МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Криптографические протоколы

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины «Криптографические протоколы» является приобретение обучающимися теоретических и практических навыков анализа и синтеза криптографических протоколов. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных технологий защиты информации.

Задачи дисциплины:

- изучение основных свойств, характеризующих защищенность криптографических протоколов, и основных механизмов, применяемых для обеспечения выполнения того или иного свойства безопасности протокола;
- приобретение навыков анализа безопасности криптографических протоколов;
- приобретение практических навыков работы с математическим аппаратом, применяемым для построения и анализа криптографических протоколов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические протоколы» относится к обязательной части образовательной программы.

Для освоения данной дисциплиной обучающиеся должны владеть математическим аппаратом алгебры, теории чисел, теории вероятностей и математической статистики, знать основные алгебраические структуры (кольца вычетов, группы точек на эллиптических кривых, кольца многочленов) и их свойства, знать и уметь осуществлять программную реализацию алгоритмов проверки чисел на простоту и факторизации чисел, генерации больших простых чисел, иметь представление о криптографических стандартах.

Для успешного освоения дисциплины «Криптографические протоколы» ей должны предшествовать следующие дисциплины:

«Алгебра»;
«Алгебраическая алгоритмика»;
«Теория чисел»;
«Теория вероятностей и математическая статистика»;
«Методы и средства криптографической защиты информации»;
«Теоретико-числовые методы в криптографии»;
«Методы программирования».

Полученные в курсе «Криптографические протоколы» знания необходимы для изучения дисциплин «Математические методы защиты банковской информации» и «Информационная безопасность электронного бизнеса», «Защита программ и данных».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	И-ОПК-2.1 знает типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности, в том числе технологии распределенного реестра	Знает: - основные атак на криптографические протоколы и методы противодействия им;
	И-ОПК-2.2 умеет применять выбранные программные средства системного и прикладного назначений для решения задач профессиональной деятельности	Умеет: - выбирать и при необходимости реализовывать криптографические протоколы при решении типовых задач.
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	И-ОПК-3.5. Знает необходимые математические методы для решения задач обеспечения защиты информации.	Знает: - основные схемы цифровой подписи; - протоколы идентификации; - протоколы передачи и распределения ключей.
	И-ОПК-3.6. Уметь: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации	Умеет: - реализовывать основные криптографические протоколы.
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации,	И-ОПК-10.3 знает методику оценки безопасности криптографических протоколов	Знает: - методику оценки безопасности криптографических алгоритмов, в том числе их полноты, корректности и нулевого разглашения.

использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	И-ОПК-10.4 умеет проводить сравнительный анализ криптографических протоколов, решающих сходные задачи	Умеет: - проводить сравнительный анализ криптографических протоколов, решающих сходные задачи по уровню безопасности и вычислительной сложности.
ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	И-ОПК-2.1_4 знает способы эффективной реализации алгоритмов	Знает: - способы эффективной реализации криптографических протоколов, в том числе применяемых для их реализации алгебраических структур.
	И-ОПК-2.1_2 Способен разрабатывать алгоритмы, используемые в современных математических методах защиты информации	Владеть навыками: - выбора и разработки криптографических протоколов при решении типовых задач.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**						**Формы текущего контроля успеваемости** **Форма промежуточной аттестации** ***(по семестрам)***
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Введение	8	1						
2	Свойства безопасности	8	1						
3	Основные атаки на криптографические протоколы	8	1						

4	Криптографические хеш-функции	8	2	4		2		10	Задания для самостоятельной работы
5	Коды аутентификации	8	2					10	Задания для самостоятельной работы
6	Схемы цифровых подписей	8	4	4		2		10	Задания для самостоятельной работы. Контрольная работа
7	Протоколы идентификации-аутентификации, использующие пароли	8	1	4					
8	Протоколы идентификации-аутентификации, использующие технику «запрос-ответ»	8	2	4					
9	Протоколы идентификации, использующие технику доказательства знания	8	4	4		1		10	Задания для самостоятельной работы
10	Протоколы с нулевым разглашением	8	4	4		1		10	Задания для самостоятельной работы
11	Протоколы передачи ключей с использованием симметричного шифрования	8	2						
12	Протоколы передачи ключей с использованием асимметричного шифрования	8	2						
13	Протоколы открытого распределения ключей	8	2	4		1		10	Задания для самостоятельной работы
14	Протоколы предварительного распределения ключей	8	4	4		1		12	Задания для самостоятельной работы
						2	**0,5**	**33,5**	Экзамен
	ИТОГО		**32**	**32**		**10**	**0,5**	**105,5**	

Содержание разделов дисциплины

Тема № 1: Введение.

