Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный
университет имени
Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«__» _____ 2024 г.
Регистрационный №УД-574/24/уч

МОДУЛЬ «ДИСЦИПЛИНЫ СПЕЦИАЛИЗАЦИИ 1-98 01 01-01 03 «ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Учебная программа учреждения образования
по учебной дисциплине для специальности
1-98 01 01 «Компьютерная безопасность (по направлениям)»,
направление специальности
1-98 01 01-01 «Компьютерная безопасность
(математические методы и программные системы)»

2024 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 1-98 01 01-2021 и учебного плана по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)». Регистрационный № 21-21/ уч. ФКНЭ от 26.07.2021г.

СОСТАВИТЕЛЬ:
Сергей Васильевич Кухта, старший преподаватель кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 5 от «20» 05 2024 г.)

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 10 от «25» 06 2024 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Криптографические протоколы предназначены для обеспечения безопасности передачи, обработки и хранения информации в небезопасной среде. Криптографический протокол – это распределенный алгоритм, определяющий порядок обмена сообщениями между несколькими агентами, в качестве которых могут выступать, например, люди компьютерные программы, вычислительные комплексы, базы данных, сети связи, банковские карточки и т.д

Учебная дисциплина «Криптографические протоколы» знакомит студентов с методами построения таких криптографических преобразований, условиями их применения, а также методами оценки их надежности.

Цели изучения учебной дисциплины «Криптографические протоколы»: ознакомление студентов с основами современной теории криптографических протоколов, задачами, решаемыми с помощью криптографических протоколов; формирование навыков использования криптографических преобразований для построения систем защиты информации.

При изложении материала учебной дисциплины важно показать возможности использования конкретных криптографических преобразований при решении прикладных задач защиты информации.

З***адачи***, решаемые при изучении учебной дисциплины «Криптографические протоколы»:

– развитие навыков построения, реализации, анализа стойкости и применения криптографических протоколов для обеспечения безопасности в современных информационных системах и компьютерных сетях;

– изучение основ создания защищенных туннелей через открытые сети;

– изучение криптографических протоколов аутентификации, распределения ключей, голосования, разделения секрета.

Требования к уровню освоения содержания учебной дисциплины. При изучении дисциплины «Криптографические протоколы» у студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по защите информации. Математик», обеспечивающих выпускникам успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

специализированные компетенции:

СК-11. Применять статистические методы для анализа стойкости криптографических алгоритмов и тестирования датчиков случайных и псевдослучайных чисел.

СК12. Уметь на практике создавать и анализировать стойкость криптографических протоколов для обеспечения безопасности современных компьютерных систем.

СК-14. Владеть основными методами построения надежных криптосистем, функций хеширования и систем электронной цифровой подписи.

СК-21. Владеть базовыми принципами построения компьютерных систем и сетей, алгоритмами маршрутизации в IP-сетях, создавать сетевые приложения, использующие базовые протоколы.

В результате освоения учебной дисциплины студент должен:

знать:

– типы ключей и их взаимосвязь, функции управления ключами, классификацию способов распределения ключевой информации;

– основные схемы криптографических протоколов аутентификации, распределения ключей, голосования, разделения секрета;

– разновидности атак на криптографические протоколы аутентификации, распределения ключей, голосования, разделения секрета;

– основы создания защищенных туннелей через открытые сети;

уметь:

– применять полученные знания на практике при создании, применении и анализе стойкости криптографических протоколов аутентификации для обеспечения безопасности современных компьютерных систем;

– создавать и производить настройку параметров защищенных виртуальных сетей и канала IPSec в туннельном и транспортном режиме средствами операционных систем;

– обеспечивать безопасность разделяемых сетевых ресурсов;

владеть:

– методами формулирования задач, возникающих при организации защиты информации;

– методами применения криптографических протоколов для построения защищенных информационных систем;

– навыками работы с современными криптографическими протоколами.

Перечень дисциплин, в продолжение и на базе которых изучается дисциплина. Базовыми для изучения учебной дисциплины «Криптографические протоколы» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» являются учебные дисциплины «Криптографические методы», «Операционные системы», «Теоретические основы информационной безопасности», «Арифметические и алгебраические основы криптографии».

