МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО Руководитель ОПОП О. Н. Выборнова «05» мая 2025 г.	УТВЕРЖДАЮ И.о. Заведующего кафедрой информационной безопасности В. А. Черкасова «05» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Криптографические протоколы»

Составитель(-и)	**Выборнова О.Н., доцент, к.т.н, доцент кафедры ИТ**
Направление подготовки / специальность	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)**
Квалификация (степень)	**бакалавр**
Форма обучения	**Очно-заочная**
Год приема	**2023**
Курс	**4**
Семестр	**7**

Астрахань – 2025

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) «Криптографические протоколы» являются изложить студентам принципы, методы и схемы защиты информации с использованием криптографических протоколов, а также продемонстрировать их практическую значимость и особенности реализации.

1.2. Задачи освоения дисциплины (модуля):

– изучение np-полных задач, криптографических стандартов, алгоритмов шифрования.

– формирование умений использовать программные и аппаратные средства персонального компьютера, пользоваться нормативными документами по защите информации.

– формирование навыков и (или) опыт деятельности: навыки работы с государственными стандартами, поиска уязвимостей в системах передачи информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Криптографические протоколы» относится к части, формируемой участниками образовательных отношений, и осваивается в 7 семестре.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

– «Математические основы защиты информации»

– «Криптографические методы защиты информации»

Знания: *np*-полных задач, криптографических стандартов, алгоритмов шифрования.

Умения: использовать программные и аппаратные средства персонального компьютера, пользоваться нормативными документами по защите информации.

Навыки: работы с государственными стандартами, поиска уязвимостей в системах передачи информации.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

– «Аттестация объектов информатизации»

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) профессиональных (ПК):

ПК-1 – способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-1: способен выполнять работы по установке, настройке и обслуживанию программ-	ПК-1.1. нормативные правовые акты в области защиты информации, организационные меры по защите информации,	ПК 1.2. определять источники и причины возникновения инцидентов, устранять нарушения правил разграничения	ПК-1.3. методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения

ных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем	программно-аппаратные средства обеспечения защиты информации автоматизированных систем, методы контроля эффективности защиты информации от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	доступа, применять программные средства обеспечения безопасности данных, осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, использовать криптографические методы и средства защиты информации в автоматизированных системах	доступа

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет 3 зачетные единицы, в том числе 36 часов, выделенных на контактную работу обучающихся с преподавателем (из них 18 часов – лекции, 18 часов – лабораторные работы), и 72 часа – на самостоятельную работу обучающихся:

Таблица 2 – Структура и содержание дисциплины (модуля)

Раздел, тема дисциплины (модуля)	Семестр	Контактная работа (в часах)			Самост. работа		Формы текущего контроля успеваемости, форма промежуточной аттестации
		Л	ПЗ	ЛР	КР	СР	
Понятие криптографического протокола	7	2		2		8	Контрольная работа 1. Опрос на экзамене.
Криптографические хеш-функции		2		2		8	Отчет по лабораторной работе 1. Опрос на экзамене.
Коды аутентификации		2		2		8	Тестирование Опрос на экзамене
Схемы цифровых подписей		2		2		8	Отчет по лабораторной работе 2. Опрос на экзамене
Протоколы идентификации		2		2		8	Отчет по лабораторной работе 3. Опрос на экзамене
Протоколы с нулевым разглашением		2		2		8	Отчет по лабораторной работе 4. Опрос на экзамене
Протоколы передачи ключей		2		2		8	Отчет по лабораторной работе 5. Опрос на экзамене
Открытое распределение ключей		2		2		8	Отчет по лабораторной работе 6. Опрос на экзамене
Предварительное распределение ключей		2		2		8	Отчет по лабораторной работе 7. Опрос на экзамене
		18		**18**		**72**	**ЭКЗАМЕН**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции	Общее количество компетенций
		ПК 1	
Понятие криптографического протокола	12	+	1
Криптографические хеш-функции	12	+	1
Коды аутентификации	12	+	1
Схемы цифровых подписей	12	+	1
Протоколы идентификации	12	+	1
Протоколы с нулевым разглашением	12	+	1
Протоколы передачи ключей	12	+	1
Открытое распределение ключей	12	+	1
Предварительное распределение ключей	12	+	1
Итого	***108***		

Краткое содержание каждой темы дисциплины (модуля)

Тема 1. Понятие криптографического протокола

Понятие криптографического протокола. Отличия криптографического протокола от криптографического алгоритма. Общая классификация криптографических протоколов: протоколы с посредником, протоколы с арбитром, самодостаточные протоколы. Понятие атаки на криптографический протокол. Основные соглашения об участниках криптографических протоколов Основные соглашения о среде выполнения криптографических протоколов.