Цели и задачи дисциплины «Криптографические протоколы». Ее место и роль при подготовке специалистов по компьютерной безопасности, связь с другими дисциплинами.

Коммуникационный и криптографический протоколы, раунд протокола, шаг протокола. Виды криптографических протоколов. Современное состояние и перспективные направления исследований по тематике дисциплины.

Тема № 2: Свойства безопасности.
Свойства, характеризующие безопасность протоколов: нешироковещательная аутентификация; аутентификация при рассылке по многим адресам или при подключении к службе подписки; свойства совместной генерации ключа; конфиденциальность; анонимность; ограниченная защищенность от атак типа «отказ в обслуживании»; инвариантность отправителя; невозможность отказа от ранее совершенных действий; безопасное временное свойство; формирование сеанса; последовательное представление; именование ключей.

Тема № 3: Основные атаки на криптографические протоколы.
Основные атаки на безопасность протоколов: подмена; повторное навязывание сообщения; отражение; задержка передачи сообщения; комбинированная атака, атака с параллельными сеансами; атака с использованием специально подобранных текстов; атака «человек по середине»; атака с известным сеансовым ключом; атака с неизвестным общим ключом; подмена открытого ключа.

Тема № 4: Криптографические хеш-функции.
Определение хеш-функции. Целостность данных и аутентификация сообщений. Криптографические хеш-функции. Одношаговые сжимающие функции. Хеш-функции, задаваемые ключом. Свойства хеш-функций, задаваемых ключом. Построение хеш-функций, задаваемых ключом на основе бесключевых. Использование хеш-функций, задаваемых ключом, и симметричного шифрования. Хеш-функции, не зависящие от ключа. Свойства хеш-функций, не зависящих от ключа. Семейство алгоритмов MD4. Хеш-функции на основе дискретного логарифмирования.

Тема № 5: Коды аутентификации.
Определение кода аутентификации. Вероятности навязывания. Связь между ортогональными массивами и кодами аутентификации. Характеристика оптимальных кодов аутентификации.

Тема № 6: Схемы цифровых подписей.
Определение и свойства схем цифровых подписей. Инфраструктура открытых ключей. Цифровые подписи на основе систем шифрования с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля, цифровые подписи семейства Эль-Гамаля. Цифровая подпись DSA. Цифровая подпись Шнорра. Цифровые подписи на основе симметричных систем шифрования. Схема цифровой подписи вслепую. Цифровой нотариат.

Тема № 7: Протоколы идентификации-аутентификации, использующие пароли.
Виды протоколов идентификации-аутентификации. Фиксированные пароли. Атаки на фиксированные пароли. Защита от перехвата паролей. Усложнение подбора паролей. Защита базы данных от компрометации. Личные идентификационные номера. Защита от повторного воспроизведения. Одноразовые пароли.

Тема № 8: Протоколы идентификации-аутентификации, использующие технику «запрос-ответ».
Случайные последовательности и метки времени. «Запрос-ответ» с использованием симметричных алгоритмов шифрования. «Запрос-ответ» с использованием асимметричных алгоритмов шифрования. Протоколы идентификации, использующие цифровую подпись.

Тема № 9: Протоколы идентификации, использующие технику доказательства знания.
Протокол идентификации Фиата-Шамира. Протокол идентификации Шнорра. Протокол Окамото. Протокол GQ.

Тема № 10: Протоколы с нулевым разглашением.
Протокол принадлежности подгруппе. Протокол привязки к биту. Протокол подбрасывания монеты по телефону. Схема и протокол Гольдвассера-Микали. Протокол подписания контракта. Сертифицированная цифровая почта. Аргумент с нулевым разглашением. Протокол цифрового голосования.

