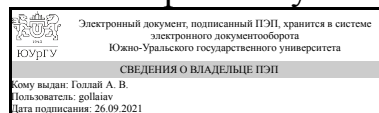


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и
компьютерных наук



А. В. Голлай

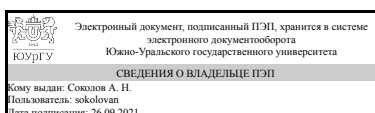
РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.41 Компьютерная экспертиза
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

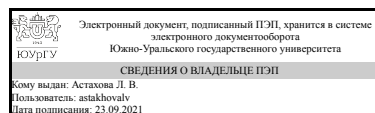
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,
д.пед.н., проф., профессор



Л. В. Астахова

1. Цели и задачи дисциплины

Цель: приобретение слушателями знаний, умений и навыков экспертного исследования объектов компьютерной экспертизы. Задачи: - изучение теоретических основ компьютерной экспертизы (далее - КЭ); - освоение понятийного аппарата КЭ; - изучение правил обращения с объектами КЭ; - овладение современными технологиями и методами экспертного исследования объектов КЭ; - приобретение навыков работы в качестве специалиста по защите информации в процессе расследования преступлений; - развитие у обучаемых потребности к самообразованию и постоянному повышению своего профессионального уровня; - привитие обучаемым творческого, научного отношения к процессу экспертного исследования.

Краткое содержание дисциплины

Дисциплина посвящена изучению теоретических основ компьютерной экспертизы (КЭ); изучению правил обращения с объектами КЭ; овладению современными технологиями и методами экспертного исследования объектов КЭ; приобретение навыков работы в качестве специалиста по защите информации в процессе расследования преступлений.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знать: систему документационного обеспечения компьютерной экспертизы
	Уметь: разрабатывать документы на все этапах компьютерной экспертизы
	Владеть: алгоритмами разработки научно-технической документации
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать: нормативные правовые акты в области компьютерных преступлений и компьютерной экспертизы
	Уметь: применять нормативные правовые акты в профессиональной деятельности
	Владеть: технологиями применения нормативных правовых актов в профессиональной деятельности
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Знать: методики исследования каналов утечки информации
	Уметь: применять методики исследования каналов утечки информации на практике
	Владеть: технологиями исследования каналов утечки информации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
---	---

Б.1.30.01 Разработка защищенных автоматизированных систем, В.1.06 Контроль безопасности автоматизированных систем	В.1.10 Методы и средства противодействия террористической деятельности в системах управления 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.1.30.01 Разработка защищенных автоматизированных систем	Знать технологии разработки защищенных автоматизированных систем, уметь их применять в процессе компьютерной экспертизы
В.1.06 Контроль безопасности автоматизированных систем	Знать технологии контроля безопасности автоматизированных систем, иметь навыки контроля и уметь применять их в процессе компьютерной экспертизы

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	
		9	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	48	48	
Лекции (Л)	32	32	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	60	60	
Моделирование этапов КЭ	60	60	
Вид итогового 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. Базовые понятия курса.	4	2	2	0
2	Правовые и организационные основы компьютерной экспертизы	8	6	2	0
3	Этапы компьютерной экспертизы: сбор, анализ, оценка и оформление данных.	10	6	4	0
4	Методики производства компьютерной экспертизы	10	6	4	0
5	Инструментальные средства производства компьютерной экспертизы.	10	8	2	0
6	Проблемы и перспективы производства компьютерной	6	4	2	0

экспертизы.				
-------------	--	--	--	--

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение. Базовые понятия курса.	2
2	2	Правовые основы компьютерной экспертизы	2
3	2	Организационные основы компьютерной экспертизы	4
4	3	Этапы компьютерной экспертизы: сбор, анализ, оценка	4
5	3	Этапы компьютерной экспертизы: оформление данных.	2
6	4	Методики производства аппаратно-компьютерной экспертизы	2
7	4	Методики программно-компьютерной экспертизы, экспертизы данных и сетевой экспертизы	4
8	5	Инструментальные средства производства программно-компьютерной экспертизы.	4
9	5	Инструментальные средства производства других видов компьютерной экспертизы.	4
10	6	Проблемы и перспективы производства компьютерной экспертизы.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Введение. Базовые понятия курса.	2
2	2	Правовые и организационные основы компьютерной экспертизы	2
3	3	Этапы компьютерной экспертизы: сбор, анализ, оценка и оформление данных.	4
4	4	Методики производства компьютерной экспертизы	4
5	5	Инструментальные средства производства компьютерной экспертизы.	2
6	6	Проблемы и перспективы производства компьютерной экспертизы.	2

