

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и
компьютерных наук



А. В. Голлай

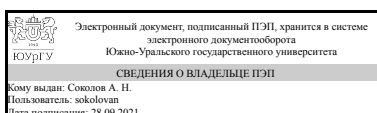
РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.21 Программно-аппаратные средства обеспечения
информационной безопасности
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

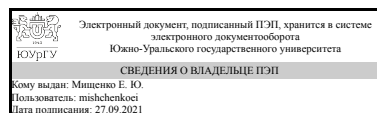
Рабочая программа составлена в соответствии с ФГОС ВО по направлению
подготовки 10.05.03 Информационная безопасность автоматизированных систем,
утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,
старший преподаватель



Е. Ю. Мищенко

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 (ЗУНы)
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Знать: программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
	Уметь: проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
	Владеть:
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать: программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
	Уметь: проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы

	Владеть:навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать:принципы организации информационных систем в соответствии с требованиями по защите информации
	Уметь:формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеть:навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.28 Безопасность операционных систем, Б.1.27 Безопасность сетей электронных вычислительных машин	В.1.08 Основы аттестации объектов информатизации критически важных объектов

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

Дисциплина	Требования
Б.1.27 Безопасность сетей электронных вычислительных машин	штатные средства защиты сетей
Б.1.28 Безопасность операционных систем	штатные средства защиты ОС

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 6 з.е., 216 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		7	8
Общая трудоёмкость дисциплины	216	108	108
<i>Аудиторные занятия:</i>	96	48	48
Лекции (Л)	48	32	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	0	16
Лабораторные работы (ЛР)	32	16	16
<i>Самостоятельная работа (СРС)</i>	120	60	60
Подготовка к лабораторным работам, оформление	54	27	27

результатов			
Курсовая работа	33	0	33
Изучение материалов по плану СРС	33	33	0
Вид итогового 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	6	6	0	0
4	Подсистема контроля доступа пользователей к ресурсам	14	6	0	8
5	Подсистема регистрации и учета	10	2	0	8
6	Подсистема контроля целостности	12	4	4	4
7	Подсистема криптографической защиты	8	4	2	2
8	Межсетевое экранирование	8	4	2	2
9	Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации	12	8	4	0
10	Виртуальные частные сети	13	7	2	4
11	Контроль защищенности информации	9	3	2	4

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	Документ РД МЭ, классы защищенности межсетевых экранов	2
4	3	Документ РД НДВ, уровни отсутствия недекларированных возможностей	2
5	3	Система сертификация средств защиты информации	2
6	4	Идентификация, аутентификация. Аппаратные и программные средства санкционированной загрузки. Авторизация. Аппаратные ключи пользователей	2
7	4	Дискреционный доступ. Реализация разграничения доступа к внешним устройствам	2
8	4	Мандатный доступ, его реализация для файлов, папок и процессов. Управление потоками информации	2
9	5	Регистрация событий в ОС и СЗИ. Реализация маркировки и учета документов. Гарантированное удаление информации	2
10	6	Контроль целостности файлов и папок. Контроль нарушения аппаратной конфигурации. Санкционированное использование внешних носителей	2
11	6	Замкнутая программная среда. Особенности реализации в различных СЗИ	2
12	7	Хранение информации в зашифрованном виде. Монопольный и коллективный доступ к контейнерам. Особенности реализации в различных СЗИ	2

13	7	Протокол Kerberos 5 в доменных сетях	2
14	8	Фильтрация пакетов. Трансляция сетевых адресов. Администрирование МЭ, схемы применения. Особенности реализации в различных СЗИ	4
15	9	Симметричное шифрование, ГОСТ 28147-89	2
16	9	ЭЦП, и асимметричное шифрование, хеширование. ГОСТ Р 34.10-2001, ГОСТ 34.11-94	4
17	9	Проблемы распределения и управления ключевой информацией. Система сертификация средств криптографической защиты информации	2
18	10	Центр управления сетью. Адресация	2
19	10	Ключевой удостоверяющий центр	2
20	10	Криптошлюз, клиент сети. Закрытый и открытый трафик. Туннелирование. Особенности реализации в различных СЗИ	3
21	11	Средства контроля защищенности информации для различных подсистем защиты	3

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	6	Подсистема контроля целостности	4
2	7	Подсистема криптографической защиты	2
3	8	Межсетевое экранирование	2
4	9	Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации	4
5	10	Виртуальные частные сети	2
6	11	Контроль защищенности информации	2

