неотслеживаемости и несвязываемости. Протоколы битовых обязательств. Автономные схемы электронных платежей.

6. Виды самостоятельной работы студентов по дисциплине

Девятый семестр (64 ч.)

Вид СРС: Подготовка рефератов (34 ч.)

Тематика заданий СРС:

Тематика рефератов:

1. Атаки на протоколы обмена ключами.
2. Атаки на хэш-функции.
3. Атаки на протоколы аутентификации.
4. Протокол Wide-Mouth Frog.
5. Протокол Yahalom.
6. Протокол Kerberos.

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.

Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.

Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.

Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.

Структура реферата.

1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.

При проверке реферата оцениваются:

- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Вид СРС: Подготовка презентации на заданную тему (30 ч.)

Тематика заданий СРС:

Тематика презентаций:

1. История криптографии.

2. Протоколы односторонней аутентификации.
3. Протоколы двусторонней аутентификации.
4. Криптосистемы RSA и Эль-Гамаля.
5. Криптографические хэш-функции.
6. Электронная цифровая подпись.

Мультимедийная (электронная/учебная) презентация - это логически связанная последовательность слайдов, объединенных одной тематикой и общими принципами оформления. Мультимедийная презентация представляет сочетание компьютерной анимации, графики, видео, музыки и звукового ряда, которые организованы в единую среду. Чаще всего демонстрация презентации проецируется на большом экране, реже - раздается собравшимся как печатный материал.
Алгоритм самостоятельной работы по подготовке презентации на заданную тему:
1) Ознакомьтесь е предлагаемыми темами презентаций.
2) Ознакомьтесь со списком рекомендуемой литературы и источников и подготовьте их для работы.
3) Повторите лекционный материал по теме презентации (при наличии).
4) Изучите материал, касающийся темы презентации не менее чем по двум-трём рекомендованным источникам.
5) Составьте план-сценарий презентации, запишите его.
6) Проработайте найденный материал, выбирая только то, что раскрывает пункты плана презентации.
7) Составьте, наберите на компьютере и распечатайте текст своего устного выступления. При защите презентации он и будет являться сценарием презентации.
8) Продумайте дизайн презентации.
9) Подготовьте медиафрагменты (аудио-, видеоматериалы, текст и т.п.)
10) Оформите презентацию в соответствии с рекомендациями. Обязательно учтите возможные типичные ошибки и постарайтесь избежать их при создании своей презентации. Внимательно проверьте текст на отсутствие ошибок и опечаток.
11) Проверьте на работоспособность все элементы презентации.
12) Прочтите текст своего выступления медленно вслух, стараясь запомнить информацию.
13) Восстановите последовательность изложения текста сообщения, пересказав его устно.
14) Еще раз устно проговорите своё выступление в соответствии с планом, теперь уже сопровождая своё выступление демонстрацией слайдов па компьютере, делая в тексте пометки в тех местах, где нужна смена слайда.
15) Будьте готовы ответить на вопросы аудитории по теме Вашего сообщения.
К критериям оценки самостоятельной работы по подготовке презентации относятся:
Критерии оценки содержания презентации:
- соответствие материала презентации заданной теме;
- грамотное использование терминологии;
- обоснованное применение эффектов визуализации и анимации;
- общая грамотность;
- логичность изложения материала, доказательность, аргументированность.
Критерии оценки оформления презентации:
- творческий подход к оформлению презентации;
- прослеживается обоснованная последовательность слайдов и информации на слайдах;
- необходимое и достаточное количество фото- и видеоматериалов, учет особенностей восприятия графической (иллюстративной) информации, корректное сочетание фона и графики;
- дизайн презентации не противоречит ее содержанию;
- грамотное соотнесение устного выступления и компьютерного сопровождения, общее впечатление от мультимедийной презентации.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели

Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Студент должен знать:

основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Вопросы, задания:

1. Основные виды уязвимостей криптографических протоколов.
2. Атаки на криптографические протоколы, защитные меры.
3. Свойства безопасных криптографических протоколов.

Студент должен уметь:

использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Задания:

1. Схемы разделения секрета. Примеры схем предварительного распределения ключей между n абонентами.
2. Протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы.
3. Типовая схема построения многоуровневых удостоверяющих центров.

Студент должен владеть навыками:

навыками и методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Задания:

1. Протоколы передачи ключей с использованием симметричного шифрования.
2. Протокол распределения ключей Диффи-Хеллмана.
3. Средства настройки протокола IPSEC.

8.3. Вопросы промежуточной аттестации

Девятый семестр (Экзамен)

1. Понятие криптографического протокола.
2. Свойства безопасных криптографических протоколов.
3. Классификация криптографических протоколов.
4. Основные виды уязвимостей и атак на криптографические протоколы, защитные меры.
5. Криптографический протокол передачи сообщений с обеспечением свойства целостности.

6. Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности.

7. Понятия идентификации и аутентификации.

8. Слабая и сильная аутентификация.

9. Односторонняя и двухсторонняя аутентификация.

10. Слабая аутентификация на основе фиксированных паролей.

11. Сильная аутентификация типа «запрос-ответ» и «рукопожатия».

12. Типы протоколов распределения ключей.

13. Двусторонние протоколы передачи ключей с использованием симметричного шифрования.

14. «Бесключевой» протокол Шамира и его модификации.

15. Трехсторонние протоколы.

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Девятый семестр

1. Контрольная работа - от 0 до 30 баллов
2. Устный опрос, собеседование - от 0 до 10 баллов
3. Письменные задания или лабораторные работы - от 0 до 60 баллов
4. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Ищукова Е. А. Криптографические протоколы и стандарты [Электронный ресурс]: учебное - Южный федеральный университет, 2016. - Режим доступа: https://biblioclub.ru/index.php?page=book&id=493059

2. Бабаш Александр Владимирович Криптографические методы защиты информации [Электронный ресурс]: учебное - Издание 2 - РИОР, 2018. - 413 с. - Режим доступа: http://new.znanium.com/go.php?id=960001

3. Лапонина, О. Р. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия: учебное - Изд-во ИНТУИТ, 2005. - 606 с.

9.2 Дополнительная литература

1. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум +CD [Электронный ресурс]: учебное - КноРус, 2017. - Режим доступа: http://www.book.ru/book/920017

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru/ - Научная электронная библиотека

2. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю

3. http://www.garant.ru/ - Гарант

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:
- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Программное обеспечение:
1. Microsoft Windows 7 Professional, 11 лицензий, номер 60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
5. Microsoft Office 2016, 1 лицензия, Сублицензионный договор No 31604241628 от 21.11.16
6. LibreOffice 12 лицензий (свободно-распространяемое программное обеспечение)

7. FreeBSD, 1 лицензия FreeBSD license свободное программное обеспечение
8. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное программное обеспечение
9. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL) свободное программное обеспечение
10. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение
11. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы (обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/
Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
3. парта со скамьей – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.

Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1

Учебная аудитория для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. парта со скамьей – 40 шт.
2. учебные места – 80 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, меловая)
2. Мультимедийное оборудование

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.