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
Моделирование этапов КЭ	1. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации / А.С. Масалков. — Москва : ДМК Пресс, 2018. — 226 с. — ISBN 978-5-97060-651-3. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/105842 (дата обращения: 01.09.2019). — Режим	60

	<p>доступа: для авториз. пользователей. 2. Бузов, Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации : справочное пособие / Г.А. Бузов. — Москва : Горячая линия-Телеком, 2015. — 240 с. — ISBN 978-5-9912-0121-6. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/111026 (дата обращения: 02.09.2019). — Режим доступа: для авториз. пользователей. 3. Пискунова, Е. В. Компьютерные технологии в судебно-экспертной деятельности : учебное пособие / Е. В. Пискунова ; под редакцией Т. Ф. Моисеевой. — Москва : РГУП, 2016. — 152 с. — ISBN 978-5-93916-531-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/123181 (дата обращения: 03.09.2020). — Режим доступа: для авториз. пользователей. 4. Шелупанов А.А., Смолина А.Р. Форе́нзика. Теория и практика расследования киберпреступлений. — М.: Горячая линия - Телеком, 2018. — 104 с. 5. Федотов, Николай Николаевич. Форе́нзика-компьютерная криминалистика / Николай Николаевич Федотов. - 2-е изд. - Москва : Onebook.ru, 2012. - 418, [1] с. : ил. ; 25 см. - Библиогр.: с. 391-398. - 1000 экз. - ISBN 978-5-905948-22-0 (в пер.) 6. Макарян, Александр Самвелович. Форе́нзика. Анализ цифровых криминалистических данных / Макарян Александр Самвелович, Швырев Борис Анатольевич ; Федеральная служба исполнения наказаний, Научно-исследовательский институт ФСИН России. - Москва : НИИ ФСИН России, 2018. - 171 с. ; 21 см. - Библиогр. в конце гл. - 500 экз. - ISBN 978-5-6042090-4-2</p>	
--	---	--

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Разработка инновационных методик производства КЭ	Самостоятельная работа студента	Разработка инновационных методик производства КЭ с использованием новых технологий	10

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Проблемное обучение	Выявление проблем производства КЭ и поиск путей их решения в России и за рубежом

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-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Письменный опрос или тест	1-7
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Письменный опрос или тест	1-7
Все разделы	ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Письменный опрос или тест	1-7
Все разделы	ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Защита Отчета о практической работе	1-7
Все разделы	ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Зачет	1-7
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Посещаемость занятий	1-7

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Письменный опрос или тест	Письменный опрос осуществляется на последнем занятии изучаемого раздела. Студенту задаются 5 вопросов из списка контрольных вопросов. Время, отведенное на опрос -20 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Правильный ответ на вопрос соответствует 2 баллам. Частично правильный ответ соответствует 1 баллу. Неправильный ответ на вопрос	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Не зачтено: Рейтинг обучающегося за мероприятие меньше

	<p>соответствует 0 баллов. Вместо письменного опроса может проводиться тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов – 10. Весовой коэффициент мероприятия (за каждый письменный опрос) – 0,05.</p>	60 %.
Защита Отчета о практической работе	<p>Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, своевременность выполнения работы и ответы на вопросы (задаются 2-3 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей (за каждое практическое задание): - правильность оформления отчета, если отчет оформлен с недочетами из оценки вычитается 1 балл; - своевременность сдачи отчета, за каждую неделю просрочки отчета из оценки вычитается 0,5 балла; - ответы на вопросы, оценка снижается на 1 балл за каждый неправильный ответ на вопрос. Максимальное количество баллов за одну работу – 10. Весовой коэффициент мероприятия (за каждую работу) – 0,05.</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %</p>
Зачет	<p>Оценка «зачтено» ставится по результатам работы в семестре на основе использования балльно-рейтинговой системы оценки деятельности студентов. Балльно-рейтинговая система базируется на учете следующих основных критериев: 1. Степень освоения теоретического материала, которая определяется по результатам выполнения студентами контрольных работ или проведения тестирования. Контрольные работы предусматривают проверку знаний, в соответствии с перечнем вопросов. В первом семестре предусматривается проведение одной контрольной работы с максимальной оценкой 10 баллов. Вместо контрольной работы возможно проведение тестирования. 2. Достигнутый уровень практических навыков, определяемый по результатам самостоятельного выполнения заданий к лабораторным работам с общей максимальной оценкой 77 баллов. 3. Посещаемость лекционных и лабораторных занятий с общей максимальной оценкой 13 баллов. Максимальная оценка, которую может получить студент при выполнении всех заданий, составляет 100 баллов.</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %.</p>
Посещаемость занятий	<p>Отмечается присутствие студента на занятиях. За каждое посещение прибавляется 0,4 балла. Максимальное количество баллов за 1-й семестр равно 19,2</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %.</p>