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	4	Аппаратные и программные средства санкционированной загрузки.	2
2	4	Авторизация. Аппаратные ключи пользователей.	2
3	4	Реализация разграничения доступа к внешним устройствам.	2
5	4	Управление потоками информации.	2
6	5	Регистрация событий входа-выхода, запуска задач.	2
7	5	Регистрация событий администрирования, доступа к объектам.	2
8	5	Реализация маркировки и учета документов.	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
13	7	Хранение информации в шифрованном виде. Монопольный и коллективный доступ к контейнерам. Особенности реализации в различных СЗИ.	2
14	8	Фильтрация пакетов.	2
16	10	Центр управления сетью. Адресация.	2
17	10	Ключевой удостоверяющий центр.	2
20	11	Средства контроля защищенности информации для подсистемы контроля доступа.	2

21	11	Средства контроля защищенности информации для подсистемы контроля целостности.	2
----	----	--	---

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Подготовка к лабораторным работам, оформление результатов	Основная литература	27
Изучение материалов по плану СРС	Дополнительная литература	33
Подготовка к лабораторным работам, оформление результатов	Основная литература	27
Курсовая работа	Дополнительная литература	33

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
анализ нормативно-методических документов	Лекции	анализ преимуществ и недостатков практического применения НМД	6

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
расширенный набор СЗИ	в лабораторных работах по всем темам применяется расширенный набор СЗИ

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-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	зачет	1-30
Все разделы	ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	зачет	1-30

Все разделы	ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	экзамен	1-50 и 1-30 тест
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	экзамен	1-50 и 1-30 тест

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
зачет	студенты в аудитории письменно отвечают на 3 вопроса теста, который включает теоретические и практические вопросы по пройденным разделам, преподаватель проверяет, беседует и оценивает	Зачтено: знает основной материал дисциплины; верно излагает и интерпретирует знания; изложение материала логически выстроено Не зачтено: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания
экзамен	студенты в аудитории письменно отвечают на теоретический и практический вопросы и один вопрос теста, который включает теоретические и практические вопросы по пройденным разделам, преподаватель проверяет, беседует и оценивает	Отлично: даны полные, развёрнутые ответы на теоретический, практический вопросы и один вопрос из теста по пройденным разделам Хорошо: даны либо неполные ответы на теоретический, практический вопросы и один вопрос из теста, либо при полных ответах на два вопроса дан неправильный ответ на вопрос теста Удовлетворительно: даны либо неполные ответы на теоретический или практический вопрос и неправильный ответ на вопрос теста, либо при одном полном ответе даны два неправильных ответа на остальные вопросы Неудовлетворительно: даны либо неполные ответы на теоретический или практический вопрос и неправильные ответы на два остальных вопроса, либо даны неправильные ответы на все три вопроса

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
зачет	см. файл 5 Тесты ПАЗИ.docx
экзамен	см. файлы Экзамен ПАЗИ.docx; 5 Тесты ПАЗИ.docx

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:

г) методические указания для студентов по освоению дисциплины:

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

из них: учебно-методическое обеспечение самостоятельной работы студента:

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

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	ШАНЬГИН В.Ф. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ. учебное пособие Год издания: 2017 Место издания: Саратов Число страниц: 702	eLIBRARY.RU	ЛокальнаяСеть / Свободный
2	Основная литература	ЧЕРНОКНИЖНЫЙ Г. М. АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ. учебное пособие. - Год издания: 2020 Место издания: Санкт-ПетербургЧисло страниц: 90	eLIBRARY.RU	Интернет / Свободный
3	Дополнительная литература	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	eLIBRARY.RU	Интернет / Свободный
4	Дополнительная литература	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	eLIBRARY.RU	Интернет / Свободный
5	Дополнительная	ИСАЕВА Ю. А., ГОЛДОБИНА А..С,	eLIBRARY.RU	Интернет /

	литература	НИКУЛИН Д. М. ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ЗНАЧИМЫХ ОБЪЕКТАХ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР РОССИЙСКОЙ ФЕДЕРАЦИИ. ИНТЕРЭКСПО ГЕО-СИБИРЬ - Том: 6 Номер: 1 Год: 2020 Страницы: 155-160		Свободный
6	Дополнительная литература	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	eLIBRARY.RU	Интернет / Свободный
7	Основная литература	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамеева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
8	Основная литература	Сертификация средств защиты информации : учебное пособие / А. А. Миняев, Юркин, М. М. Ковцур, К. А. Ахрамеева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 88 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
9	Дополнительная литература	Бульчев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Бульчев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
10	Дополнительная литература	Бульчев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Бульчев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -Консультант Плюс(31.07.2017)

10. 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 (36)	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
Лабораторные занятия	906 (36)	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: ОС Windows 7, Консультант+
Лекции	912 (36)	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+.