МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Криптографические протоколы и стандарты»

Направление подготовки (специальность) 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки 01.12.2016 г. №1509.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Кандидат физико-математических наук, доцент _____ С.В. Сейфуллина

ОБСУЖДЕНО:
на заседании кафедры МиАОИС 30 «августа» 2017 г., протокол № 1

заведующий кафедрой _____ Д. В. Ильин

СОГЛАСОВАНО:

Методическая комиссия ИВТ 30 «августа» 2017 г., протокол № 1

Декан факультета _____ А. В. Щипцова

Директор научной библиотеки _____ Н. Д. Никитина

Начальник управления информатизации _____ И. П. Пивоваров

Начальник учебно-методического управления _____ В. И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Цель - ознакомление слушателей с существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Основными задачами дисциплины являются: получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, основных уязвимостях протоколов.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина относится к базовой части образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Алгебра и геометрия», «Языки программирования», «Информатика», «Дискретная математика», «Структуры и алгоритмы компьютерной обработки данных», «Криптографические методы защиты информации.

Дисциплина является предшествующей для прохождения преддипломной практики, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- как формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям (З1);
- криптографические стандарты (З2);
- типовые криптографические протоколы и основные требования к ним (З3);
- принципы построения криптографических хеш-функций (З4);
- основные схемы цифровой подписи (З5);
- протоколы идентификации (З7);
- протоколы передачи и распределения ключей (З8);

уметь:

- использовать симметричные и асимметричные шифры системы для построения криптографических протоколов (У1);
- формулировать свойства безопасности криптографических протоколов (У2);

– проводить сравнительный анализ криптографических протоколов, решающих сходные задачи (У3);

владеть навыками:

– программной реализации криптографических протоколов (Н1);
– оценки эффективности протокола (Н2);
– подходов к анализу безопасности криптографических протоколов (Н3).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (практические занятия, лабораторные работы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Модуль 1. Примитивные протоколы.	ОПК-6, ПК-16, ПК-19 ПСК-4.3	З1-З8, У1-У3, Н1-Н3
Модуль 2. Идентификация и сделки.		
Модуль 3. Управление ключами и прикладные протоколы.		
Зачет, РГР	ОПК-6, ПК-16, ПК-19 ПСК-4.3	З1-З8, У1-У3, Н1-Н3
Экзамен	ОПК-6, ПК-16, ПК-19 ПСК-4.3	З1-З8, У1-У3, Н1-Н3

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Модуль 1. Примитивные протоколы.								
Тема 1. Основные понятия.	3	1				2		
Тема 2. Привязка к биту и электронная жеребьевка.	11	1	2	4		4	4	
Тема 3. Разделение секрета.	12	2	2	4		4	4	
Модуль 2. Идентификация и сделки.								
Тема 4. Идентификация и аутентификация.	13	2	2	4		5	4	
Тема 5. Протоколы идентификации с нулевым разглашением.	13	2	2	4		5	4	
Тема 6. Протоколы открытых сделок.	13	2	2	4		5	4	
Модуль 3. Управление ключами и прикладные протоколы.								

Тема 7. Инфраструктура открытых ключей.	13	2	2	4		5	4	
Тема 8. Управление ключами.	12	2	2	4		4	4	
Тема 9. Прикладные протоколы.	12	2	2	4		4	4	
РГР	4					4		
Зачет	2				2			
Экзамен	36							36
Итого	144 4з.е.	16	16	32	2	42	32	36

5. Содержание разделов дисциплины

5.1. Лекции

Модуль 1. Примитивные протоколы.

Тема 1. Основные понятия.

Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов

Тема 2. Привязка к биту и электронная жеребьевка.

Вычислительная и безусловная связанность, секретность. Блоб. Протоколы привязки к биту на основе проблемы дискретного логарифмирования, на основе симметричной криптосистемы, на основе односторонней функции, односторонней перестановки.

Тема 3. Разделение секрета.

Понятие схемы разделения секрета (СРС). Группа доступа. Структура доступа. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках. Разделение секрета для произвольной группы доступа. Совершенная СРС. Идеальное разделение секрета. Проверяемое разделение секрета. Протоколы конфиденциальных вычислений. Пример для схемы Шамира.

Модуль 2. Идентификация и сделки.

Тема 4. Идентификация и аутентификация.

Понятие об идентификации. Классификация схем идентификации и аутентификации. Парольные схемы. Разновидности парольных схем. Требования к парольным схемам. Использование хэш-функций в парольных схемах. Одноразовые пароли. Схема Лампорта. Протоколы рукопожатия. Требования к протоколам рукопожатия. Область применения протоколов рукопожатия.

