ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Ткачева Н. В.
Пользователь: tkachevanv
Дата подписания: 20.05.2022

Н. В. Ткачева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.09 Основы информационной безопасности в профессиональной деятельности
для специальности 40.05.02 Правоохранительная деятельность
уровень Специалитет
форма обучения заочная
кафедра-разработчик Конституционное и административное право

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 40.05.02 Правоохранительная деятельность, утверждённым приказом Минобрнауки от 28.08.2020 № 1131

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

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Титова Е. В.
Пользователь: ttovaev
Дата подписания: 20.05.2022

Е. В. Титова

Разработчик программы,
преподаватель

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Мамаев В. В.
Пользователь: vvmamaev
Дата подписания: 18.05.2022

В. В. Мамаев

Челябинск

1. Цели и задачи дисциплины

Цели: ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами РФ. Задачи: - приобретение студентами теоретических знаний и практических навыков защиты информации представленной в электронном виде, прежде всего средствами криптографии, типичными криптосистемами и другими методами, лежащими в ее основе; - получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации; - формирование у студентов навыков защиты информации в локальных и глобальных компьютерных сетях.

Краткое содержание дисциплины

В программу включены темы, связанные с изучением доктрины информационной безопасности Российской Федерации, национальными интересами в информационной сфере и их обеспечением, концептуальной модели информационной безопасности, а также видами и источниками угроз информационной безопасности и направлениями обеспечения информационной безопасности. Рассматриваются правовое, организационное и инженерно-техническое обеспечения информационной безопасности, основные угрозы и стратегии защиты компьютерной информации, криптографические методы защиты данных, антивирусная защита компьютеров; методы и средства получения информации в локальных и глобальных компьютерных сетях, анализ конфигурации персонального компьютера, поиск информации с помощью специальных шаблонов и масок; организационно-технические аспекты получения и передачи компьютерной информации, компьютерные преступления.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-2 Способность целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы (банки) данных, решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Имеет практический опыт: сбора, обработки, анализа и защиты юридически значимой информации с учетом основных требований информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.06 Основы делопроизводства, 1.Ф.07 Информатика	1.Ф.21 Практикум по виду профессиональной деятельности,

	1.Ф.15 Правоохранительная деятельность по обеспечению экономической безопасности, 1.О.17 Информационное право, 1.Ф.13 Практикум по основам оперативно-розыскной деятельности, 1.Ф.12 Основы оперативно-розыскной деятельности

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

Дисциплина	Требования
1.Ф.07 Информатика	Знает: информационно-коммуникационные технологии;основные приемы и средства визуализации информации; CRM-системы (управление взаимоотношениями с клиентами), протокол http, понятие URLпринципы работы поисковых машин, Определение искусственного интеллекта (ИИ), его уровни (сильный и слабый ИИ).Классификацию методов машинного обучения. Принципы формирования обучающих наборов данных. Умеет: применять информационно-коммуникационные технологии для решения профессиональных задач; Осуществлять поиск в сети Интернет, использовать Яндекс Взгляд, Google формы Имеет практический опыт:
1.Ф.06 Основы делопроизводства	Знает: принципы планирования индивидуальной и коллективной работы в рамках проекта подготовки распорядительных документов Умеет: определять оптимальные пути решения тактических задач в рамках поставленной цели на основе действующих правовых норм, имеющихся ресурсов и ограничений Имеет практический опыт: грамотного оформления юридических и служебных документов на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 18,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		5

Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	12	12
Лекции (Л)	4	4
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	8	8
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	89,75	89,75
с применением дистанционных образовательных технологий	0	
Поиск информации по теме: "Угрозы безопасности технических средств обработки информации"	14	14
Подготовка к зачету	7,75	7.75
Изучение нормативно-правовой базы по защите персональных данных	14	14
Поиск, изучение и анализ информации по теме: "Теоретические основы аутентификации"	10	10
Поиск информации по теме: "Концепции обеспечения информационной безопасности"	16	16
Изучение и анализ информации по теме: "Защита интеллектуальной собственности средствами патентного и авторского права"	10	10
Подготовка докладов на предложенные темы	18	18
Консультации и промежуточная аттестация	6,25	6,25
Вид 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	Введение в информационную безопасность. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности.	2	2	0	0
2	Механизмы обеспечения "информационной безопасности". Программно-аппаратные средства и методы обеспечения информационной безопасности.	5	1	4	0
3	Криптографические методы защиты информации. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей.	5	1	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.	2

2	2	Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Антивирусные программы. Правила защиты от компьютерных вирусов. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Адресация в глобальных сетях.	1
2	3	Инженерная защита объектов. Защита информации от утечки по техническим каналам. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Системы шифрования. Цифровые подписи (ЭЦП). Инфраструктура открытых ключей. Криптографические протоколы.	1

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Технические средства и методы защиты информации. Программные средства обеспечения информационной безопасности.	2
2	2	Криптография и шифрование. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Механизм электронной цифровой подписи. Компьютерные вирусы и информационная безопасность. Классификация компьютерных вирусов. Методы обнаружения компьютерных вирусов. Изучение настроек средств антивирусной защиты информации.	2
3	3	Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Методы профилактики заражения технических устройств и носителей компьютерными вирусами	2
4	3	Особенности обеспечения информационной безопасности в компьютерных сетях. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Адресация в глобальных сетях. Система доменных имен	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
Поиск информации по теме: "Угрозы безопасности технических средств обработки информации"	ЭУМД, доп. лит. №1 тема 2, доп. лит. №2 раздел 3	5	14
Подготовка к зачету	Все источники	5	7,75
Изучение нормативно-правовой базы по защите персональных данных	ЭУМД, доп. лит. №2 раздел 2, осн. лит. №5 глава 14	5	14
Поиск, изучение и анализ информации по теме: "Теоретические основы аутентификации"	ЭУМД, осн. лит. №5 главы 11-12	5	10
Поиск информации по теме: "Концепции обеспечения информационной	ЭУМД, осн. лит. №5 глава 2, справочно-правовая система по законодательству	5	16

