ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

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: 04.06.2023

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.33 Программно-аппаратные средства защиты информации
для направления 10.03.01 Информационная безопасность
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 17.11.2020 № 1427

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: 04.06.2023

А. Н. Соколов

Разработчик программы,
к.техн.н., старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Мищенко Е. Ю.
Пользователь: mishchenkoei
Дата подписания: 04.06.2023

Е. Ю. Мищенко

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины является подготовка специалистов в области проектирования средств обеспечения информационной безопасности автоматизированных систем и привитие навыков разработки и анализа компонентов автоматизированных систем. Задачи дисциплины: - изучение моделей угроз и модели нарушителя информационной безопасности автоматизированной системы; - изучение методов анализа проектных решений по обеспечению безопасности автоматизированных систем; - получение практических навыков проектирования систем защиты информации автоматизированной системы; - изучение методов анализа угроз и уязвимостей проектируемых и эксплуатируемых автоматизированных систем; - получение навыков использования программно-аппаратных средств обеспечения безопасности сетей автоматизированных систем.

Краткое содержание дисциплины

Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки. Правовые, нормативно-технические и организационные требования к средствам защиты информации. Подсистема контроля доступа пользователей к ресурсам. Подсистема регистрации и учета. Подсистема контроля целостности. Подсистема криптографической защиты. Межсетевое экранирование. Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации. Виртуальные частные сети. Контроль защищенности информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Знает: программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях Умеет: конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Не предусмотрены

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

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 6 з.е., 216 ч., 111,75 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		7	8
Общая трудоёмкость дисциплины	216	108	108
Аудиторные занятия:	96	48	48
Лекции (Л)	56	32	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	0	24
Лабораторные работы (ЛР)	16	16	0
Самостоятельная работа (СРС)	104,25	53,75	50,5
Подготовка к лабораторным работам, оформление результатов	12	12	0
Курсовая работа	33	0	33
Изучение материалов по плану СРС	59,25	41.75	17.5
Консультации и промежуточная аттестация	15,75	6,25	9,5
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет	экзамен,КР

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение	2	2	0	0
2	Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки	2	2	0	0
3	Правовые, нормативно-технические и организационные требования к средствам защиты информации	16	16	0	0
4	Подсистема контроля доступа пользователей к ресурсам	12	4	4	4
5	Подсистема регистрации и учета	6	2	2	2
6	Подсистема контроля целостности	12	4	4	4
7	Подсистема криптографической защиты	6	4	2	0
8	Межсетевое экранирование	8	4	2	2
9	Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации	10	6	4	0
10	Виртуальные частные сети	14	8	4	2
11	Контроль защищенности информации	8	4	2	2

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение	2
2	2	Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки	2
3	3	Требования к защищенности средств вычислительной техники, классы защищенности средств защиты информации от несанкционированного доступа	2
4	3	Требования к доверию, уровни отсутствия недекларированных возможностей (НДВ)	2
5	3	Требования к межсетевым экранам (МЭ), типы и классы защищенности МЭ	2
21	3	Требования к системам обнаружения вторжений (СОВ), типы и классы защищенности СОВ	2
22	3	Требования к средствам антивирусной защиты (САВЗ), типы и классы защищенности САВЗ	2
23	3	Требования к средствам доверенной загрузки (СДЗ), типы и классы защищенности СДЗ	2
24	3	Требования безопасности операционных систем (ОС), типы и классы защищенности ОС	2
25	3	Система сертификации ФСТЭК РФ	2
6	4	Идентификация, аутентификация. Аппаратные и программные средства санкционированной загрузки. Авторизация. Аппаратные ключи пользователей	2
7	4	Дискреционный доступ. Мандатный доступ, его реализация для файлов, папок и процессов. Управление потоками информации	2
8	5	Регистрация событий в ОС и СЗИ. Реализация маркировки и учета документов. Гарантированное удаление информации	2
9	6	Контроль целостности файлов и папок. Контроль нарушения аппаратной конфигурации. Санкционированное использование внешних носителей	2
10	6	Замкнутая программная среда. Особенности реализации в различных СЗИ	2
11	7	Хранение информации в шифрованном виде. Монопольный и коллективный доступ к контейнерам. Особенности реализации в различных СЗИ	2
12	7	Протокол Kerberos 5 в доменных сетях	2
13	8	Фильтрация пакетов. Трансляция сетевых адресов. Администрирование МЭ, схемы применения. Особенности реализации в различных СЗИ	4
14	9	Симметричное шифрование, ГОСТ Р 34.12-2018	2
15	9	ЭЦП, и ассиметричное шифрование, хеширование. ГОСТ Р 34.10-2018, ГОСТ 34.11-2018	2
16	9	Проблемы распределения и управления ключевой информацией. Система сертификация средств криптографической защиты информации	2
17	10	Центр управления сетью. Адресация	2
18	10	Ключевой удостоверяющий центр	2
19	10	Криптошлюз, клиент сети. Закрытый и открытый трафик. Туннелирование. Особенности реализации в различных СЗИ	4
20	11	Средства контроля защищенности информации для различных подсистем защиты	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	4	Мандатный доступ, его реализация для файлов, папок и процессов.	4
2	5	Регистрация событий входа-выхода, запуска задач.	2
3	6	Подсистема контроля целостности	4
4	7	Подсистема криптографической защиты	2
5	8	Межсетевое экранирование	2
6	9	Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации	4
7	10	Виртуальные частные сети	2
8	10	Криптошлюз. Туннелирование.	2
9	11	Контроль защищенности информации	2

