ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 03.11.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.34 Криптографические протоколы
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 03.11.2021

А. Н. Соколов

Разработчик программы,
д.физ.-мат.н., доц., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зюляркина Н. Д.
Пользователь: ziuliarkinand
Дата подписания: 03.11.2021

Н. Д. Зюляркина

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является изучение студентами основных видов современных криптографических протоколов, методов их анализа и оценки стойкости, основных сфер практического применения и особенностей реализации. Задачами дисциплины являются: - ознакомление студентов со структурой современных сложных криптосистем, основными классами криптографических протоколов; - обзор методов анализа стойкости криптографических протоколов и средств криптографической защиты информации, в которых они реализуются; - изучение основных нормативно-технических документов, регламенти-рующих применение криптографических методов защиты информации, а также проектирование, разработку и применение средств криптографической защиты информации.

Краткое содержание дисциплины

В рамках данной дисциплины исследуются основные виды криптографических протоколов, различные типы атак на используемые протоколы и методы защиты от них. Кроме этого изучаются нормативно-технических документы, регламентирующие проектирование, разработку и применение средств крипто-графической защиты информации..

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Знать:виды криптографических протоколов и их место в комплексной системе защиты информации
	Уметь:проводить аудит по результатам исполняемого протокола
	Владеть:криптографической терминологией
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать:предназначение криптографических протоколов в реализации политик информационной безопасности
	Уметь:правильно подобрать протокол исходя из требований политики безопасности
	Владеть:навыками работы с программно-аппаратными криптографическими средствами
ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	Знать:виды математических задач, лежащих в основе криптографических протоколов
	Уметь:производить вычисления в алгебраических структурах (группах, кольцах и полях), применять теоретико-графовые и теоретико множественные методы при реализации протоколов
	Владеть:навыками работы с программным обеспечением, связанным с алгебраическими и комбинаторными объектами
ПСК-3.2 способностью участвовать в разработке,	Знать:область применения криптографических

осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	протоколов в системе защиты автоматизированных систем
	Уметь:производить аудит результатов выполненного протокола
	Владеть:программистскими навыками и криптографической терминологией

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.23 Криптографические методы защиты информации	ДВ.1.05.02 Защита информации в автоматизированных системах управления

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.23 Криптографические методы защиты информации	Знать: виды криптографических систем. Уметь: производить процедуру шифрования и расшифровывания данных Владеть: криптографической терминологией

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	60	60
Разработка программ, реализующих различные криптографические протоколы.	20	20
Подготовка к практическим занятиям, выполнение домашних заданий.	40	40
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР

1	Основные понятия	8	6	2	0
2	Схемы цифровой подписи	6	4	2	0
3	Протоколы идентификации	8	4	4	0
4	Протоколы распределения ключей	12	6	6	0
5	Протоколы открытых сделок	8	6	2	0
6	Прикладные протоколы	4	4	0	0
7	Нормативные документы в области криптографических протоколов.	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие криптографического протокола. Роль криптографи-ческих протоколов в системах защиты информации. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей.	2
2	1	Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол.	2
3	1	Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.	2
4	2	Схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем.	2
5	2	Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением под-делки.	2
6	3	Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования.	2
7	3	Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением	2
8	4	Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли.	2
9	4	Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей.	2
10	4	Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	2
11	5	Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону.	2
13	5	Протоколы электронного голосования.	2
14	5	Протокол использования электронных денег	2
15	6	Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей.	2
16	6	Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE.	2

18	7	Протоколы SKIP, SSL/TLS и особенности их реализации.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Примеры протоколов на основе симметричных и асимметричных криптографических систем.	2
2	2	Примеры схем цифровых подписей. Контрольная работа "Цифровые подписи"	2
3	3	Протоколы «рукопожатия» и идентификации типа «запрос-ответ» с криптографической терминологией Протоколы доказательства знания с нулевым разглашением	3
4	3	Контрольная работа "Игровые протоколы"	1
5	4	Протоколы генерации и передачи ключей для симметричных шифрсистем. Протоколы генерации и передачи ключей для асимметричных шифрсистем. Протоколы разделения секрета	4
6	4	Контрольная работа "Схемы предварительного распределения ключей".	1
7	4	Контрольная работа "Схемы разделения секрета "	1
8	5	Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.)	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Разработка программ, реализующих различные криптографические протоколы.	Литература из основного и дополнительного списка.	20
Подготовка к практическим занятиям, выполнение домашних заданий.	Литература из основного и дополнительного списка.	40

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
использование презентаций	Практические занятия и семинары	выступление с докладом с использованием презентации	10

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
не предусмотрены	не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	контрольная работа	1
Все разделы	ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	подготовка доклада	2
Все разделы	ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	подготовка доклада	3
Все разделы	ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	контрольная работа	4

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
подготовка доклада	оценка выступления и текста доклада	Зачтено: тема доклада раскрыта Не зачтено: тема доклада не раскрыта
контрольная работа	проверка контрольных заданий	Зачтено: правильные ответы получены более чем в половине заданий Не зачтено: менее половины правильных ответов

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
подготовка доклада	Темы докладов.docx
контрольная работа	подписи.docx; Схемыраспределения.pdf

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Зюляркина Н. Д. Криптографические методы защиты информации. Методические указания по проведению практических занятий

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Музыкантский А.И., Фурин В.В. Лекции по криптографии [Электронный ресурс] / -- Московский центр непрерывного математического образования, 2013 — 68 с. http://e.lanbook.com/
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. http://e.lanbook.com/

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические	913	Комплект компьютерного оборудования; Локальная вычислительная сеть;

занятия и семинары	(3б)	Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2