Тема 2. Криптографические хеш-функции

Основные свойства хэш- функций. Понятие хеш-функции. Использование блочных алгоритмов шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.

Тема 3. Коды аутентификации

Основные понятия и концепции. Аутентификация источника данных. Аутентификация сущности. Генерация аутентифицированных ключей. Основные методы и механизмы аутентификации. Стратегия «оклик-отзыв». Механизм меток времени. Протоколы аутентификации. Аутентификация с помощью пароля. Протокол взаимоблокировки. Протокол Ву-Лама. Протокол Отвея-Рииса.

Тема 4. Схемы цифровых подписей

Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамаля. Стандарты на алгоритмы цифровой подписи. Стандарт цифровой подписи ГОСТ Р34.10- 94. Новый отечественный стандарт ЭЦП. Управление открытыми ключами.

Тема 5. Протоколы идентификации

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.

Тема 6. Протоколы с нулевым разглашением

Общие сведения о доказательствах с нулевым разглашением. Доказательство с нулевым разглашением и аргументация с нулевым разглашением. Свойства доказательств с нулевым разглашением. Схема Фейге-Фиата- 10 Шамира. Параллельная схема Фейге-Фиата-Шамира. Схема Гиллоу- Куискуотера.

Тема 7. Протоколы передачи ключей

Протоколы передачи сеансовых секретных ключей. Протокол WideMouth Frog. Обмен зашифрованными ключами EKE. Трехпроходный протокол Шамира. Протоколы предварительного распределения ключей. Схема распределения ключей Блома. Протоколы совместной выработки общего ключа. Протокол Диффи-Хеллмана. Протокол "станция-станция".

Тема 8. Открытое распределение ключей

Алгоритмы построения систем с открытым ключом: система Диффи-Хеллмана, шифры Шамира, Эль-Гамаля.

Тема 9. Предварительное распределение ключей

Резервные копии ключей шифрования. Скомпрометированные ключи. Время жизни ключей. Уничтожение ключей. Управление ключами в системах с открытым ключом.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Лекционные занятия проводятся с демонстрацией тезисов материалов в виде презентации.

На лабораторных занятиях преподаватель озвучивает цель и основные задачи лабораторной работы, комментирует ход выполнения работы и требования к отчету.

При подготовке к учебным занятиям необходимо воспользоваться учебно-методической литературой из п.8.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

При подготовке к учебным занятиям рекомендуется воспользоваться учебно-методической литературой из п.8, а также материалами, загруженными в ЭИОС.

В случае пропуска лекционного занятия необходимо ознакомиться с презентацией по теме в ЭИОС. При возникновении вопросов по содержимому лекции – обратиться за разъяснениями к преподавателю.

При подготовке к отчету лабораторной работы необходимо ответить на контрольные вопросы. Отчет осуществляется в виде демонстрации преподавателю хода выполнения работы, полученных результатов, а также ответа на контрольные вопросы. Допускается добавление ответов на контрольные вопросы в конец отчета по лабораторной работе.

Таблица 4 – Содержание самостоятельной работы обучающихся

Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Основные атаки на безопасность протоколов. Формальные методы анализа протоколов обеспечения безопасности	8	Подготовка к контрольной работе 1.
Возможные атаки на функции хеширования	8	Выполнение лабораторной работы 1.
Характеристика оптимальных кодов аутентификации	8	Подготовка к тестированию

Цифровые подписи на основе симметричных систем шифрования. Другие протоколы цифровой подписи.	8	Выполнение лабораторной работы 2.
Протоколы идентификации, использующие технику доказательства знания	8	Выполнение лабораторной работы 3.
Сертифицированная электронная почта. Аргумент с нулевым разглашением. Протокол электронного голосования.	8	Выполнение лабораторной работы 4.
Возможные атаки на протоколы передачи ключей.	8	Выполнение лабораторной работы 5.
Аутентифицированные протоколы.	8	Выполнение лабораторной работы 6.
Возможные атаки на схемы предварительного распределения ключей.	8	Выполнение лабораторной работы 7.