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
3	4	Реализация разграничения доступа к внешним устройствам.	2
5	4	Управление потоками информации.	2
9	5	Гарантированное удаление информации.	2
10	6	Контроль целостности файлов и папок.	2
11	6	Контроль нарушения аппаратной конфигурации. Санкционированное использование внешних носителей.	2
14	8	Фильтрация пакетов.	2
16	10	Центр управления сетью. Адресация. Ключевой удостоверяющий центр.	2
21	11	Средства контроля защищенности информации для подсистемы контроля целостности.	2

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к лабораторным работам, оформление результатов		7	12
Курсовая работа		8	33
Изучение материалов по плану СРС	ЧЕРНОКНИЖНЫЙ Г. М. АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ. учебное пособие. - Год издания: 2020 Место издания: Санкт-ПетербургЧисло страниц: 90	7	41,75
Изучение материалов по плану СРС	ЧЕРНОКНИЖНЫЙ Г. М. АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ. учебное пособие. - Год издания: 2020 Место издания: Санкт-	8	17,5

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	7	Проме-жуточная аттестация	контрольная работа	-	2	0 - неправильный ответ, 1- неполный ответ, 2- полный ответ	зачет
2	8	Проме-жуточная аттестация	контрольная работа	-	2	0 - неправильный ответ, 1- неполный ответ, 2- полный ответ	экзамен
3	7	Текущий контроль	отчет о лабораторной работе №1	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
4	7	Текущий контроль	отчет о лабораторной работе №2	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
5	7	Текущий контроль	отчет о лабораторной работе №3	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
6	7	Текущий контроль	отчет о лабораторной работе №4	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
7	7	Текущий контроль	отчет о лабораторной работе №5	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
8	8	Текущий контроль	работа с реестром ФСТЭК, средства обнаружения вторжений	1	2	0 - не найдено, 1 - найдено менее 3-х СЗИ, 2 - найдено 3 СЗИ	экзамен
9	8	Текущий контроль	работа с реестром ФСТЭК, средства антивирусной защиты	1	2	0 - не найдено, 1 - найдено менее 3-х СЗИ, 2 - найдено 3 СЗИ	экзамен
10	8	Текущий контроль	работа с реестром ФСТЭК, средства доверенной загрузки	1	2	0 - не найдено, 1 - найдено менее 3-х СЗИ, 2 - найдено 3 СЗИ	экзамен
11	8	Текущий контроль	работа с реестром ФСТЭК, межсетевые экраны	1	2	0 - не найдено, 1 - найдено менее 3-х СЗИ, 2 - найдено 3 СЗИ	экзамен
12	8	Текущий	работа с реестром	1	2	0 - не найдено, 1 - найдено менее 3-х	экзамен