Тема № 11: Протоколы передачи ключей с использованием симметричного шифрования.
Протокол рукопожатия для процедуры удаленного вызова Remote Procedure Calls (RPC), «бесключевой» протокол Шамира; протокол Wide-Mouth Frog; протокол Yahalom; протокол BAN-Yahalom, протокол Woo-Lam взаимной аутентификации и распределения ключей; протокол NS; протокол Denning-Sacco; протокол Kerberos; протокол Otway-Rees. Семейство протоколов KriptoKnight: Push- и Pull-протоколы 3PAKDP.

Тема № 12: Протоколы передачи ключей с использованием асимметричного шифрования.
Протоколы без использования цифровой подписи: протокол NSPK; протокол Woo-Lam. Смешанные протоколы: протокол EKE, протокол SPX. Протоколы с использованием цифровой подписи. Сертификаты открытых ключей.

Тема № 13: Протоколы открытого распределения ключей.
Виды протоколов открытого распределения ключей и их свойства. Протокол Диффи — Хеллмана и его усиления: протокол DH; статический DH, протоколы MTI. Открытое распределение ключей с использованием самосертифицируемых ключей. Протокол KEA. Протокол «унифицированная модель». Протокол MQV. Аутентифицированные протоколы с применением цифровых подписей: протокол STS; протокол DHKE. Аутентифицированные протоколы с применением хеш-функций, задаваемых ключом: модифицированный протокол STS, протокол «унифицированная модель с подтверждением».

Тема № 14: Протоколы предварительного распределение ключей.
Схемы предварительного распределения ключей в сети связи и их свойства. Схема Блома. Схема KDP. Групповые протоколы: схема разделения секрета, случай единственной группы, пороговая схема. Протоколы установления ключей для конференц-связи. Протокол DH с тремя участниками. Протокол Бурместера-Десмедта.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Лекция-беседа или «диалог с аудиторией», является наиболее распространенной и сравнительно простой формой активного вовлечения студентов в учебный процесс. Эта лекция предполагает непосредственный контакт преподавателя с аудиторией. Преимущество лекции-беседы состоит в том, что она позволяет привлекать внимание студентов к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей студентов.

Лекция с заранее запланированными ошибками – рассчитана на стимулирование студентов к постоянному контролю предлагаемой информации (поиск ошибки: содержательной, методологической, методической). Используется для развития у студентов умения оперативно анализировать профессиональные ситуации, выступать в роли экспертов, оппонентов, рецензентов, вычленять неверную или неточную информацию. Подготовка преподавателя к лекции состоит в том, чтобы заложить в ее содержание определенное количество ошибок содержательного или методического характера. Лектор строит изложение таким образом, чтобы ошибки были тщательно «замаскированы» и их не так-то легко было заметить слушателям. Задача слушателей состоит в том, чтобы по ходу лекции отмечать в конспекте замеченные ошибки, чтобы назвать их в конце лекции. На разбор ошибок отводится 10-15 минут.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение

- Microsoft Visual Studio.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487 (дата обращения: 31.01.2022).

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242 (дата обращения: 31.01.2022).

б) дополнительная литература

1. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие для вузов. / А. В. Черемушкин; УМО по образованию в обл. информационной безопасности - М.: Академия, 2009. - 272 с.

2. Дурнев В. Г. Методы комбинаторной теории групп в современной криптографии [Электронный ресурс]: учеб.-метод. пособие. / В. Г. Дурнев, О. В. Зеткина; Яросл. гос. ун-т. им. П. Г. Демидова - Ярославль: ЯрГУ, 2017. - 49 с. http://www.lib.uniyar.ac.ru/edocs/iuni/20170207.pdf

3. Алферов, А.П. Основы криптографии: Учебное пособие / А.П. Алферов А.П., А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005. – 480 с.

4. Запечников, С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности : учеб. пособие для вузов / С.В. Запечников. – М.: Горячая линия-Телеком, 2007. – 319 с.

в) ресурсы сети «Интернет» (при необходимости)

1. Общероссийский математический портал (http://www.mathnet.ru/).