Перечень дисциплин, которые изучаются на базе дисциплины. Знания, полученные при изучении учебной дисциплины «Криптографические протоколы», являются основой для дипломного проектирования, используются учебными дисциплинами «Программно-аппаратные и технические средства защиты информации», «Технологии разработки и защиты серверных веб-приложений и веб-служб», «Методы и стандарты оценки защищенности компьютерных систем».

Форма получения высшего образования – дневная.

В соответствии с учебным планом специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» на изучение учебной дисциплины «Криптографические протоколы» отводится:

Форма получения высшего образования первой ступени	дневная
Курс (курсы)	4
Семестр	7
Всего часов по дисциплине	94
Всего аудиторных часов по дисциплине	50
В том числе:	
Лекций, часов	24
Лабораторные занятия, часов	26
Самостоятельная работа, часов	44
Форма промежуточной аттестации	экзамен
Трудоемкость дисциплины, зачетные единицы	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ВВЕДЕНИЕ

Тема 1.1. Криптографические протоколы: общие положения.

Определение, назначение, область применения криптографических протоколов. Задачи, решаемые с помощью криптографических протоколов. Параметры, используемые для обеспечения подлинности сеанса связи: временные отметки, порядковые номера, случайные числа.

Тема 1.2. Атаки на криптографические протоколы.

Что понимается под атакой на криптографические протоколы. Модель угрозы Долева-Яо. Пассивная и активная атаки. Взаимодействие атакующего с каналом связи. Разновидности атак на криптографические протоколы.

Раздел 2. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

Тема 2.1. Введение в криптографические протоколы аутентификации.

Определение понятий идентификация, аутентификация и авторизация. Разновидности протоколов аутентификации.

Тема 2.2. Протоколы простой аутентификации.

Протоколы аутентификации, основанные на использовании одноразового пароля. Протоколы аутентификации, основанные на пароле пользователя.

Тема 2.3. Протоколы строгой аутентификации.

Протоколы аутентификации Международных стандартов ISO/IEC 9798 части 2, 3, и 4, основанные на использовании симметричного алгоритма шифрования, цифровой подписи и кода аутентификации сообщений (MAC-коде); их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости. Протокол Нидхема-Шрёдера.

Раздел 3. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ГОЛОСОВАНИЯ

Тема 3.1. Протоколы вручения обязательств.

Разновидности протоколов голосования. Определение схемы вручения обязательств. Протокол схемы вручения обязательств. Организация торгов, проблемы и их решения.

Тема 3.2. Протоколы идентификации с нулевым разглашением.

Протокол голосования с использование ЭЦП, числовой протокол голосования. Вычислительная и теоретико-информационная связность. Проблемы протоколов типа «запрос-ответ». Идея ZK-протоколов идентификации. Протокол Шнорра. ZK-свойство протокола Шнорра. Недостаток протокола Шнорра.

Раздел 4. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Тема 4.1. Управление ключами в криптографических системах и протоколах.

Определение криптографического ключа и ключевой системы, основные функции по управлению ключами. Типы ключей в зависимости от практического использования. Криптопериод ключа, типы ключей по криптопериоду. Способы распределения ключей. Классификация способов распределения ключей.

Тема 4.2. Криптографические протоколы распределения ключей.

Протоколы распределения ключей без использования третьей доверенной стороны, основанные на симметричной криптосистеме. Протоколы распределения ключей с участием третьей доверенной стороны, основанные на симметричной криптосистеме. Протоколы распределения ключей, основанные на асимметричной криптосистеме. Их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости.

Раздел 5. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Тема 5.1. Схемы разделения секрета.

Постановка задачи разделения секрета. Базовые понятия схемы разделения секрета. Протокол SHARE. Протокол RECON. Совершенная, идеальная и пороговая схемы разделения секрета.

Тема 5.2. Протоколы разделения секрета. Визуальная криптография.

Схема Шамира разделения секрета. Реплицированная схема разделения секрета. Схема разделения секрета с использованием визуальной криптографии. Способ Наора-Шамира схемы разделения секрета с использованием визуальной криптографии. Протоколы многосторонних вычислений. Примитивный криптографический протокол забывчивой передачи.