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

Лабораторные работы. Для подготовки необходимо изучить теоретический материал по соответствующей теме и разработать программное обеспечение на любом языке программирования. Отчет должен быть представлен в печатном виде и включать в себя описание алгоритма, скриншоты разработанных интерфейсов. При сдаче необходимо продемонстрировать корректно работающее программное обеспечение.

Контрольные работы. Для подготовки к контрольной работе необходимо изучить теоретический материал по соответствующей теме. При написании контрольной работы необходимо развернуто ответить на вопросы, дать аргументированный ответ, привести примеры, подтверждающие точку зрения.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий, в том числе разбор конкретных ситуаций.

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Понятие криптографического протокола	Обзорная лекция	Не предусмотрено	выполнение контрольной работы
Криптографические хеш-функции	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Коды аутентификации	Лекция	Не предусмотрено	выполнение теста
Схемы цифровых подписей	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Протоколы идентификации	Лекция	Не предусмотрено	выполнение лабораторной работы
Протоколы с нулевым разглашением	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы

Протоколы передачи ключей	Лекция	Не предусмотрено	выполнение лабораторной работы
Открытое распределение ключей	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Предварительное распределение ключей	Лекция	Не предусмотрено	выполнение лабораторной работы

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

На лекционных и практических занятиях применяются следующие образовательные технологии: интерактивные лекции, групповые дискуссии, тематические дискуссии, групповая консультация.

На лабораторных занятиях применяются ролевые игры.

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

– использование возможностей интернета в учебном процессе (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.);

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование виртуальной обучающей среды (LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 10 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
Microsoft Visual Studio	Среда разработки
PyCharm EDU	Среда разработки

6.3.2. Современные профессиональные базы данных и информационные справочные системы:

1. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС» http://dlib.eastview.com
2. Электронные версии периодических изданий, размещенные на сайте информационных ресурсов www.polpred.com
3. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информсистем»: https://library.asu-edu.ru/catalog/.
4. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/issledovaniya-i-innovacii/11745-nauchnye-jurnaly-agu.html.
5. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС) http://mars.arbicon.ru
6. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Криптографические протоколы» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Понятие криптографического протокола	ПК – 1	Контрольная работа 1. Опрос на экзамене.
Криптографические хеш-функции	ПК – 1	Отчет по лабораторной работе 1. Опрос на экзамене.
Коды аутентификации	ПК – 1	Тестирование Опрос на экзамене
Схемы цифровых подписей	ПК – 1	Отчет по лабораторной работе 2. Опрос на экзамене
Протоколы идентификации	ПК – 1	Отчет по лабораторной работе 3. Опрос на экзамене
Протоколы с нулевым разглашением	ПК – 1	Отчет по лабораторной работе 4. Опрос на экзамене
Протоколы передачи ключей	ПК – 1	Отчет по лабораторной работе 5. Опрос на экзамене
Открытое распределение ключей	ПК – 1	Отчет по лабораторной работе 6. Опрос на экзамене
Предварительное распределение ключей	ПК – 1	Отчет по лабораторной работе 7. Опрос на экзамене

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Для оценки результатов обучения применяются следующие критерии:

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема «Понятие криптографического протокола»

Контрольная работа 1 «Криптографические протоколы»

Вопросы по теме:

1. Охарактеризуйте понятие «протокол обеспечения безопасности».
2. Приведите пример некриптографического протокола обеспечения безопасности.
3. Перечислите виды аутентификации.
4. Приведите примеры защищенных протоколов, в которых не требуется обеспечение конфиденциальности.
5. Перечислите возможные подходы к классификации криптографических протоколов.
6. Перечислите наиболее распространенные атаки на криптографические протоколы.

