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: 10.09.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины П.1.В.07.01 Моделирование информационного противодействия угрозам безопасности информации
для направления 10.06.01 Информационная безопасность
уровень аспирант **тип программы**
направленность программы
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.06.01 Информационная безопасность, утверждённым приказом Минобрнауки от 29.07.2014 № 874

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: 08.09.2021

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: 08.09.2021

Н. Д. Зюляркина

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является формирование знаний о возможностях программной реализации различных методов защиты информации и обеспечения информационной безопасности, а также практических навыков реализации программных алгоритмов защиты информации. Дисциплина раскрывает основные подходы к реализации программных алгоритмов защиты информации, современные тенденции в области криптографии и доступный инструментарии для прикладных и научно-прикладных работ в области разработки специализированных средств защиты информации. Задачи изучения дисциплины: - изучение основных понятий, определений и программных алгоритмов защитой информации; - формирование знаний о теоретической и научно-исследовательской базе реализации программных алгоритмов защиты информации; - развитие навыков прикладных разработок в области программных алгоритмов.

Краткое содержание дисциплины

Основные понятия и алгоритмы защиты информации. Оценка качества шифров. Системы открытого распределения ключей и открытого шифрования. Электронная цифровая подпись. Программная реализация алгоритмов шифрования. Методы и средства хранения ключевой информации. Реализация алгоритмов асимметричной криптографии. Алгоритмы генерации случайных чисел. Обеспечение надежности программной реализации криптографических алгоритмов защиты информации. Основные подходы к обеспечению качества программного обеспечения, отказоустойчивости и предотвращению неисправностей. Системные вопросы реализации СКЗИ. Криптографическая защита транспортного уровня кс. Криптографическая защита на прикладном уровне кс. Особенности сертификации и стандартизации криптографических средств.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-1.3 способностью моделировать угрозы и процессы противодействия угрозам безопасности информации	Знать:основные угрозы безопасности информации в информационных системах.
	Уметь:организовывать противодействие угрозам безопасности информации.
	Владеть:навыками моделирования угроз и процессов противодействия угрозам безопасности информации.
ОПК-2 способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Знать:методы исследования, применяемые в области обеспечения информационной безопасности
	Уметь:применять частные методы исследования для решения конкретных исследовательских задач в области обеспечения информационной безопасности
	Владеть:навыками применения частных методов исследования для решения конкретных исследовательских задач в области обеспечения

	информационной безопасности
ПК-1.2 способностью исследовать методологические подходы обеспечения информационной безопасности и применять их при разработке систем защиты информации	Знать:существующие методы и средства, применяемые для анализа систем защиты информации.
	Уметь:анализировать методы и средства, применяемые для создания систем защиты информации; разрабатывать предложения по их совершенствованию и повышению эффективности.
	Владеть:навыками анализа и разработки методов и средств, применяемых для создания систем защиты информации.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
П.1.В.06.01 Методы и системы защиты информации, информационная безопасность, П.1.В.04 Математическое моделирование	Подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук (6 семестр), Производственная (по получению профессиональных умений и опыта профессиональной деятельности) практика (6 семестр), Подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук (7 семестр), Подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук (8 семестр)

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

Дисциплина	Требования
П.1.В.06.01 Методы и системы защиты информации, информационная безопасность	Знать основные методы защиты информации в автоматизированных системах, специфику защиты информации на критически важных объектах, особенности проведения анализа защищенности автоматизированных систем. Уметь проводить инструментальный и экспертный анализ защищенности автоматизированных систем.

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

		5
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	38	38
Лекции (Л)	38	38
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	70	70
Самостоятельное изучение теоретического материала	35	35
Творческая самостоятельная работа	35	35
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия и алгоритмы защиты информации	12	12	0	0
2	Программная реализация алгоритмов защиты информации	20	20	0	0
3	Особенности реализации криптографических подсистем защиты информации	6	6	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные понятия и алгоритмы защиты информации. Криптографическая защита информации и ее программная реализация	2
2	1	Определение шифра. Априорные требования к шифру. Примеры шифрующих преобразований	2
3	1	Оценка качества шифров. Разновидности задач криптографического анализа. Абсолютная стойкость и стойкость в операциях	2
4	1	Синтез качественных шифров. Блочные шифры. Усложнение псевдослучайных последовательностей	2
5	1	Системы открытого распределения ключей и открытого шифрования. Математические основы. Системы Диффи-Хеллмана и RSA	2
6	1	Электронная цифровая подпись. Компоненты ЭЦП. Понятие и свойства хеш-функции. Протокол ЭЦП Эль-Гамаля	2
1	2	Программная реализация алгоритмов шифрования. Базовые циклы криптографических преобразований	2
2	2	Основные режимы шифрования. Оптимизация алгоритмов на языке высокого уровня	2
3	2	Методы и средства хранения ключевой информации	2
4	2	Типовые решения в организации ключевых систем и процедур идентификации- аутентификации	2
5	2	Реализация алгоритмов асимметричной криптографии. Базовые процедуры реализации. Внутреннее представление длинных чисел, основные операции	2
6	2	Реализация алгоритма хеширования и ЭЦП. Параметры, формирование и проверка	2