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Письменный опрос или тест	2. В чем заключается сущность этапа сбора данных для проведения компьютерной экспертизы? а. В опросе лиц, имеющих отношение к инциденту б. В составлении плана по реагированию в критических ситуациях с. В правильном оформлении улик д. В создании копий всех данных специализированными средствами ФОС_Оформление результатов.docx; ФОС_Контрфорензика.docx; ФОС__Анализ данных.docx; Форензика.docx
Защита Отчета о практической работе	
Зачет	
Посещаемость занятий	

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:

1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"
2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн
3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"
4. Безопасность информационных технологий ,12+ ,М-во образования и науки Рос. Федера-ции, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ
5. Вестник УрФО : Безопасность в информационной сфере ,Юж.-Урал. гос. ун-т; ЮУрГУ
6. Судебная экспертиза: науч.-практ. журн., Саратов. юрид. ин-т МВД России
7. Судебная экспертиза:науч.-практ. журн. Волгоград. акад. МВД России
8. 3. Журнал «Компьютерно-техническая экспертиза» (издается с 2007 г.) https://e.lanbook.com/journal/2692#journal_name

г) методические указания для студентов по освоению дисциплины:

1. Астахова Л.В._Методика производства КТЭ_Методическое пособие
2. Методические указания "Компьютерная экспертиза" для студентов образовательного направления "ИНформационная безопасность"
3. Компьютерная экспертиза_Лекционный материал

4. Компьютерная криминалистика

из них: учебно-методическое обеспечение самостоятельной работы студента:

5. Астахова Л.В. _Методика производства КТЭ_ Методическое пособие
6. Методические указания "Компьютерная экспертиза" для студентов образовательного направления "Информационная безопасность"
7. Компьютерная экспертиза_Лекционный материал
8. Компьютерная криминалистика

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации / А.С. Масалков. — Москва : ДМК Пресс, 2018. — 226 с. — ISBN 978-5-97060-651-3. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/105842 (дата обращения: 01.09.2019). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	Бузов, Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации : справочное пособие / Г.А. Бузов. — Москва : Горячая линия-Телеком, 2015. — 240 с. — ISBN 978-5-9912-0121-6. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/111026 (дата обращения: 02.09.2019). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Основная литература	Васильева И.Н. Расследование инцидентов информационной безопасности: Учебное пособие / Санкт-Петербург: Издательство: Санкт-Петербургский государственный экономический университет, 2019. 113 с.	eLIBRARY.RU	Интернет / Авторизованный
4	Основная литература	Макарян, Александр Самвелович. Форензика. Анализ цифровых криминалистических данных / Макарян Александр Самвелович, Швырев Борис Анатольевич ; Федеральная служба исполнения наказаний, Научно-исследовательский институт ФСИН России. - Москва : НИИ ФСИН России, 2018. - 171 с. ; 21 см. - Библиогр. в конце гл. - 500 экз. -	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

		ISBN 978-5-6042090-4-2		
5	Дополнительная литература	Пискунова, Е. В. Компьютерные технологии в судебно-экспертной деятельности : учебное пособие / Е. В. Пискунова ; под редакцией Т. Ф. Моисеевой. — Москва : РГУП, 2016. — 152 с. — ISBN 978-5-93916-531-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/123181 (дата обращения: 03.09.2020). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
6	Дополнительная литература	Федотов, Николай Николаевич. Форензика-компьютерная криминалистика / Николай Николаевич Федотов. - 2-е изд. - Москва : Onebook.ru, 2012. - 418, [1] с. : ил. ; 25 см. - Библиогр.: с. 391-398. - 1000 экз. - ISBN 978-5-905948-22-0 (в пер.)	eLIBRARY.RU	Интернет / Свободный

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. ООО "ГарантУралСервис"-Гарант(бессрочно)
2. EBSCO Information Services-EBSCOhost Research Databases(бессрочно)
3. -Техэксперт(30.10.2017)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+.
Практические занятия и семинары	913 (36)	Комплект компьютерного оборудования, проектор, коммутатор, экран для проектора, программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Virtual Box, Ms Visual Studio Express. Операционные системы семейства Linux, Windows, СУБД промышленного масштаба (например, Microsoft SQL Server 2010, Oracle 9i и т.п), свободно распространяемые пакеты прикладных программ: утилиты резервного копирования и восстановления файловых систем и разделов НЖМД; средства диагностики и тестирования ПК; межсетевые экраны; системы обнаружения вторжений; антивирусы.