Раздел 6. ПРАКТИЧЕСКИЕ КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Тема 6.1. Виртуальная частная сеть (VPN).

Определение, цели и задачи VPN. Качество обслуживания в VPN. Защита данных в VPN. Организация VPN. Характеристики услуги VPN. Оценка надежности услуги VPN. Оценка безопасности услуги VPN.

Учебно-методическая карта учебной дисциплины «Криптографические протоколы»
Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		Лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
Раздел 1	**Введение**	**4**					
Тема 1.1	***Криптографические протоколы: общие положения.*** Определение, назначение, область применения криптографических протоколов. Задачи, решаемые с помощью криптографических протоколов. Параметры, используемые для обеспечения подлинности сеанса связи: временные отметки, порядковые номера, случайные числа.	2				Осн. лит.: [1], [2]. Доп. лит.: [2].	Блиц-опрос
Тема 1.2	***Атаки на криптографические протоколы.*** Что понимается под атакой на криптографические протоколы. Модель угрозы Долева-Яо. Пассивная и активная атаки. Взаимодействие атакующего с каналом связи. Разновидности атак на криптографические протоколы.	2				Осн. лит.: [1], [2]. Доп. лит.: [2].	Блиц-опрос
Раздел 2	**Криптографические протоколы аутентификации**	**6**	**6**				
Тема 2.1	***Введение в криптографические протоколы аутентификации.*** Определение понятий идентификация, аутентификация и авторизация. Разновидности протоколов аутентификации.	2				Осн. лит.: [2], [3], [4]. Доп. лит.: [1], [2].	Блиц-опрос
Тема 2.2	***Протоколы простой аутентификации.*** Протоколы аутентификации, основанные на использовании одноразового пароля. Протоколы аутентификации, основанные на пароле пользователя.	2				Осн. лит.: [2], [3], [4]. Доп. лит.: [1], [2].	Блиц-опрос

1	2	3	4	5	6	7	8
	Лабораторная работа №1. Реализация протокола аутентификации пользователей информационной системы.		2			Методические указания	Защита отчета по лабораторной работе
Тема 2.3	***Протоколы строгой аутентификации.*** Протоколы аутентификации Международных стандартов ISO/IEC 9798 части 2, 3, и 4, основанные на использовании симметричного алгоритма шифрования, цифровой подписи и кода аутентификации сообщений (MAC-коде); их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости. Протокол Нидхема-Шрёдера.	2				Осн. лит.: [1], [3], [4]. Доп. лит.: [1], [2].	Блиц-опрос
	Лабораторная работа №2. Реализация протоколов односторонней и двусторонней аутентификации.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №2. Реализация протоколов односторонней и двусторонней аутентификации.		2				
Раздел 3	**Криптографические протоколы голосования**	**4**	**8**				
Тема 3.1	***Протоколы вручения обязательств.*** Разновидности протоколов голосования. Определение схемы вручения обязательств. Протокол схемы вручения обязательств. Организация торгов, проблемы и их решения.	2				Осн. лит.: [1], [3], [4]. Доп. лит.: [1]	Контрольное тестирование 1
	Лабораторная работа №3. Реализация протоколов вручения обязательств.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №3. Реализация протоколов вручения обязательств.		2				
Тема 3.2	***Протоколы идентификации с нулевым разглашением.*** Протокол голосования с использование ЭЦП, числовой протокол голосования. Вычислительная и теоретико-информационная связность. Проблемы протоколов типа «запрос-ответ». Идея ZK-протоколов идентификации. Протокол Шнорра. ZK-свойство протокола Шнорра. Недостаток протокола Шнорра.	2				Осн. лит.: [2], [3]. Доп. лит.: [2].	Блиц-опрос
	Лабораторная работа №4. Реализация ZK-протоколов.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №4. Реализация ZK-протоколов.		2				

