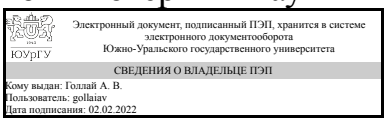
**ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



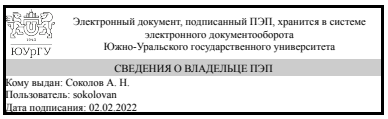

А. В. Голлай

# РАБОЧАЯ ПРОГРАММА

**дисциплины** В.1.05 Практикум по виду профессиональной деятельности
**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

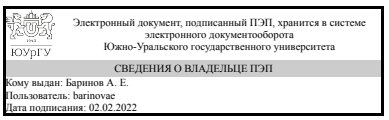
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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




А. Н. Соколов

Разработчик программы,
старший преподаватель




А. Е. Баринов

Челябинск

## 1. Цели и задачи дисциплины

Цели: Получение практических навыков научно-исследовательской и проектно-конструкторской деятельности в лабораторных и производственных условиях путем непосредственного участия студентов в решении актуальных производственных и научно-технических задач с раскрытием индивидуальных особенностей и способностей. Задачи: Подготовка студентов к самостоятельной работе в сфере информационной безопасности. Применение студентами знаний и умений, полученных при изучении дисциплин специальности для решения междисциплинарных задач в сфере информационной безопасности. Овладение навыками анализа имеющихся ресурсов и управления ими для решения поставленных задач обеспечения защиты информации.

## Краткое содержание дисциплины

Практикум предполагает решение задач полного цикла обеспечения информационной безопасности объекта информатизации, начиная от анализа угроз до построения комплексной системы защиты. При этом обучающиеся вовлекаются во все аспекты обеспечения ее информационной безопасности: организационные, программно-аппаратные и технические.

## 2. Компетенции обучающегося, формируемые в результате освоения дисциплины

| Планируемые результаты освоения ОП ВО (компетенции) | Планируемые результаты обучения по дисциплине (ЗУНы) |
|---|---|
| ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности | Знать:принципы организации информационных систем в соответствии с требованиями по защите информации |
| | Уметь:разрабатывать частные политики информационной безопасности информационных (автоматизированных) систем |
| | Владеть:профессиональной терминологией в области информационной безопасности |
| ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций | Знать:принципы организации информационных систем в соответствии с требованиями по защите информации |
| | Уметь:разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем |
| | Владеть:навыками выбора и обоснования критериев эффективности функционирования защищенных информационных (автоматизированных) систем |
| ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем | Знать:организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы |
| | Уметь:осуществлять управление и администрирование защищенных |

| | |
|---|---|
| | автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем |
| | Владеть:навыками разработки политик информационной безопасности автоматизированных систем |
| ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | 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 автоматизированных систем с целью обеспечения требуемого уровня ее защищенности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю |
| | Владеть: |
| ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы | Знать:принципы формирования политики информационной безопасности в информационных (автоматизированных) системах |
| | Уметь:формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе |
| | Владеть:методами управления информационной безопасностью информационных (автоматизированных) систем |
| ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы | Знать:отечественные и зарубежные стандарты в области информационной безопасности |
| | Уметь:применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем |
| | Владеть: |
| ПК-3 способностью проводить анализ защищенности автоматизированных систем | Знать:методики расчета и инструментального контроля показателей технической защиты информации |
| | Уметь: |
| | Владеть:методами расчета и инструментального контроля показателей технической защиты информации |
| ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности | Знать:безопасные сетевые технологии, в которых используются программно-аппаратные средства обеспечения информационной безопасности автоматизированных систем |
| | Уметь: |
| | Владеть:навыками применения программно- |

| | |
|---|---|
| | аппаратных средств обеспечения информационной безопасности автоматизированных систем |
| ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | Знать:основные угрозы безопасности информации и модели нарушителя в информационных (автоматизированных) системах |
| | Уметь:анализировать и оценивать угрозы информационной безопасности информационных (автоматизированных) систем |
| | Владеть:методами мониторинга угроз информационной безопасности информационных (автоматизированных) систем |

## 3. Место дисциплины в структуре ОП ВО

| Перечень предшествующих дисциплин, видов работ учебного плана | Перечень последующих дисциплин, видов работ |
|---|---|
| Б.1.17 Основы информационной безопасности,<br>Б.1.27 Безопасность сетей электронных вычислительных машин,<br>Б.1.28 Безопасность операционных систем | В.1.08 Основы аттестации объектов информатизации критически важных объектов,<br>Б.1.43 Аудит информационной безопасности,<br>Б.1.30.02 Эксплуатация защищенных автоматизированных систем |