безопасности"	Российской Федерации		
Изучение и анализ информации по теме: "Защита интеллектуальной собственности средствами патентного и авторского права"	ЭУМД, осн. лит. №4, глава 4, справочно-правовая система по законодательству Российской Федерации	5	10
Подготовка докладов на предложенные темы	Все источники	5	18

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-мест	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	5	Текущий контроль	Сумма оценок за текущие тестирования	0,6	40	В курсе представлено 8 тестов. За каждый можно получить максимум 5 баллов.	зачет
2	5	Текущий контроль	Подготовка докладов	0,4	20	Студенту предлагается подготовить 2 доклада по темам из списка. Каждый доклад приносит максимум 10 баллов. Балы начисляются следующим образом: Тема доклада раскрыта да - 6 баллов частично - 3 балла нет - 0 баллов Использована актуальная информация - 2 балла Использована устаревшая информация - 0 баллов Документ оформлен в соответствии с требованиям - 2 балла Документ не оформлен - 0 баллов	зачет
3	5	Проме-жуточная аттестация	Зачётный тест	-	40	Тест состоит из 30 вопросов. 1 правильный ответ - 1 балл. Ответ на теоретический вопрос оценивается следующим образом: Вопрос раскрыт полностью - 10 баллов Вопрос раскрыт с незначительными неточностями - 8 баллов Вопрос раскрыт со значительными	зачет

						неточностями, либо раскрыт частично - 6 баллов Вопрос не раскрыт - 0 баллов	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Оценивание знаний производится по результатам текущего контроля. В случае нехватки баллов сдаётся зачет. Зачет проходит в 2 этапа Тест состоит из 30 вопросов. 1 правильный ответ - 1 балл. Проходной балл за тест – 18 баллов. Ответ на теоретический вопрос оценивается следующим образом: Вопрос раскрыт полностью - 10 баллов Вопрос раскрыт с незначительными неточностями - 8 баллов Вопрос раскрыт со значительными неточностями, либо раскрыт частично - 6 баллов (минимальный балл) Вопрос не раскрыт - 0 баллов Для получения оценки «зачтено» необходимо прохождение обоих этапов на минимальную оценку.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ		
		1	2	3
ПК-2	Имеет практический опыт: сбора, обработки, анализа и защиты юридически значимой информации с учетом основных требований информационной безопасности	+	+	+

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:

1. Закиров, Р. Ш. Информационная безопасность [Текст] конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия

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

1. Вестник УрФО : Безопасность в информационной сфере Юж.-Урал. гос. ун-т; ЮУрГУ журнал. - Челябинск: Издательство ЮУрГУ, 2011-

г) методические указания для студентов по освоению дисциплины:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования /

А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525 (дата обращения: 30.01.2022).

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525 (дата обращения: 30.01.2022).

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Образовательная платформа Юрайт	Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476294 (дата обращения: 02.11.2021)
2	Дополнительная литература	Образовательная платформа Юрайт	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 02.11.2021)
3	Основная литература	Образовательная платформа Юрайт	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968 (дата обращения: 02.11.2021)
4	Основная литература	Образовательная платформа Юрайт	Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476798 (дата обращения: 02.11.2021)
5	Основная литература	Образовательная платформа Юрайт	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:

			https://urait.ru/bcode/469133 (дата обращения: 02.11.2021)

Перечень используемого программного обеспечения:

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

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. -База данных polpred (обзор СМИ)(бессрочно)
2. -База данных ВИНИТИ РАН(бессрочно)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	206 (8Э)	Рабочее место преподавателя. Компьютер конфигурации: Pentium-915 2800/1024Mb/250G Устройства коммутации и усиления аудио и видеосигналов, звуковая система. Проектор BenQ, проекционный экран. парты аудиторные- 40 шт. Посадочных мест -160 Окна -7 шт. Вх. двери-2 шт.
Практические занятия и семинары	112 (8Э)	Компьютер (рабочее место пользователя) - 16 шт. (Системный блок Intel 10 series/c 230/Celeron G3930 2.9GHz/4Gb/500Gb, монитор Samsung 943 LCD 19", клавиатура, мышь); системное программное обеспечение Windows 7 pro (тип лицензии: DreamSpark Retail Key), прикладное программное обеспечение Офисный пакет Microsoft 2007 (тип лицензии: Подписка MSDN (44938187))
Самостоятельная работа студента	112 (8Э)	Компьютер (рабочее место пользователя) - 16 шт. (Системный блок Intel 10 series/c 230/Celeron G3930 2.9GHz/4Gb/500Gb, монитор Samsung 943 LCD 19", клавиатура, мышь); системное программное обеспечение Windows 7 pro (тип лицензии: DreamSpark Retail Key), прикладное программное обеспечение Офисный пакет Microsoft 2007 (тип лицензии: Подписка MSDN (44938187))