1	2	3	4	5	6	7	8
Раздел 4	**Криптографические протоколы распределения ключей**	**4**	**6**				
Тема 4.1	***Управление ключами в криптографических системах и протоколах.*** Определение криптографического ключа и ключевой системы, основные функции по управлению ключами. Типы ключей в зависимости от практического использования. Криптопериод ключа, типы ключей по криптопериоду. Способы распределения ключей. Классификация способов распределения ключей.	2				Осн. лит.: [1], [3], [4]. Доп. лит.: [2].	Блиц-опрос
Тема 4.2	***Криптографические протоколы распределения ключей.*** Протоколы распределения ключей без использования третьей доверенной стороны, основанные на симметричной криптосистеме. Протоколы распределения ключей с участием третьей доверенной стороны, основанные на симметричной криптосистеме. Протоколы распределения ключей, основанные на асимметричной криптосистеме. Их назначение, область применения, необходимые условия выполнения, описание и анализ стойкости.	2				Осн. лит.: [1], [2], [5]. Доп. лит.: [2].	Блиц-опрос
	Лабораторная работа №5. Реализация протоколов распределения криптографических ключей.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №5. Реализация протоколов распределения криптографических ключей.		2				
	Лабораторная работа №5. Реализация протоколов распределения криптографических ключей.		2				
Раздел 5	**Криптографические протоколы разделения секрета**	**4**	**4**				
Тема 5.1	***Схемы разделения секрета.*** Постановка задачи разделения секрета. Базовые понятия схемы разделения секрета. Протокол SHARE. Протокол RECON. Совершенная, идеальная и пороговая схемы разделения секрета.	2				Осн. лит.: [2], [4]. Доп. лит.: [2].	Блиц-опрос

1	2	3	4	5	6	7	8
Тема 5.2	***Протоколы разделения секрета. Визуальная криптография.*** Схема Шамира разделения секрета. Реплицированная схема разделения секрета. Схема разделения секрета с использованием визуальной криптографии. Способ Наора-Шамира схемы разделения секрета с использованием визуальной криптографии. Протоколы многосторонних вычислений. Примитивный криптографический протокол забывчивой передачи.	2				Осн. лит.: [1], [2], [5]. Доп. лит.: [2].	Блиц-опрос
	Лабораторная работа №6. Реализация протоколов разделения секрета.		2			Методические указания	Защита отчета по лабораторной работе
	Лабораторная работа №6. Реализация протоколов разделения секрета.		2				
Раздел 6	**Практические криптографические протоколы**	**2**	**2**				
Тема 6.1	***Виртуальная частная сеть (VPN).*** Определение, цели и задачи VPN. Качество обслуживания в VPN. Защита данных в VPN. Организация VPN. Характеристики услуги VPN. Оценка надежности услуги VPN. Оценка безопасности услуги VPN.	2				Осн. лит.: [1], [2]. Доп. лит.: [2].	Контрольное тестирование 2
	Лабораторная работа №7. Управление VPN.		2			Методические указания	Защита отчета по лабораторной работе
	Всего (50 часов)	**24**	**26**				

Примечание: в соответствии с рейтинговой системой для определения результата текущего контроля за семестр в виде отметки в баллах по десятибалльной шкале используются отметки, полученные за мероприятия текущего контроля в течение семестра, обозначенные в графе «Форма контроля знаний»

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Васильева, И.Н. Криптографические протоколы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – Москва: Юрайт, 2023. – 349 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника и практикума для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

2. Деза, Е.И. Введение в криптографию. Теоретико-числовые основы защиты информации: учебное пособие / Е. И. Деза, Л. В. Котова. - издание стереотипное. – Москва : ЛЕНАНД, 2022. – 368 с. – (Основы защиты информации. № 14).

3. Романьков, В.А. Введение в криптографию: курс лекций / В. А. Романьков. – 2 издание, исправленное и дополненное. – Москва: ИНФРА-М, 2023. – 234 с. – Рекомендовано в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки 01.03.01 «Математика», 02.03.01 «Математика и компьютерные технологии», 01.03.02 «Прикладная математика и информатика» (квалификация (степень) «бакалавр»).

4. Фомичев, В.М. Криптографические протоколы защиты информации: учебник для вузов: в 2 частях / В. М. Фомичев, Д. А. Мельников; под редакцией В.М. Фомичева. – Москва: Юрайт, 2023. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. Часть 1 : Математические аспекты. – 2023. – 209 с.

