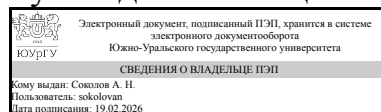


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности



А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.04 Защита информации в сети Интернет
для специальности 10.05.03 Информационная безопасность автоматизированных систем

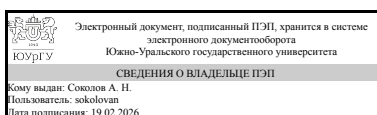
уровень Специалитет

форма обучения очная

кафедра-разработчик Защита информации

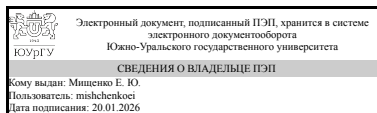
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

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



А. Н. Соколов

Разработчик программы,
к.техн.н., доцент



Е. Ю. Мищенко

1. Цели и задачи дисциплины

Подготовка специалистов в сфере защиты информации, передаваемой посредством сети "Интернет", ознакомление с основными понятиями безопасности, правовой защиты информации, подготовка к организации защиты компьютерных систем и сетей от несанкционированного доступа к хранимой информации. Задачи дисциплины: - изучение способов правовой защиты информации, распространяемой посредством сети "Интернет"; - изучение способов организационной защиты информации, распространяемой посредством сети "Интернет"; - изучение способов технической защиты информации, распространяемой посредством сети "Интернет"; - оценка эффективности существующих средств защиты; - изучение механизма организации централизованной антивирусной защиты.

Краткое содержание дисциплины

Дисциплина "Защита информации в сети "Интернет" относится к числу дисциплин вариативной части. Данная дисциплина включает в себя изучение технических, организационных и правовых средств защиты информации и ее носителей, а также позволяет овладеть технологиями защиты информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-5 Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	Знает: основные направления защиты информации в информационно-телекоммуникационных системах в соответствии с законодательством Российской Федерации; современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет Умеет: проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет; реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет Имеет практический опыт: использования антивирусного программного обеспечения для защиты информации в информационно-телекоммуникационных системах, подключенных к сети Интернет

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	1.Ф.09 Кибербезопасность автоматизированных систем управления технологическими процессами

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 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		10
Общая трудоёмкость дисциплины	144	144
<i>Аудиторные занятия:</i>	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	69,5	69,5
Самостоятельная работа	69,5	69,5
Консультации и промежуточная аттестация	10,5	10,5
Вид 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	Введение, Политика доступа	20	10	10	0
2	Атаки в сети "Интернет"	16	8	8	0
3	Архитектура браузера	28	14	14	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение, история WEB, устройство браузера	2
2	1	HTTP-протокол, DNS	2
3	1	HTTP-сессия. Понятия о Cookies	2
4	1	Политика одинакового происхождения. Подделка межсайтовых запросов	2
5	1	Политика одинакового происхождения. Исключения	2
1	2	Межсайтовый скриптинг	2
2	2	Атаки типа XSS	2
3	2	Противодействие атакам XSS	2
4	2	Приватность в сети "Интернет"	2
1	3	Отпечаток браузера (fingerprints)	2

2	3	Атаки типа UI DoS, фишинг и др.	2
3	3	Безопасность пользовательского интерфейса	2
4	3	Протокол защиты транспортного уровня	2
5	3	HSTS HPKP	2
6	3	Веб - Аутентификация	2
7	3	Архитектура браузера	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Установка NMap, Wireshark	2
2	1	Основы работы с NMap, Wireshark	2
3	1	Регулярные выражения. Принципы защиты и нападения	2
4	1	Сбор информации с использованием bash	2
5	1	Обработка данных	2
1	2	Анализ данных	2
2	2	Мониторинг журналов в режиме реального времени	2
3	2	Мониторинг сети	2
4	2	Контроль файловой системы	2
1	3	Добавление записей в журнал	2
2	3	Мониторинг доступности системы	2
3	3	Аудит учетных записей	2
4	3	Разведка, обфускация сценария	2
5	3	Ревизор сети	2
6	3	Сканер ВС	2
7	3	Анализ уязвимости информационной системы	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Самостоятельная работа	Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей.	10	69,5

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	Учитывается в ПА
1	10	Текущий контроль	Практическая работа №1	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла, Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	экзамен
2	10	Текущий контроль	Практическая работа №2	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла, Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	экзамен
3	10	Текущий контроль	Практическая работа № 3	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла, Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	экзамен
4	10	Текущий контроль	Практическая работа № 4	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла, Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	экзамен
5	10	Текущий контроль	Практическая работа № 5	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла, Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	экзамен
6	10	Текущий контроль	Практическая работа № 6	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла,	экзамен

						Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	
7	10	Текущий контроль	Практическая работа № 7	1	4	Все сделано и студент отвечает на вопросы и может выполнить дополнительное задание - 4 балла, Все сделано и студент отвечает на вопросы - 3 балла, Все сделано - 2 балла, Сделана хотя бы часть задания - 1 балл, Ничего не сделано - 0 баллов.	экзамен
21	10	Промежуточная аттестация	контрольная работа	-	10	выполнено верно 2 задания - 10 баллов, выполнено верно 1 задание - 5 баллов, Ничего не сделано - 0 баллов.	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	контрольная работа, 1 задание теоретическое, 1 задание практическое. Максимум 10 баллов	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	21
ПК-5	Знает: основные направления защиты информации в информационно-телекоммуникационных системах в соответствии с законодательством Российской Федерации; современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет	++			+			++	
ПК-5	Умеет: проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет; реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет			+					
ПК-5	Имеет практический опыт: использования антивирусного программного обеспечения для защиты информации в информационно-телекоммуникационных системах, подключенных к сети Интернет				+		+		

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:

1. Журнал "Вестник УРФО. Безопасность в информационной сфере"

г) методические указания для студентов по освоению дисциплины:

1. По дисциплине

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	ЭБС издательства Лань	Ворожевич, А. С. Современные информационные технологии и право : монография / А. С. Ворожевич, Е. В. Зайченко, Е. Е. Кирсанова ; под редакцией Е. Б. Лаутс. — Москва : СТАТУТ, 2019. — 288 с. — ISBN 978-5-8354-1578-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130674 (дата обращения: 01.07.2025). — Режим доступа: для авториз. пользователей.
2	Основная литература	ЭБС издательства Лань	Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717 (дата обращения: 01.07.2025). — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	ЭБС издательства Лань	Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 01.07.2025). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	ЭБС издательства Лань	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804 (дата обращения: 01.07.2025). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. Microsoft-Windows(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
-------------	--------	--

Лекции	615 (3)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows 10 , ОС Kali Linux, Mozilla Firefox
Практические занятия и семинары	626 (3)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows 10 , ОС Kali Linux, Mozilla Firefox