7	2	Алгоритмы генерации случайных чисел. Понятие программного датчика случайных чисел (ПДСЧ). Основные требования к ПДСЧ	2
8	2	Обоснование выбора алгоритма ПДСЧ. Сложность определения выходных последовательностей и состояний ПДСЧ	2
9	2	Обеспечение надежности программной реализации криптографических алгоритмов защиты информации. Основные подходы к обеспечению качества программного обеспечения, отказоустойчивости и предотвращению неисправностей	2
10	2	Исследование корректности реализации и верификация. Специфические вопросы обеспечения надежности программной реализации криптографических алгоритмов защиты информации. Слабость ключевой системы и ошибки в проектировании программ	2
1	3	Системные вопросы реализации СКЗИ. Способы и особенности реализации криптографических подсистем	2
2	3	Криптографическая защита транспортного уровня кс. Криптографическая защита на прикладном уровне кс	2
3	3	Особенности сертификации и стандартизации криптографических средств	2

5.2. Практические занятия, семинары

Не предусмотрены

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
Самостоятельное изучение теоретического материала. Основные понятия и алгоритмы защиты информации. Криптографическая защита информации и ее программная реализация	Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012. - 400 с.	35
Творческая самостоятельная работа. Программная реализация алгоритма защиты информации	Свинарёв Н.А., Ланкин О.В., Данилкин А.П., Потехецкий С.П., Перетокин О.И. Инструментальный контроль и защита информации: учебно-методическое пособие - Воронеж: ВГУИТ, 2013. - 192 с.	35

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проектное управление	Лекции	Организация надежной системы защиты информации и проведение инструментального анализа защищенности на основе проекта-модели автоматизированной системы	38

Собственные инновационные способы и методы, используемые в образовательном процессе

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
Основные понятия и алгоритмы защиты информации	ПК-1.2 способностью исследовать методологические подходы обеспечения информационной безопасности и применять их при разработке систем защиты информации	экзамен	1-71
Программная реализация алгоритмов защиты информации	ПК-1.3 способностью моделировать угрозы и процессы противодействия угрозам безопасности информации	экзамен	1-71
Особенности реализации криптографических подсистем защиты информации	ПК-1.3 способностью моделировать угрозы и процессы противодействия угрозам безопасности информации	экзамен	1-71

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
экзамен	студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает теоретические вопросы и задачи по пройденным разделам, преподаватель проверяет, беседует и оценивает	Отлично: обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы Хорошо: знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал Удовлетворительно: знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности в изложении материала Неудовлетворительно: не знает значительной части материала дисциплины; ответ не дан или допускает

		грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
экзамен	1-71 ФОС.pdf

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Борисов, М. А. Основы программно-аппаратной защиты информации [Текст] учеб. пособие для вузов по направлениям 010400 "Приклад. мат. и информ" и 010300 "Фундам. информ. и информ. технологии" М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 3-е изд., перераб. и доп. - М.: URSS : ЛЕНАНД, 2014. - 406 с. ил.
2. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] учеб. пособие для вузов по специальностям 090102 "Компьютер. безопасность", 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем" В. В. Платонов. - М.: Академия, 2006. - 238, [1] с. ил.
3. Грушо, А. А. Теоретические основы компьютерной безопасности [Текст] учеб. пособие для вузов по специальности 090100 "Информационная безопасность" А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М.: Академия, 2009. - 267, [1] с.
4. Девянин, П. Н. Модели безопасности компьютерных систем Учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность" и 075500 "Комплексное обеспечение информац. безопасности автоматизир. систем" П. Н. Девянин. - М.: Academia, 2005. - 142, [1] с.

б) дополнительная литература:

Не предусмотрена

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

г) методические указания для студентов по освоению дисциплины:

1. Свинарёв Н.А., Ланкин О.В., Данилкин А.П., Потехецкий С.П., Перетокин О.И. Инструментальный контроль и защита информации: учебно-методческое пособие - Воронеж: ВГУИТ, 2013. - 192 с.

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в	Доступность (сеть Интернет /

			электронной форме	локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Издательство "ДМК Пресс", 2012. - 592 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Издательство "Горячая линия-Телеком", 2012. - 320 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Основная литература	База текстов статей ScienceDirec (https://www.sciencedirect.com/)	ScienceDirect	Интернет / Авторизованный
4	Дополнительная литература	База текстов статей IEEE Xplore Digital Library (https://ieeexplore.ieee.org/)	IEEE Xplore Digital Library	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -База данных ВИНИТИ РАН(бессрочно)

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+