Тема 5. Протоколы идентификации с нулевым разглашением.

Понятие об интерактивных системах доказательства (ИСД). Примеры ИСД (квадратичные невычеты; неизоморфизм графов). Примеры ИСД с нулевым разглашением (изоморфизм графов). Вопросы реализации ИСД. Нулевое разглашение при параллельной композиции раундов. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Схема Шнорра. Схема Брикелла-МакКарли. Схема Окамото и теорема о ее условной стойкости. Схема Гиллу- Кискатр. Доказательства полноты и корректности этих схем.

Тема 6. Протоколы открытых сделок.

Слепая подпись. Затемненная подпись. Применение слепых подписей. Скрытый канал. Подписи со скрытым каналом. Скрытый канал на основе подписи Онга-Шнорра-Шамира. Подход к построению скрытого канала. Подписи, свободные от скрытого канала.

Покер по телефону. Электронная монета и электронные платежи. Протоколы голосования. Протоколы установления подлинности.

Модуль 3. Управление ключами и прикладные протоколы.

Тема 7. Инфраструктура открытых ключей.

Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа.

Тема 8. Управление ключами.

Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. Схемы Wide-Mouth Frog, Yahalom, протокол Нидхема-Шредера, Отвея-Рииса. Бесключевой протокол Шамира. Протокол Диффи-Хэллмана. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Протокол Kerberos.

Тема 9. Прикладные протоколы.

Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации.

5.2. Темы лабораторных и практических работ

Модуль 1. Примитивные протоколы.

Тема 1: Основные понятия.

1. Анализ безопасности простейших протоколов. Классификация атак.

2. Анализ протоколов цифровых подписей. Анализ DSA и ГОСТ.

Тема 2: Привязка к биту и электронная жеребьевка.

3. Компьютерная реализация схем электронной жеребьевки и привязки к биту.

Тема 3: Разделение секрета.

4. Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа.

5. Проверяемое разделение секрета и конфиденциальные вычисления. 10 Модуль 2. Идентификация и сделки.

Тема 4: Идентификация и аутентификация.

6. Парольные схемы. Одноразовые пароли.

7. Схемы рукопожатия.

Тема 5: Протоколы идентификации с нулевым разглашением.

8. Интерактивные системы доказательства.

9. Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.

Тема 6: Протоколы открытых сделок.

10. Компьютерная реализация схем слепой подписи и скрытого канала. Компьютерная реализация протокола «Покер по телефону» для 3-х игроков.

11. Имитационное моделирование схемы электронных денег с монетами одинакового достоинства.

Модуль 3. Управление ключами и прикладные протоколы.

Тема 7: Инфраструктура открытых ключей.

12. Изучение работы с удостоверяющим центром при помощи CryptoPro.

13. Формирование и проверка сертификата с использованием CryptoPro. Тема 8: Управление ключами.

14. Компьютерная реализация протокола передачи секретного ключа через доверенный центр (работа в группах).

15. Компьютерная реализация протокола передачи секретного ключа средствами асимметричной криптографии(работа в группах).

Тема 9: Прикладные протоколы.

16. Протоколы семейства KriptoKnight для различных сетевых конфигураций и условий применения.

17. Протоколы семейства IPSec.

18. Протоколы семейства SSL/TLS.

5.3. Вопросы для самостоятельной работы студента.

1. Применение привязки к биту и электронной жеребьевки для совместной выработки ключей.
2. Применение схем разделения секрета для безопасной отправки сообщений и депонирования ключей.
3. Идентификация и аутентификация в ОС Windows и Unix.
4. Разновидности цифровых подписей в электронном документообороте.
5. Схемы электронных денег WebMoney и payCash. f. Схемы электронных денег eCash и PayCash.
6. Криптографические средства в электронном документообороте федеральных и местных органов управления в РФ.
7. Системы управления криптографическими ключами в федеральных и местных органах управления в РФ.
8. Обзор криптографических протоколов, использующих цифровую подпись.
9. Практика электронного голосования на примере ЕС.
10. Применение протокола «Покер по телефону» к раздаче электронных бланков.
11. Идентификация на основе биометрических данных

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся;

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;

– практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-

исследовательский характер: аннотирование и конспектирование литературы по теме, составление вопросов и тестов к теме.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета и экзамена. Принимается зачет и экзамен преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы.
2. Понятие о криптографических протоколах. Полнота и корректность.
3. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.
4. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.
5. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.
6. Протоколы привязки к биту. Блоб.
7. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.
8. Совершенная СРС (система разделения доступа), идеальная СРС.
9. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.
10. Схема Блэкли. Вопрос о ее совершенности и идеальности.
11. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.
12. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.
13. Протоколы конфиденциальных вычислений.
14. Проверяемое разделение секрета.
15. Протоколы идентификации. Классификация. Требования.
16. Парольные схемы. Разновидности. Область применения.
17. Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».
18. Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».
19. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.
20. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.
21. Схема идентификации Окамото и теорема о ее условной стойкости.
22. Схема Гиллу-Кискатр. Ее полнота и корректность.
23. Слепая подпись.