7. Приведите способы защиты от атак на криптографические протоколы.

Тема «Криптографические хеш-функции»

Лабораторная работа 1 «Программная реализация алгоритма любой хеш-функции»

Задание:

Разработать программу, реализующую любую из изученных на лекции хэш-функций. Продемонстрировать работу программы.

Контрольные вопросы:

- Понятие хэш-функции.
- Сервисы безопасности, обеспечиваемые с помощью хэширования
- Алгоритмы хэширования

Тема «Коды аутентификации»

Тестирование

Банк тестовых заданий размещен на сайте методического центра электронного обучения http://moodle.asu-edu.ru

ТЗ №1

Вставить пропущенное слово.

… - это описание распределенного алгоритма, в процессе выполнения которого два (или более) участника последовательно выполняют определенные действия и обмениваются сообщениями.

ТЗ №2

Имитозащита

- Защиты проникновения в локальную сеть
- Физическая защита сети
- Защита от расшифрования зашифрованного текста
- Защита системы шифрования связи от навязывания ложных данных

ТЗ №3

В системе ЭЦП используется:

- Только один открытый ключ.
- Только один секретный ключ.
- Пара ключей: открытый и секретный.

ТЗ №4

Для генерации пары ключей в алгоритмах ЭЦП используется:

- Случайная строка битов.
- Математические схемы, основанные на применении однонаправленных функций.
- Генерирование непредсказуемых двойных последовательностей.

ТЗ №5

Выбрать правильный вариант ответа.

Протокол, при помощи которого получатель сообщения убеждается в подлинности и целостности этого сообщения –

- Самоутверждающийся
- Аутентификационный
- Хэш-протокол
- Идентификационный

ТЗ №6
Выбрать правильный вариант ответа.
Протокол, устанавливающий последовательность действий участников при передаче информации в информационном обмене –

- Протокол передачи данных
- Коммуникационный
- Сетевой
- Криптографический

ТЗ №7
Пароль для аутентификации пользователя хранится:

- В открытом виде
- В виде блоков по 64 бита
- В виде хэша

Тема «Схемы цифровых подписей»

Лабораторная работа 2 «Программная реализация любой схемы цифровой подписи»
Задание:
Разработать программу, демонстрирующую подписания документа или сообщения, а также проверку подписи. Продемонстрировать работу программы.
Контрольные вопросы:

- Понятие цифровой подписи
- Виды цифровой подписи
- Понятие удостоверяющего центра

Тема «Протоколы идентификации»

Лабораторная работа 3 ««Программная имитация любого протокола идентификации»»
Задание:
Разработать программу, имитирующую работу одной из схем: схема Фейге-Фиата-Шамира, схема Гиллу-Кискате, схема Шнорра. Продемонстрировать работу.
Контрольные вопросы:

- Понятия идентификации, аутентификации
- Схема Фейге-Фиата-Шамира,
- Схема Гиллу-Кискате,
- Схема Шнорра

Тема «Протоколы с нулевым разглашением»

Лабораторная работа 4 «Программная имитация любого протокола с нулевым разглашением»
Задание:
Разработать программу, имитирующую работу протокола с нулевым разглашением. Продемонстрировать работу программы
Контрольные вопросы:

- Понятие протокола с нулевым разглашением
- Применение на практике
- Возможные атаки

Тема «Протоколы передачи ключей»

Лабораторная работа 5 «Программная имитация любого протокола передачи ключей»

Задание:

Разработать программу, имитирующую работу протокола передачи ключей. Продемонстрировать работу программы.

Контрольные вопросы:

- Понятие протокола передачи ключей
- Желаемые свойства протокола
- Атаки

Тема «Открытое распределение ключей»

Лабораторная работа 6 «Программная реализация протокола Диффи-Хеллмана»

Задание:

Разработать программу, реализующую протокол Диффи-Хеллмана. Продемонстрировать работу программы.

Контрольные вопросы:

- Описание алгоритма
- Атака “man-in-the-middle”

Тема «Предварительное распределение ключей»

Лабораторная работа «Программная имитация любого протокола предварительного распределения ключей»

Задание:

Разработать программу, имитирующий работу протокола предварительного распределения ключей. Продемонстрировать работу программы.