5. Фомичев, В.М. Криптографические протоколы защиты информации: учебник для вузов: в 2 частях / В. М. Фомичев, Д. А. Мельников; под редакцией В.М. Фомичева. – Москва: Юрайт, 2023. – (Высшее образование). – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. Часть 2: Системные и прикладные аспекты. – 2023. – 245 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

Дополнительная:

1. **Вонг, Д.** Реальная криптография = Real-World Cryptography / Д. Вонг ; пер. с англ. Д. Романовская. – Санкт-Петербург: Питер, 2024. – 432 с.

2. Криптология: учебник / Харин Ю. С. [и др.] - Минск : БГУ, 2013. – 511 с. – (Классическое университетское издание).

Чуркова Е.В

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Реализация протокола аутентификации пользователей информационной системы.

Лабораторная работа №2 Реализация протоколов односторонней и двусторонней аутентификации.

Лабораторная работа №3 Реализация протоколов вручения обязательств.

Лабораторная работа №4 Реализация ZK-протоколов.

Лабораторная работа №5 Реализация протоколов распределения криптографических ключей.

Лабораторная работа №6 Реализация протоколов разделения секрета.

Лабораторная работа №7 Управление VPN.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЭКЗАМЕНА

1. Определение протокола. Его участники, их действия. Цели протоколов
2. Протокол безопасности. Цели безопасности. Стойкость протокола
3. Криптографический протокол. Полнота, корректность криптографического протокола. Цели криптографического протокола
4. Предположения, используемые при анализе протоколов. Модель угрозы Долева–Яо
5. Типичные атаки на протоколы. Примеры атак на протоколы
6. Классификация протоколов. Криптографические методы, используемые в протоколах
7. Аутентификация, ее виды. Идентификация
8. Фазы протокола аутентификации. Схема аутентификации. Многофакторная аутентификация пользователя
9. Слабая аутентификация пользователя на основе фиксированного пароля. Атаки на неё
10. Общая схема аутентификации. Аутентификация на основе симметричного шифра
11. Аутентификация на основе асимметричного шифра и электронной цифровой подписи
12. Протоколы двусторонней аутентификации. Атака отражением. Частичная защита от атаки. Способы исключения симметричности
13. Протокол Нидхема-Шрёдера. Атака на него. Исправленная версия протокола Нидхема-Шрёдера
14. Пример и задача подбрасывания монеты по телефону. Определение схемы вручения обязательств
15. Протокол схемы вручения обязательств. Проблемы подбрасывания монеты по телефону
16. Организация торгов, проблемы и их решения
17. Строгое определение схемы вручения обязательств. Требования безопасности
18. Вычислительная и теоретико-информационная связность. Требования безопасности
19. Проблемы протоколов типа «запрос-ответ». Идея ZK-протоколов идентификации. Пример не ZK-протокола
20. Протокол Шнорра
21. Корректность протокола Шнорра
22. ZK-свойство протокола Шнорра. Недостаток протокола Шнорра
23. Протокол Шнорра с одной итерацией. Его корректность и ZK-свойство
24. Протокол распределения ключей, его типы. Цель протокола. Атаки на протокол
25. Протоколы распределения ключей без электронной цифровой подписи
26. Протоколы распределения ключей с применением электронной цифровой подписи
27. Протоколы передачи ключа с использованием симметричной криптографии
28. Протокол передачи ключа с односторонней аутентификацией на основе сертификатов публичных ключей. Протокол передачи ключа с взаимной аутентификацией на основе сертификатов публичных ключей
29. Протокол Диффи-Хэллмана. Свойства протокола
30. Назначение протоколов предварительного распределения ключей
31. Схема Блома предварительного распределения ключей
32. Функция формирования ключа
33. Постановка задачи разделения секрета
34. Базовые понятия схемы разделения секрета. Протокол SHARE. Протокол RECON
35. Совершенная, идеальная и пороговая схемы разделения секрета
36. Схема Шамира разделения секрета: протокол SHARE; протокол RECON
37. Схема Шамира разделения секрета: стойкость; коэффициенты рекомбинации; пример схемы
38. Реплицированная схема разделения секрета: постановка задачи; протокол SHARE; протокол RECON; пример схемы
39. Схема разделения секрета с использованием визуальной криптографии: постановка задачи

