МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Кубанский государственный университет» (ФГБОУ ВО «КубГУ»)

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

Р А Б О Ч А Я П Р О Г Р А М М А У Ч Е Б Н О Й Д И С Ц И П Л И Н Ы

Б1.В.ДВ.10.01 «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

Направление подготовки/специальность 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) / специализация Вычислительные технологии

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Краснодар 2018

Рабочая программа дисциплины Б1.В.ДВ.10.01 «Криптографические протоколы» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению 02.03.02 Фундаментальная информатика и информационные технологии.

Составитель:

кандидат физико-математических наук, С.А. Жуков
доцент кафедры вычислительных технологий

Рабочая программа дисциплины «Криптографические протоколы» утверждена на заседании кафедры вычислительных технологий № 7 «03» апреля 2018 г.
Заведующий кафедрой (разработчика) __ Миков А.И. ____
фамилия , инициалы подпись

Рабочая программа дисциплины «Криптографические протоколы» обсуждена на заседании кафедры вычислительных технологий протокол № 7 «03» апреля 2018 г.
Заведующий кафедрой (выпускающей) __ Миков А.И. ____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 1 «20» апреля 2018 г.

Председатель УМК факультета К.В. Малыхин

Рецензенты:
Зайков В.П. Ректор НЧОУ ВО “Кубанский институт информзащиты” д. экон. наук, к.т.н., доцент.

Гаркуша Олег Васильевич, доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», канд. физ.-мат. наук.

1. Цели и задачи освоения дисциплины

1.1 Цели освоения дисциплины

Целью преподавания и изучения дисциплины «Криптографические протоколы» является формирование у студентов знаний и навыков по использованию методов согласованного решения задач информационного обмена с использованием криптографии.

1.2 Задачи дисциплины

Студент должен **знать** основные понятия, подходы и методы, используемые в криптографических протоколах; **уметь** применять базовые алгоритмы и стандарты

криптографических протоколов; **владеть** технологиями, способствующими использованию криптографических протоколов.

1.3 Место дисциплины в образовательной программе

Дисциплина «Криптографические протоколы» относится к блоку дисциплин по выбору вариативной части Б1.В.ДВ профессиональных дисциплин.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по информационной безопасности, криптографии и распределенным задачам и алгоритмам.

Знания, получаемые при изучении дисциплины «Криптографические протоколы», могут использоваться при работе над выпускной работой, а также при изучении дисциплин магистерского цикла.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **компетенций:**

№ п.п.	Индекс компе-тенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающие должны		
			знать	уметь	владеть
1.	ПК-4	способностью решать задачи профессиональной деятельности в составе научно-исследователь-ского и производствен-ного коллектива	способы решать задачи профессиональной деятельности	решать задачи профессиональной деятельности в составе научно-исследовательског о и производствен-ного коллектива	способностью решать задачи профессиональной деятельности в составе научно-исследовательского и производствен-ного коллектива
2.	ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	информационно-коммуникационные технологии и основные требования информационной безопасности	решать стандартные задачи профессиональной деятельности на основе информационной и библиографическо й культуры	способами использования криптографических протоколов в области информационных технологий, а также знаниями, которые находятся на передовом рубеже криптографической науки, инструментами

		безопасности			поддерживающими информационную безопасность информационных систем

2. Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 4 зач.ед. (144 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			8	_		
Контактная работа, в том числе:		**54,3**	**54,3**			
Аудиторные занятия (всего):		**48**	**48**			
Занятия лекционного типа		16	16	-	-	-
Лабораторные занятия		32	32	-	-	-
Занятия семинарского типа (семинары, практические занятия)		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		6	6			
Промежуточная аттестация (ИКР)		0,3	0,3			
Самостоятельная работа, в том числе:		**45**	**45**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		36	36	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		9	9	-	-	-
Реферат		-	-	-	-	-
Подготовка к текущему контролю		-	-	-	-	-
Контроль:		**экзамен**	**экзамен**			
Подготовка к экзамену		44,7	44,7	-	-	-
Общая трудоемкость	**час.**	**144**	**144**	-	-	-
	в том числе контактная работа	**54,3**	**54,3**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в _8_ семестре *(очная форма).*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Криптографические протоколы и основные требования	14	2		4	8

2	Протоколы рукопожатия	14	2		4	8
3	Протоколы генерации ключей	20	4		8	8
4	Протоколы идентификации и аутентификации	18	4		8	6
5	Протоколы распределения ключей	13	2		4	7
6	Доказательства с нулевым разглашением секрета	14	2		4	8
7	Подготовка к экзамену	44,7				
8	КСР	6				
9	ИКР	0,3				
	Итого по дисциплине:	**144**	**16**	**–**	**32**	**45**