		контроль	ФСТЭК, операционные системы			СЗИ, 2 - найдено 3 СЗИ	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Студент получает два вопроса и устно отвечает преподавателю. Два полных ответа - отл, Один полный, другой неполный - хор, Два неполных ответа - удов, Один неправильный ответ - неуд	В соответствии с пп. 2.5, 2.6 Положения
зачет	Студент получает один вопрос и устно отвечает преподавателю. Неправильный ответ - незачет, правильный - зачет	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ											
		1	2	3	4	5	6	7	8	9	10	11	12
ОПК-10	Знает: программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	+	+	+	+	+	+	+	+	+	+	+	+
ОПК-10	Умеет: конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	+	+	+	+	+	+	+					
ОПК-10	Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа	+	+	+	+	+	+	+	+	+	+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. 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. Программно-аппаратная защита информации - Конспект лекций
2. Программно-аппаратные средства защиты информации: Методические указания к курсовой работе
3. Программно-аппаратные средства защиты информации: Методические указания к курсовой работе

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Программно-аппаратные средства защиты информации: Методические указания к курсовой работе

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	eLIBRARY.RU	БАГАНОВА З.А., МАГОМЕДОВА П.О., АРИПОВА М.М. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. - ВОПРОСЫ УСТОЙЧИВОГО РАЗВИТИЯ ОБЩЕСТВА - Номер: 4 Год: 2021 Страницы: 396-406 https://elibrary.ru/item.asp?id=45672526
2	Дополнительная литература	eLIBRARY.RU	ИСАЕВА Ю. А., ГОЛДОБИНА А..С, НИКУЛИН Д. М. ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ЗНАЧИМЫХ ОБЪЕКТАХ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР РОССИЙСКОЙ ФЕДЕРАЦИИ. ИНТЕРЭКСПО ГЕО-СИБИРЬ - Том: 6Номер: 1 Год: 2020 Страницы: 155-160 https://elibrary.ru/item.asp?id=44010566
3	Дополнительная литература	eLIBRARY.RU	КУЦ Д. В., ПОРШНЕВ С. В. ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПОЛНОМОЧНОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В СОВРЕМЕННЫХ СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. - ВЕСТНИК УРФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ - Номер: 3 (37) Год: 2020 Страницы: 27-33 https://elibrary.ru/item.asp?id=44306108
4	Дополнительная литература	eLIBRARY.RU	БОЧКАРЕВА Т.О., КОВШИКОВ В.А., БОГАТИКОВ В.Н. СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ. - АКТУАЛЬНЫЕ ПРОБЛЕМЫ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ УИС сборник трудов конференции Год издания: 2016 Страницы: 67-70 https://elibrary.ru/item.asp?id=27597207
5	Основная литература	eLIBRARY.RU	ЧЕРНОКНИЖНЫЙ Г. М. АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ. учебное пособие. - Год издания: 2020 Место издания: Санкт-ПетербургЧисло страниц: 90 https://elibrary.ru/item.asp?id=46410288
6	Основная литература	eLIBRARY.RU	ШАНЬГИН В.Ф. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ. учебное пособие Год издания: 2017 Место издания: Саратов Число страниц: 702 https://elibrary.ru/item.asp?id=29994910
7	Основная литература	Электронно-библиотечная система издательства Лань	Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. https://e.lanbook.com/book/180093
8	Основная литература	Электронно-библиотечная	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А.

		система издательства Лань	Ахрамееева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с. https://e.lanbook.com/book/180100
9	Дополнительная литература	Электронно-библиотечная система издательства Лань	Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с. https://e.lanbook.com/book/163812
10	Дополнительная литература	Электронно-библиотечная система издательства Лань	Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с. https://e.lanbook.com/book/163932

Перечень используемого программного обеспечения:

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

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(31.12.2022)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (3б)	Автоматизированные рабочие места (на базе ОС Windows 10). Программные средства управления доступом к данным: Secret Net 8.5 (автономный вариант), Страж 4.0. Программные средства шифрования ViPNet Custom 4.4. Межсетевые экраны ViPNet, Custom 4.4. Программные средства дублирования и восстановления данных Cobian Backup 11. Средства мониторинга состояния автоматизированных систем AlienVault OSSIM SIEM
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows 7 , MS Office 2016, Matlab, WinRar, Mozila Firefox, Консультант+.
Лабораторные занятия	906 (3б)	Средство антивирусной защиты Kaspersky Endpoint Security; Программно-аппаратный комплекс защиты информации от несанкционированного доступа - Secret Net 8.5 (включая аппаратные средства аутентификации пользователя); Межсетевой экран ViPNet Custom 4.4 (включающий криптографические средства защиты информации); Средство сканирования защищенности компьютерных сетей Ревизор Сети 3.0; Устройство чтения смарт-карт и радиометок PC-Linked Smart Card Reader ACR3901; ПО: Windows 7, Консультант+