40. Способ Наора-Шамира схемы разделения секрета с использованием визуальной криптографии: протокол SHARE; протокол RECON
41. Протоколы многосторонних вычислений: постановка задачи; требования к протоколу
42. Протокол многосторонних вычислений суммы
43. Протокол многосторонних вычислений произведения
44. Примитивный криптографический протокол забывчивой передачи (oblivious transfer – OT)
45. Протокол многосторонних вычислений арифметических выражений: постановка задачи; пример схемы
46. Протокол многосторонних вычислений арифметических выражений: инициализация; реализация суммирования, умножения на скаляр, умножения
47. Определение, цели и задачи VPN. Качество обслуживания в VPN. Защита данных в VPN
48. Организация VPN: устройства, их расположение в сети
49. Характеристики услуги VPN. Оценка надежности услуги VPN
50. Оценка безопасности услуги VPN: экспертная модель; экономическая модель; вероятностная модель

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Криптографические протоколы» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка конспекта лекций и учебной литературы;

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

– изучение вопросов для самоконтроля;

– подготовка к аудиторному выполнению лабораторных работ (предварительное знакомство с методическими указаниями, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к лабораторным занятиям;

–подготовка к защите лабораторных работ (оформление отчёта по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

–углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;

– изучение основной и дополнительной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

–систематизация полученных знаний при подготовке к экзамену.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе учебного курса по дисциплине «Криптографические протоколы» в системе дистанционного обучения Moodle для доступа студентов к электронным вариантам курса лекций и учебно-методических указаний по основным разделам дисциплины, для организации учебной деятельности студентов и контроля ее результативности.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Учебный курс по дисциплине «Криптографические протоколы» в системе дистанционного обучения Moodle (ссылка https://moodle.psu.by/course/view.php?id=269).

2. Методические указания к выполнению лабораторных работ по дисциплине «Криптографические протоколы» для студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)», направления специальности 1-98 01 01-01 «Компьютерная безопасность (математические методы и программные системы)».

Содержание самостоятельной работы студентов

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 2.3. Протоколы строгой аутентификации.* Протоколы аутентификации Международных стандартов ISO/IEC 9798 части 2, 3, и 4, основанные на использовании симметричного алгоритма шифрования, цифровой подписи и кода аутентификации сообщений (MAC-коде); их необходимые условия выполнения, описание и анализ стойкости. Протокол Нидхема-Шрёдера. Осн. лит.: [2], [3]. Доп. лит.: [2].	2
	Тема 3.2. Протоколы идентификации с нулевым разглашением. Протокол голосования с использование ЭЦП, числовой протокол голосования. Вычислительная и теоретико-информационная связность. Протокол Шнорра. ZK-свойство протокола Шнорра. Осн. лит.: [1], [2], [4]. Доп. лит.: [2].	2
	Тема 4.2. Криптографические протоколы распределения ключей. Протоколы распределения ключей без использования третьей доверенной стороны, основанные на симметричной криптосистеме. Протоколы распределения ключей с участием третьей доверенной стороны, основанные на симметричной криптосистеме. Протоколы распределения ключей, основанные на асимметричной криптосистеме. Осн. лит.: [1], [2], [5]. Доп. лит.: [2].	2
	Тема 5.2. Протоколы разделения секрета. Визуальная криптография. Схема Шамира разделения секрета. Реплицированная схема разделения секрета. Способ Наора-Шамира схемы разделения секрета с использованием визуальной криптографии. Протоколы многосторонних вычислений. Осн. лит.: [1], [2], [5]. Доп. лит.: [2].	2
Подготовка к защите отчетов по лабораторным работам	*Лабораторная работа №1* Реализация протокола аутентификации пользователей информационной системы.	3
	Лабораторная работа № 2 Реализация протоколов односторонней и двусторонней аутентификации.	3
	Лабораторная работа №3 Реализация протоколов вручения обязательств.	3
	Лабораторная работа №4 Реализация ZK-протоколов.	3
	Лабораторная работа №5 Реализация протоколов распределения криптографических ключей.	3
	Лабораторная работа №6 Реализация протоколов разделения секрета.	3