Контрольные вопросы:

- Понятие протокола распределения ключей
- Описание алгоритма
- Атаки на протокол

Перечень вопросов к экзамену

1. Коды аутентификации сообщений, вероятности навязывания, критерии оптимальности.
2. Связь кодов аутентификации с ортогональными массивами.
3. Схемы цифровых подписей на основе симметричного шифрования.
4. Схемы цифровой подписи на основе систем с открытыми ключами.
5. Схема цифровой подписи Фиата-Шамира и ее свойства.
6. Схема цифровой подписи Эль-Гамаля и ее свойства.
7. Схемы цифровых подписей семейства Эль-Гамаля. Стандарты цифровой подписи ГОСТ Р.34.10-94 и DSA.
8. Протокол идентификации Шнорра и его связь с цифровой подписью.
9. Протокол идентификации Фиата-Шамира и его связь с цифровой подписью.
10. Протокол идентификации Окамото и его безопасность.
11. Протокол идентификации Guillou-Quisquater и его безопасность.
12. Протокол идентификации на основе самосертифицируемых открытых ключей, зависящих от идентификаторов.
13. Схемы битовых обязательств. Протокол подбрасывания монеты по телефону.
14. Двухсторонние протоколы передачи ключей с использованием симметричного шифрования.
15. «Бесключевой» протокол Шамира и его свойства.
16. Трехсторонние протоколы распределения ключей с использованием симметричного шифрования.

17. Протокол распределения ключей NSPK и его уязвимость.
18. Протокол аутентификации и распределения ключей Kerberos V5.
19. Протоколы аутентификации и распределения ключей KriptoKnight фирмы IBM.
20. Передача ключей с использованием систем с открытыми ключами.
21. Протокол распределения ключей EKE с использованием пароля.
22. Протокол аутентификации/распределения ключей SPX.
23. Сертификаты открытых ключей и протоколы их выдачи. Протокол обмена сертификатами X.509.
24. Протокол открытого распределения ключей Диффи – Хеллмана и его свойства.
25. Протокол открытого распределения ключей MTI. Пример атаки.
26. Протокол открытого распределения ключей на основе самосертифицируемых ключей, зависящих от идентификаторов.
27. Протокол открытого распределения ключей KEA.
28. Протокол открытого распределения ключей STS. Пример атаки.
29. Однопроходные версии протоколов открытого распределения ключей.
30. Предварительное распределение ключей. Нижняя оценка на объем ключевых материалов для схем предварительного распределения ключей.