2. Научная электронная библиотека (http://elibrary.ru).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

Приложение № 1 к рабочей программе дисциплины
«Криптографические протоколы»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

Задания по теме № 4 «Криптографические хеш-функции»

1. Пусть при случайном выборе $x \in X$ значение функции $h: X \to Y$, $|Y| = m$, имеет равномерное распределение. Покажите, что при $r \geq 2$:

1) вероятность r-кратного совпадения значений функции h при попарно различных значениях аргумента равна
$$P(h(x_1) = \ldots = h(x_r) | x_i \neq x_j, 1 \leq i < j \leq r) = \frac{1}{m^{r-1}};$$

2) среднее число r-кратных совпадений значений функции h в выборке с возвращением объема $N_r = c(m^{r-1})^{1/r}, c \geq 1$ равно
$$\left(\frac{N_r}{r}\right)\frac{1}{m^{r-1}} \approx \frac{c^r}{r!}.$$

2. Пусть при случайном выборе x значение $h(x)$ функции $h: \{0,1\}^N \to \{0,1\}^n$ $(3 \leq n \leq N)$ имеет равномерное распределение. Покажите, что в выборке $x_1, x_2, \ldots, x_k$ объемом $k = 2^{\left\lceil \frac{n+1}{2} \right\rceil}$ при независимых испытаниях вероятность p существования коллизии будет не больше ½.

3. Пусть при случайном выборе x значение $h(x)$ функции $h: \{0,1\}^N \to \{0,1\}^n$ $(3 \leq n \leq N)$ имеет равномерное распределение. Покажите, что в выборке $x_1, x_2, \ldots, x_k$ объемом $k = 2^{\left\lfloor \frac{n-t}{2} \right\rfloor}$ $(1 \leq t \leq n)$ при независимых испытаниях вероятность p существования коллизии будет не больше $1/2^{t+1}$.

Задания по теме № 5 «Коды аутентификации»

1. Покажите, что наборы из n^2 троек $(i, j, L(i, j))$, $1 \leq i, j \leq n$, построенные по таблице латинского квадрата L порядка n, задают ортогональный массив OA(n, 3, 1).

2. Два латинских квадрата L_1 и L_2 называют ортогональными, если все пары $(L_1(i, j), L_2(i, j))$ при различных $1 \leq i, j \leq n$ различные. Покажите, что по набору из m попарно ортогональных латинских квадратов порядка n можно построить ортогональный массив OA(n, m + 2, 1).

3. Покажите, что каждый ортогональный массив OA(n, n, 1) можно дополнить до OA(n, n+1, 1).

4. Покажите, как построить ортогональный массив OA(p^m, p^m+1, 1) на основе поля из p^m элементов.

Задания по теме № 6 «Схемы цифровых подписей»

1. Авторство в схеме цифровой подписи RSA. Алиса и Боб претендуют на авторство подписанного сообщения <*M*, 7>. Известно, что открытые ключи Алисы и Боба имеют следующие значения n_A = 55, e_A = 3, n_B = 44, e_B =9, а значение хеш-функции от *M* равно 13. Определите настоящего автора.

2. Авторство в схеме цифровой подписи Эль-Гамаля. Пусть p = 23, g =5 – общие параметры для Алисы и Боба. Алиса и Боб претендуют на авторство подписанного сообщения <*M*, 20, 21>. Определите настоящего автора, если известно, что открытые ключи Алисы и Боба имеют следующие значения p_A = 13, p_B = 17, а значение хеш-функции от *M* равно 3.

Задания по теме № 9 «Протоколы идентификации, использующие технику доказательства знания»

1. Докажите, что если участник A в схеме GQ применяет некачественный генератор случайных чисел для получения числа *r*, приводящий к повторному появлению использованных ранее чисел, то противник может вычислить секретный ключ *u*.

Задания по теме № 10 «Протоколы с нулевым разглашением»

1. Предложите способ, позволяющий модифицировать протокол сертифицированной электронной почты так, чтобы для него выполнялось свойство конфиденциальности.

2. Покажите, что протокол электронного голосования обладает требуемыми свойствами.

3. Сколько нечестных комиссий может участвовать в протоколе электронного голосования, не нарушая его основных свойств?