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Криптографические протоколы и основные требования	Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола	ЛР
2	Протоколы рукопожатия	Протоколы аутентификации “запрос-ответ”, основанные на криптосистемах разных типов: классификация, примеры, стандартизация	ЛР
3	Протоколы генерации ключей	Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”.	ЛР
4	Протоколы идентификации и аутентификации	Классификация протоколов идентификации и аутентификации. Протоколы аутентификации “запрос-ответ”, основанные на разных криптосистемах: классификация, примеры, стандартизация	ЛР
5	Протоколы распределения ключей	Общая классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы.	ЛР
6	Доказательства с нулевым разглашением секрета	Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы	ЛР

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	Наименование лабораторных работ	Форма текущего контроля
1	Производство и применение систем криптографической защиты информации	ЛР
2	Функции органа криптографической защиты информации. Обязанности пользователей СКЗИ.	ЛР
3	Требования к средствам защиты информации используемым в криптопрооколах	ЛР
4	Обязанности пользователей СКЗИ и криптопротоколов	ЛР
5	Функции органа управления СКЗИ и использования криптопротоколов	ЛР
6	Механизмы контроля за организацией и обеспечением безопасности хранения обработки и передачи конфиденциальных данных на основе криптопротоколов	ЛР
7	Іротоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder	ЛР
8	Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол протокол Kerberos	ЛР
9	Протоколы транспортировки ключей, рекомендованные стандартом X.509	ЛР
10	Протокол транспортировки ключей Beller-Yacobi	ЛР
11	Протокол обмена ключами Диффи-Хеллмана, атаки на него	ЛР
12	Іротокол обмена ключами MTI, атаки на него	ЛР
13	Протокол обмена ключами STS	ЛР
14	Каналы защищенной передачи информации: постановка задачи, классификация средств обеспечения конфиденциальности и аутентичности	ЛР
15	Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол Otway-Rees	ЛР
16	Доказательства с нулевым разглашением знаний. Алгоритмы разделения секрета	ЛР

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

3. Образовательные технологии

При проведении занятий по дисциплине используются следующие образовательные технологии:

- технология разноуровневого обучения (дифференцированное обучение);
- технология коллективного взаимодействия (организованный диалог, коллективный способ обучения).

Технология адаптивного обучения (индивидуализированное обучение).

Семестр	Вид занятия (Л, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
8	Л	Компьютерные презентации и обсуждение	16

	ЛР	Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области верификации программных систем, программирование и аннотирование алгоритмов	32
Итого:			48

2.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного материала, выполнение индивидуальных заданий.	Источники основной и дополнительной литературы

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются

- формах, адаптированных к ограничениям их здоровья и восприятия информации: Для лиц с нарушениями зрения:
  – в печатной форме увеличенным шрифтом,
  – в форме электронного документа,

  Для лиц с нарушениями слуха:
  – в печатной форме,
  – в форме электронного документа.
  Для лиц с нарушениями опорно-двигательного аппарата:
  – в печатной форме,
  – в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств итоговой аттестации (экзамен в 8 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на экзамене (для выявления знания и понимания теоретического материала дисциплины и практических навыков).

4.1.1 Примеры типовых заданий

1. Как преобразовать протокол аутентификации запрос-ответ на базе схемы открытого шифрования в протокол аутентичного распределения ключей? Приведите два примера: для протокола односторонней аутентификации и для протокола взаимной аутентификации.

2. Приведите описание процедуры восстановления секрета из схемы разделения секрета Шамира двумя способами: для случая, когда общее число участников равно 3, максимально допустимое количество утраченных (скомпроментированных) долей секрета равно 2, длина разделяемого секрета равно 128 битам.

3. Какими из основных свойств протоколов распределения ключей (неявная аутентификация ключа, подтверждение ключа, явная аутентификация) обладает протокол Kerberos? Какие практические задачи он позволяет решать?

4. Оцените вычислительную сложность (количество выполненных операций) и коммуникационную сложность (количество пересылок сообщений и объем передаваемых данных) протокола доказательства знания дискретного логарифма для каждого участника. Приведите пример такого задания параметров протокола, при котором вероятность обмана доказывающим проверяющего не превысит 2^{-30}.

5. Сравните по стойкости к различным видам атак два метода аутентификации по одноразовым паролям: метод Лэмпорта и последовательно обновляемые одноразовые пароли. Какие выводы о предпочтительности того или иного метода можно сделать?

4.2 Фонд оценочных средств для проведения промежуточной аттестации

4.2.1 Перечень вопросов к экзамену

1. Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола.
2. Критерии оценки стойкости криптографических алгоритмов и протоколов.
3. Характеристики вычислительно сложных задач теории чисел, возможности их применения в ассиметричной криптографии (задача факторизации и производные от нее задачи, задача дискретного логарифмирования и производные от нее задачи).
4. Парные отображения и их свойства. Вычислительно сложные задачи, основанные на парных отображениях.
5. Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”.
6. Интерактивные системы доказательства: цель доказательства, общий принцип построения протокола, свойства полноты и корректности.
7. Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы.
8. Классификация протоколов аутентификации. Атаки на протоколы с фиксированными паролями.
9. Протоколы аутентификации с одноразовыми паролями. Схема Лэмпорта.
10. Протоколы аутентификации “запрос-ответ”, основанные на симметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
11. Протоколы аутентификации “запрос-ответ”, основанные на асимметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
12. Протоколы аутентификации, основанные на доказательствах с нулевым разглашением знаний (на примере проокола Фиата-Шамира).
13. Общая классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК.
14. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы (без центра доверия).

15. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder, протокол Kerberos.
16. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Otway-Rees, атаки на него.
17. Классификация ПРК, основанных на симметричных криптосхемах. Протокол транспортировки ключей Needham-Schroeder с использованием схем открытого шифрования.
18. Протоколы транспортировки ключей, рекомендованные стандартом X.509.
19. Протокол транспортировки ключей Beller-Yacobi.
20. Протокол обмена ключами Диффи-Хеллмана, атаки на него.
21. Протокол обмена ключами MTI, атаки на него.
22. Протокол обмена ключами STS.
23. Каналы защищенной передачи информации: постановка задачи, классификация средств обеспечения конфиденциальности и аутентичности.
24. Криптографические механизмы в спецификации SSH: аутентичное распределение ключей, защита передаваемых по каналу сообщений.
25. Криптографические механизмы в спецификации SSL/TLS: аутентичное распределение ключей, защита передаваемых по каналу сообщений.
26. Криптографические механизмы в спецификации IPSec: аутентичное распределение ключей, защита передаваемых по каналу сообщений.
27. Схема проверяемого разделения секрета Фельдмана.
28. Схема проверяемого разделения секрета Педерсена.

4.2.2 Критерии оценивания к экзамену

Оценка «отлично»: точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «хорошо»: при ответе на один вопрос даны точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями; при ответе на второй вопрос имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «удовлетворительно»: при ответе на оба вопроса имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «неудовлетворительно»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

5.1 Основная литература

1. Ищукова, Е.А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ, Южный

федеральный университет, Инженерно-технологическая академия. - Таганрог : Издательство Южного федерального университета, 2016. - 80 с. : ил. - Библиогр. в кн. - ISBN 978-5-9275-2066-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493059

2. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 331 с. : ил. - (Высшее профессиональное образование . Информатика и вычислительная техника) (Учебное пособие). - Библиогр.: с. 327-328. . (36 экз. в библиотеке КубГУ).

5.2 Дополнительная литература

1. Алгебраические задачи криптографии [Текст] : практикум / [сост. С. В. Нагорный] ; М-во образования и науки Рос. Федерации ; КубГУ. - Краснодар : [КубГУ], 2005. - 26 с. (29 экз. в библиотеке КубГУ).
2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092
3. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации [Текст] : учебное пособие для студентов вузов /. - М. : Горячая линия-Телеком , 2005. - 229 с. . (10 экз. в библиотеке КубГУ).
4. Лапонина О. Р. [под ред. В. А. Сухомлина] Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Текст] : учебное пособие для студентов вузов / - 2-е изд., испр. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний , 2007. - 531 с. (10 экз. в библиотеке КубГУ).

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Гультяева, Т.А. Основы теории информации и криптографии : конспект лекций / Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2010. - 88 с. : табл., схем. - ISBN 978-5-7782-1425-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228963

7. Методические указания для обучающихся по освоению дисциплины (модуля)

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, контрольной работы, экзамена.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором,

способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

Методические указания по выполнению лабораторных работ

Лабораторные работы выполняются, как правило, в компьютерном классе. Отдельные работы могут выполняться в аудитории при наличии у бакалавриантов портативных компьютеров.

На лабораторных занятиях осуществляется проработка и закрепление методов и инструментария для верификации программ учебного характера. По отдельным темам бакалавриантам поручается подготовить презентации и выступить с докладами на занятиях.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

8.1 Перечень информационных технологий

– Проверка домашних заданий и консультирование посредством электронной почты.

– Использование электронных презентаций при проведении лекций и практических занятий.

8.2 Перечень необходимого программного обеспечения

1. Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2. Microsoft Visual Studio 2012+ : Visual C++, C#.
3. Python

8.3 Перечень информационных справочных систем:

1. Электронный каталог Научной библиотеки КубГУ (http://megapro.kubsu.ru/MegaPro/Web).
2. Электронная библиотечная система "Университетская библиотека ONLINE" (www.biblioclub.ru).
3. Электронная библиотечная система издательства "Лань" (https://e.lanbook.com).
4. Электронная библиотечная система "Юрайт" (http://www.biblio-online.ru).

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) PowerPoint. ауд. 129, 131, А305.
2.	Лабораторные занятия	Лаборатория, укомплектованная специализированными техническими средствами обучения – компьютерный класс, с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета (лаб. 102-106.).
3.	Групповые (индивидуальные)	Аудитория, (кабинет) – компьютерный класс

	консультации	
4.	Текущий контроль, промежуточная аттестация	Аудитория, приспособленная для письменного ответа при промежуточной аттестации.
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.