Таблица 9. Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК – 1 способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты				
1.	Задание закрытого типа	Процесс, выполняемый после создания сеансового ключа DES: а) Подписание ключа б) Передача ключа на хранение третьей стороне (key escrow) в) Кластеризация ключа г) Обмен ключом	г	5
2.		Разработчик первого алгоритма с открытыми ключами: а) Ади Шамир б) Росс Андерсон в) Брюс Шнайер г) Мартин Хеллман	г	5
3.		Выберите то, что лучше всего описывает удостоверяющий центр? а) Организация, которая выпускает закрытые ключи и соответствующие алгоритмы б) Организация, которая проверяет процессы шифрования в) Организация, которая проверяет ключи шифрования г) Организация, которая выпускает сертификаты	г	5
4.		Причина, по которой удостоверяющий центр отзывает сертификат: а) Если открытый ключ пользователя скомпрометирован	в	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		б) Если пользователь переходит на использование модели PEM, которая использует сеть доверия в) Если закрытый ключ пользователя скомпрометирован г) Если пользователь переходит работать в другой офис		
5.		Выберите то, что лучше всего описывает цифровую подпись: а) Это метод переноса собственноручной подписи на электронный документ б) Это метод шифрования конфиденциальной информации в) Это метод, обеспечивающий электронную подпись и шифрование г) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения	г	5
6.	Задание открытого типа	Опишите кратно в чем заключается режим гаммирования с обратной связью в ГОСТ 28147-89.	Данный режим очень похож на режим гаммирования и отличается от него только способом выработки элементов гаммы – очередной элемент гаммы вырабатывается как результат преобразования по циклу 32-З предыдущего блока зашифрованных данных, а для зашифрования первого блока массива данных элемент гаммы вырабатывается как результат преобразования по тому же циклу синхропосылки. Этим достигается зацепление блоков – каждый блок шифротекста в этом режиме зависит от соответствующего и всех предыдущих блоков открытого текста. Поэтому данный режим иногда называется гаммированием с зацеплением блоков. На стойкость шифра факт зацепления блоков не оказывает никакого влияния.	5
7.		В чем состоит назначение имитовставки в ГОСТ 28147-89?	Для решения задачи обнаружения искажений в зашифрованном массиве данных с заданной вероятностью в ГОСТе предусмотрен допол-	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			нительный режим криптографического преобразования – выработка имитовставки. Имитовставка – это контрольная комбинация, зависящая от открытых данных и секретной ключевой информации. Целью использования имитовставки является обнаружение всех случайных или преднамеренных изменений в массиве информации.	
8.		Свойства криптографических хеш-функций	Криптографические хеш-функции должны иметь следующие свойства: 1. Одно и то же сообщение всегда приводит к одному и тому же хеш-значению (т.е. детерминистический). 2. Хеш-значение вычисляется быстро. 3. Невозможно иметь два сообщения с одинаковым значением хеш-функции (так называемое «столкновение»). 4. Невозможно намеренно создать сообщение, которое дает заданное значение хеш-функции. 5. Небольшие изменения в сообщении должны значительно изменить результирующее значение хеш-функции, чтобы оно казалось не связанным с исходным хеш-значением.	8
9.		Что такое SHA-1?	SHA-1 (безопасный алгоритм хеширования 1) - это криптографическая хеш-функция, которая может преобразовывать произвольно длинную строку данных в дайджест с фиксированным размером 160 бит.	5
10.		Что такое SHA-2?	SHA-2 (безопасный алгоритм хеширования 2) относится к семейству криптографических хеш-функций, которые могут преобразовывать произвольно длинные строки данных в дайджесты фиксированного размера (224, 256, 384 или 512 бит).	5

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля).

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

За семестр студент может набрать максимум 50 баллов. За ответ на экзамене студент может получить максимум 50 баллов. Баллы, полученные в течение семестра, суммируются с баллами, полученными на экзамене. Исходя из получившегося результата выставляется итоговая оценка:

- 0-59 баллов – 2, «неудовлетворительно»
- 60-74 баллов – 3, «удовлетворительно»
- 75-89 баллов – 4, «хорошо»
- 90-100 баллов – 5, «отлично»

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю) в каждом семестре

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	7/4	28	По расписанию
2.	*Выполнение контрольной работы*	2/3	6	
3.	*Тест*	2/3	6	
Всего			**40**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*	1	3	
5.	*Своевременное выполнение всех заданий*	1	3	
6.	*Активность студента на занятии*	1	4	
Всего			**10**	-
Дополнительный блок				
7.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале
90–100	5 (отлично)
85–89	4 (хорошо)
75–84	
70–74	
65–69	3 (удовлетворительно)
60–64	
Ниже 60	2 (неудовлетворительно)

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Криптография и безопасность в технологии .NET / Торстейнсон П. - М. : БИНОМ, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785996313457.html (ЭБС «Консультант студента»).

2. Основные методы криптографической обработки данных: Учеб. пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Родионов. - М. : Издательство МГТУ им. Н. Э. Баумана, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785703838334.html (ЭБС «Консультант студента»).

3. Криптографические методы защиты информации / Аверченков В.И. - М. : ФЛИНТА, 2017. - URL: http://www.studentlibrary.ru/book/ISBN9785976529472.html (ЭБС «Консультант студента»).

4. Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н. - 2-е изд. - М. : Горячая линия - Телеком, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785991203500.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Практическая криптография: алгоритмы и их программирование [/ Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - URL: http://www.studentlibrary.ru/book/ISBN5980030026.html (ЭБС «Консультант студента»).

2. Компьютерная безопасность. Криптографические методы защиты / Петров А.А. - М. : ДМК Пресс, 2008. - URL: http://www.studentlibrary.ru/book/ISBN5898180648.html (ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).