Задания по теме № 13 «Протоколы открытого распределения ключей»

1. Покажите, что протокол STS может обеспечить аутентификацию сторон, если проводить аутентификацию не только передаваемых сообщений α^x и α^y, но и идентификаторов сторон.

2. Как модифицировать протоколы KEA и MQV, чтобы для них выполнялось свойство взаимного подтверждения правильности получения ключа?

3. Как преобразовать протоколы KEA и «унифицированная модель с подтверждением» в однопроходные с подтверждением правильности получения ключа?

Задания по теме № 14 «Протоколы предварительного распределения ключей»

1. Пусть имеется KDP(n, q)-схема с матрицей инцидентности *A*. Обозначим строки матрицы *A* символами a_1, …, a_n. Покажите, что:

а) матрица A' размера $n^2 \times 3q$, составленная из строк вида $(a_i, a_j, \ldots, a_{i+j})$, где $i, j \in \{1, \ldots, n\}$ и сумма индексов рассматривается по модулю n, является матрицей инцидентности KDP(n^2, $3q$)-схемы;

б) если к матрице инцидентности A' добавить три строки вида

$$0 \ldots 0\ 1 \ldots 1\ 1 \ldots 1$$

$$1 \ldots 1\ 0 \ldots 0\ 1 \ldots 1$$

$$1 \ldots 1\ 1 \ldots 1\ 0 \ldots 0$$

то получится матрица KDP($n^2 + 3$, $3q$)-схемы;

в) Как можно построить KDP(n, q)-схемы с параметрами

n	147	364	787	21 612	132 499	619 372	467 078 547	17 555 985 004	383 621 674 387
q	27	36	45	81	108	135	243	324	405

2. Структура инцидентности называется t-(v, k, λ)-схемой ($1 \le t \le k$), если все блоки инцидентны k точкам и каждые t точек инцидентны λ блокам. Докажите следующие свойства:

а) всякая t-(v, k, λ_t)-схема является (t – 1)-(v, k, λ_{t-1})-схемой, причем

$\lambda_t (v - t + 1) = (k - t + 1)\ \lambda_{t-1}$;

б) если для 3-(v, k, λ_3)-схемы выполнено условие $\lambda_2 > w\lambda_3$, то ей соответствует w -KDP(n, q)-схема;

в) всякой (w + 2)-схеме соответствует w -KDP(n, q)-схема.

Контрольная работа

Вариант № 1.

1. Дайте определение понятию «раунд протокола».
2. Опишите схему цифровой подписи Диффи-Лампорта.

Вариант № 2.

1. Дайте определение понятию «шаг протокола».
2. Опишите схему цифровой подписи DSA.

Вариант № 3.

1. Дайте определение понятию «коммуникационный протокол».
2. Опишите схему цифровой подписи Шнорра.

Вариант № 4.

1. Дайте определение понятию «криптографический протокол».
2. Опишите схему цифровой подписи Эль-Гамаля.

Вариант № 5.

1. Дайте определение понятию «идентификация».
2. Опишите схему цифровой подписи Фиата-Шамира.

Вариант № 6.

1. Дайте определение понятию «аутентификация сеанса».
2. Опишите схему цифровой подписи вслепую.

Вариант № 7.

1. Дайте определение понятию «конфиденциальность».
2. Докажите теорему о вероятностях навязывания.

Вариант № 8.

1. Дайте определение понятию «анонимность».
2. Докажите теорему о связи свойств устойчивости к коллизиям и устойчивости к нахождению второго прообраза хеш-функций.

Вариант № 9.

1. Дайте определение понятию «инвариантность отправителя».
2. Докажите теорему о связи свойств однонаправленности и устойчивости к коллизиям хеш-функций.

Вариант № 10.

1. Дайте определение понятию «криптографическая хеш-функция».
2. Опишите методы противодействия атаке «подмена».

Вариант № 11.

1. Дайте определение понятию «оптимальный код аутентификации».
2. Опишите методы противодействия атаке «повторное навязывание».

Вариант № 12.

1. Дайте определение понятию «ортогональный массив».
2. Опишите методы противодействия атаке «отражение».

Вариант № 13.

1. Дайте определение понятию «цифровая подпись».
2. Опишите методы противодействия атаке «задержка передачи сообщения».