24. Скрытый канал.
25. Протокол «Покер по телефону».
26. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.
27. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Разного достоинства. Схема с копилкой.
28. Протоколы голосования.
29. Протоколы установления подлинности.
30. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.
31. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.
32. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.
33. Схемы Wide-Mouth Frog, Yahalom. Их анализ.
34. Протокол Нидхема-Шредера. Его анализ.
35. Протокол Отвея-Рииса. Его анализ.
36. Бесключевой протокол Шамира и атака «Человек посередине».
37. Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.
38. Протокол Нидхема-Шредера на основе шифра с открытым ключом.
39. Широковещательное распределение ключей.
40. Стандарт x.509. 18 41. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров.

Оценивание результатов зачета.

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания и лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно» (п.2.1). Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания и лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

7.2 Вопросы к экзамену

1. Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы.
2. Понятие о криптографических протоколах. Полнота и корректность.
3. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.
4. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.
5. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.
6. Протоколы привязки к биту. Блоб.
7. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.
8. Совершенная СРС (система разделения доступа), идеальная СРС.

9. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.
10. Схема Блэкли. Вопрос о ее совершенности и идеальности.
11. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.
12. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.
13. Протоколы конфиденциальных вычислений.
14. Проверяемое разделение секрета.
15. Протоколы идентификации. Классификация. Требования.
16. Парольные схемы. Разновидности. Область применения.
17. Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».
18. Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».
19. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.
20. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.
21. Схема идентификации Окамото и теорема о ее условной стойкости.
22. Схема Гиллу-Кискатр. Ее полнота и корректность.
23. Слепая подпись.
24. Скрытый канал.
25. Протокол «Покер по телефону».
26. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.
27. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Разного достоинства. Схема с копилкой.
28. Протоколы голосования.
29. Протоколы установления подлинности.
30. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.
31. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.
32. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.
33. Схемы Wide-Mouth Frog, Yahalom. Их анализ.
34. Протокол Нидхема-Шредера. Его анализ.
35. Протокол Отвея-Рииса. Его анализ.
36. Бесключевой протокол Шамира и атака «Человек посередине».
37. Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.
38. Протокол Нидхема-Шредера на основе шифра с открытым ключом.
39. Широковещательное распределение ключей.
40. Стандарт x.509. 18 41. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров.

Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме

пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия: учебное пособие / Лапонина О.Р., О.Р. Лапонина - Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 242 c.. - http://www.iprbookshop.ru/52217.html
2.	Петров А.А. Компьютерная безопасность. Криптографические методы защиты: монография / Петров А.А., А.А. Петров - Компьютерная безопасность. Криптографические методы защиты - Саратов: Профобразование, 2017. - 446 c.http://www.iprbookshop.ru/63800.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Отрыванкина Т. М. Криптографические свойства булевых функций: учебно-методическое пособие / Благовисная А. Н., Отрыванкина Т. М. - Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014. - 55c.. - ISBN.http://www.iprbookshop.ru/51536.html
2.	Лось Алексей Борисович Криптографические методы защиты информации: Учебник / Алексей Борисович, Лось А.Б., Лось Алексей Борисович, Нестеренко А.Ю., Рожков М.И. - 2-е изд. - М.: Юрайт, 2018. - 473 - (Бакалавр. Академический курс). http://www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A

Нормативные правовые и методические документы в области защиты информации доступны по ссылке https://fstec.ru/component/tags/tag/informatsionnoe-soobshchenie

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания

1.	MS Windows/CentOS	лицензия университета/ свободное лицензионное соглашение (https://www.centos.org/download/)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Российская Государственная Библиотека	http://www.rsl.ru
2.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
3.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
4.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
5.	Научная электронная библиотека	http://elibrary.ru
6.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
7.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением;

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях: фронтальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.

Лист актуализации

№ п/п	Наименование документа	Решение кафедры		Подпись	Должность, ФИО
		Дата	протокол №		