1	2	3
	Лабораторная работа №7 Управление VPN.	3
Подготовка к экзамену		15
		44

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в соответствии с Положением о рейтинговой системе оценки знаний и компетенций студентов (приказ ректора УО ПГУ № 294 от 06.06.2014 (в редакции, утверждённой приказом № 605 от 17.11.2014) в форме текущего контроля и промежуточной аттестации.

Мероприятия текущего контроля проводятся в течение семестра и включают в себя следующие формы контроля:

–устная форма (блиц-опрос на лекциях);

–письменная форма (письменные отчёты по лабораторным работам);

–устно-письменная форма (отчёты по лабораторным работам с их устной защитой);

–техническая форма (электронные тесты).

Лабораторные работы предполагают выполнение и защиту. При их выполнении выдаётся индивидуальное задание. Отчёт по лабораторной работе представляется в электронном виде. Содержание отчёта: название работы, вариант задания, анализ задания, ход выполнения работы, основные и промежуточные результаты, выводы по работе. Защита работ проводится индивидуально и оценивается в соответствии с установленными правилами.

Результат текущего *контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится исходя из отметок, выставленных в ходе проведения мероприятий текущего контроля в течение семестра по следующей формуле:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_{n1}) + (\text{ЛР}_1 + \cdots + \text{ЛР}_{n2}) + (\text{УО}_1 + \cdots + \text{УО}_{n3})}{(n1 + n2 + n3)},$$

где $\text{КТ}_1, \ldots, \text{КТ}_{n1}$ – отметки, выставленные по результатам контрольного тестирования; $n1$ – количество тестов; $\text{ЛР}_1, \ldots, \text{ЛР}_{n2}$ – отметки, выставленные по результатам защит лабораторных работ; $n2$ – количество работ; УО_1, ..., УО_{n3} – отметки, выставленные по результатам устных опросов на лекциях; $n3$ – количество устных опросов.

Результат текущего контроля рассчитывается как округлённое среднее значение. Результат может быть увеличен в соответствии с п.п. 6.8 и 6.9 Положения.

Промежуточная аттестация проводится в форме экзамена. Экзамен проводится согласно Положению.

Итоговая экзаменационная отметка по дисциплине рассчитывается по формуле:

$$\text{ИЭ} = k \cdot \text{Т} + (1-k) \cdot O,$$

где k – весовой коэффициент текущего контроля; Т – результат текущего контроля за семестр; О – отметка, полученная студентом на экзамене за ответ по билету.

Весовой коэффициент принимается равным $k = 0.5$.

Результат итоговой экзаменационной отметки округляется до целого значения.

Информация о весовом коэффициенте доводится до студентов на первом занятии в семестре. Положительной является отметка не ниже 4 баллов.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на лабораторных занятиях.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Криптографические протоколы» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

На лекционных занятиях по дисциплине «Криптографические протоколы» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и лабораторных занятиях.

На лекционных занятиях студенты овладевают системой теоретических знаний в области методов криптографической защиты информации. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их математический кругозор, использованием интерактивных методов обучения.

На лабораторных занятиях развиваются и формируются необходимые практические умения и навыки программной реализации криптографических методов защиты информации.

Применяется индивидуальный, творческий подход. Также во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, по которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу
Дипломное проектирование	математики и компьютерной безопасности	Предложений и замечаний нет	
Программно-аппаратные и технические средства защиты информации	математики и компьютерной безопасности	Предложений и замечаний нет	
Технологии разработки и защиты серверных веб-приложений и веб-служб	математики и компьютерной безопасности	Предложений и замечаний нет	
Методы и стандарты оценки защищенности компьютерных систем	математики и компьютерной безопасности	Предложений и замечаний нет	

Заведующий кафедрой математики и компьютерной безопасности, к.т.н., доцент И. Б. Бураченок