Вариант № 14.

1. Дайте определение понятию «схема цифровой подписи».
2. Опишите методы противодействия атаке с параллельными сеансами.

Вариант № 15.

1. Перечислите основные свойства хеш-функций, не зависящих от ключа.
2. Опишите методы противодействия атаке на основе связывания.

Вариант № 16.

1. Перечислите основные свойства хеш-функций, задаваемых ключом.
2. Опишите методы противодействия атаке с известным сеансовым ключом.

Вариант № 17.

1. Перечислите элементарные свойства ортогональных массивов.
2. Опишите методы использования хеш-функций совместно с симметричным шифрованием.

Вариант № 18.

1. Перечислите основные свойства схем цифровой подписи.
2. Опишите методы построения ключевых функций на основе бесключевых.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену:

1. Основные понятия. Протокол, раунд и шаг протокола. Коммуникационные и криптографические протоколы.
2. Основные понятия. Коммуникационные и криптографические протоколы. Функции безопасности.
3. Свойства безопасности. Аутентификация. Свойства G1 – G5.
4. Свойства безопасности. Авторизация. Свойство G6. Совместная генерация ключа. Свойства G7 – G11.
5. Свойства безопасности. Конфиденциальность. Свойство G12. Анонимность. Свойства G13, G14. Ограниченная защищенность от атак типа «отказ в обслуживании». Свойство G15.
6. Свойства безопасности. Инвариантность отправителя. Свойство G16. Невозможность отказа от ранее совершенных действий. Свойства G17 – G19. Безопасное временное свойство. Свойство G20.
7. Свойства безопасности. Формирование сеанса, последовательное представление, именование ключей.
8. Основные атаки. Подмена, повторное навязывание, атака отражением. Методы противодействия.

9. Основные атаки. Задержка передачи сообщения, комбинированная атака, атака с параллельными сеансами, с использованием специально подобранных текстов. Методы противодействия.
10. Основные атаки. Атака с известным сеансовым ключом, атака с неизвестным общим ключом, атака на основе связывания. Методы противодействия.
11. Понятие хеш-функции, целостность данных и аутентификация сообщений. Криптографические хеш-функции. Отличие обычных хеш-функций от криптографических хеш-функций.
12. Свойства хеш-функций, задаваемых ключом. Свойства хеш-функций, не зависящих от ключа. Одношаговые сжимающие функции. Бесключевые хеш-функции на основе блочных шифров. Построение хеш-функций, задаваемых ключом, на основе бесключевых.
13. Хеш-функции, не зависящие от ключа. Однонаправленность, устойчивость к коллизиям, устойчивость к нахождению второго прообраза. Взаимосвязь свойств. Теоремы об оценках вероятности коллизий.
14. Хеш-функции на основе дискретного логарифмирования. Использование хеш-функций совместно с симметричным шифрованием.
15. Коды аутентификации. Определения и свойства, характеристики. Оптимальные коды. Определение и простейшие свойства ортогональных массивов.
16. Теоремы о существовании ортогональных массивов с определенными параметрами. Связь кодов аутентификации и ортогональных массивов. Теорема Стинсона, 1990.
17. Связь кодов аутентификации и ортогональных массивов. Теорема Стинсона, 1992.
18. Цифровые подписи. Общие положения. Цифровая подпись, схема цифровой подписи, свойства схемы цифровой подписи, сравнение цифровой и собственноручной подписей.
19. Схемы цифровой подписи Фиата-Шамира и метод решения задачи извлечения квадратного корня в конечном поле.
20. Семейство схем цифровых подписей Эль-Гамаля.
21. Схемы цифровой подписи Шнорра и DSA.
22. Схема цифровой подписи Диффи-Лампорта. Схема цифровой подписи вслепую, схема конфиденциальной цифровой подписи, групповой подписи, нотаризация цифровых подписей.
23. Слабость парольных схем и протоколов типа «запрос-ответ». Протоколы идентификации. Интерактивное доказательство, доказательство знания. Полнота, корректность, нулевое разглашение, протокол с нулевым разглашением.
24. Протокол идентификации Фиата-Шамира, полнота, корректность, нулевое разглашение.
25. Протокол идентификации GQ, полнота, корректность, нулевое разглашение. Протокол GQ с ключами, зависящими от идентификаторов.
26. Протокол идентификации Шнорра, полнота, корректность, нулевое разглашение.
27. Протокол идентификации Окамото, корректность.
28. Протокол идентификации Окамото, полнота, нулевое разглашение, устойчивость к компрометации ключа одного из абонентов.
29. Протокол принадлежности подгруппе, полнота, корректность, нулевое разглашение. Протокол привязки к биту, связывание и сокрытие.
30. Протокол подбрасывания монеты по телефону. Схема Гольдвассера-Микали.
31. Протокол электронного голосования A. Cramer, M. Pranclin, B. Shoenmakers, M. Young, 1996.
32. Протоколы передачи ключей. Типы и виды протоколов. Двусторонние протоколы передачи ключей с использованием симметричного шифрования (с двухсторонней аутентификацией, с аутентификацией сеанса, с генерацией ключа путем двухстороннего обмена).

33. Открытое распределение ключей. Их свойства и особенности. Протокол Диффи-Хеллмана. Атака «человек по середине» на протокол.
34. Схемы коррекции протокола DH. Их достоинства и недостатки. Статический DH. Протоколы MTI.
35. Схема Гиролта и протокол KEA (проверка принадлежности подгруппе порядка q). Их достоинства и недостатки.
36. Протокол KEA (проверка принадлежности интервалу [2, p – 1], вариант с использованием хеш-функций).
37. Свойства схем предварительного распределения ключей. Условия и теоремы.
38. Схема предварительного распределения ключей Блома.

Правила выставления оценки на экзамене.

В экзаменационный билет включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом криптографических протоколов; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминов криптографических протоколов, но при этом допускаются ошибки в определениях некоторых основных понятий, формулировках положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении сущности раскрываемых понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие

вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Криптографические протоколы»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Криптографические протоколы» отводится один семестр. В конце семестра в качестве итогового контроля предусмотрен экзамен. В процессе изучения дисциплины проводится одна контрольная работа и выполняется семь домашних заданий. Контрольная работа запланирована после завершения изучения 1/3 материалов дисциплины по темам, изученным к этому времени.

Основной формой изучения учебного материала по дисциплине «Криптографические протоколы» являются практические занятия. Это связано с тем, что основной задачей в рамках дисциплины является получение обучающимся практических навыков работы с особым математическим аппаратом, применяемым для построения и анализа криптографических протоколов.

Для успешного освоения дисциплины очень важна практическая программная реализация большого количества криптографических протоколов и математических объектов и структур, лежащих в их основе. Примеры криптографических протоколов разбираются на лекционных и практических занятиях. Основная цель программной реализации – помочь усвоить основные понятия, дать возможность «поиграть» практически реализованными теоретическими объектами и структурами. Для успешной программной реализации необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

Дополнительную роль при связи теории и практики играют домашние работы. В качестве заданий для самостоятельной работы дома обучающимся предлагаются математические задачи, которые должны позволить студенту переосмыслить изученные на лекциях понятия и методы, применить их для решения типовых задач из соответствующих разделов дисциплины. Решения задач должны быть подготовлены, оформлены в письменном виде и представлены в установленные сроки.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с математическим аппаратом, применяемым для построения и анализа криптографических протоколов, в течение обучения проводятся мероприятия текущей аттестации в виде контрольной работы в 9-ом семестре. Также проводятся консультации (при необходимости) по разбору заданий для контрольной работы, которые вызвали затруднения.

В конце семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Опыт преподавания дисциплины «Криптографические протоколы» говорит о сложности ее самостоятельного изучения для обучающегося, несмотря на наличие достаточно качественных учебных пособий. Обучающиеся, вставшие на путь

самоподготовки, часто неверно расставляют приоритеты при изучении данной дисциплины, что не позволяет им на высоком уровне овладеть изучаемым материалом. Это связано с насыщенностью изучаемого материала и большим числом практических занятий, необходимых для приобретения навыков практического использования изучаемых математических структур и объектов. Поэтому посещение всех аудиторных занятий является настоятельно рекомендуемым.