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 | Знать структуру и способы организации сетей, уметь строить карту сетей различных классов, владеть навыками использования программных средств и методов обеспечения безопасности сетей ЭВМ. |
| Б.1.28 Безопасность операционных систем | Знать основные виды и классы операционных систем, методологически и практические подходы к обеспечению безопасности ОС, основные программно-аппаратные средства защиты информации в ОС. Уметь использовать на практике базовые средства безопасности ОС различных классов. |
| Б.1.17 Основы информационной безопасности | Знать структуру комплексной системы защиты информации, состав видов защиты информации, основное действующее законодательство в области защиты информации. Уметь определять структуру КСЗИ, формулировать требования и состав к конкретной КСЗИ. |

## 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 | | |
| | | 6 | 7 | 8 |
| Общая трудоёмкость дисциплины | 216 | 72 | 72 | 72 |
| *Аудиторные занятия:* | 128 | 64 | 32 | 32 |
| Лекции (Л) | 0 | 0 | 0 | 0 |
| Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ) | 128 | 64 | 32 | 32 |
| Лабораторные работы (ЛР) | 0 | 0 | 0 | 0 |
| *Самостоятельная работа (СРС)* | 88 | 8 | 40 | 40 |
| Изучение стандартов и и документирования процедур по обеспечению ИБ. | 40 | 0 | 0 | 40 |
| Поиск и аналитико-синтетическая обработка информации по проблемам ИБ | 48 | 8 | 40 | 0 |
| Вид итогового контроля (зачет, диф.зачет, экзамен) | - | зачет | зачет | экзамен |

## 5. Содержание дисциплины

| № раздела | Наименование разделов дисциплины | Объем аудиторных занятий по видам в часах | | | |
|---|---|---|---|---|---|
| | | Всего | Л | ПЗ | ЛР |
| 1 | Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность) | 64 | 0 | 64 | 0 |
| 2 | Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность) | 32 | 0 | 32 | 0 |
| 3 | Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность) | 32 | 0 | 32 | 0 |

### 5.1. Лекции

Не предусмотрены

### 5.2. Практические занятия, семинары

| № занятия | № раздела | Наименование или краткое содержание практического занятия, семинара | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Методика НИР: основные этапы | 6 |
| 2 | 1 | Поиск и формулировка проблемы ИБ, составление перечня ключевых слов. | 6 |
| 3 | 1 | Поиск научной литературы в русскоязычных электронных ресурсах | 6 |
| 4 | 1 | Поиск научной литературы в зарубежных электронных ресурсах | 6 |
| 5 | 1 | Поиск экспертной информации по проблеме | 6 |
| 6 | 1 | Поаспектная систематизация и отбор выявленной литературы | 6 |
| 7 | 1 | Поаспектное реферирование выявленной литературы | 6 |
| 8 | 1 | Аналитико-синтетическая переработка информации | 6 |
| 9 | 1 | Подготовка текста по научной проблеме ИБ | 6 |
| 10 | 1 | Оформление текста и Списка использованной литературы, подготовка Презентации. | 6 |

| | | | |
|---|---|---|---|
| 11 | 1 | Защита НИР | 4 |
| 12 | 2 | Изучение системы нормативных правовых документов по ПД: ФЗ, постановления правительства РФ. | 6 |
| 13 | 2 | Изучение системы нормативных правовых документов по ПД: документы ФСТЭК РФ. | 6 |
| 14 | 2 | Изучение системы нормативных правовых документов по ПД: документы ФСБ РФ. | 6 |
| 15 | 2 | Определение актуальных угроз безопасности ИСПДн | 6 |
| 16 | 2 | Разработка Модели угроз безопасности ГИС (МИС) | 6 |
| 17 | 2 | Определение актуальных угроз безопасности по отраслевым стандартам | 2 |
| 18 | 3 | Разработка Модели нарушителя | 6 |
| 19 | 3 | Изучение требований к ТЗ | 6 |
| 20 | 3 | Разработка ТЗ на обеспечение безопасности ИСПДн | 6 |
| 21 | 3 | Разработка ТЗ на обеспечение безопасности ГИС (МИС) | 6 |
| 22 | 3 | Организационные аспекты реализации ТЗ | 6 |
| 23 | 3 | Защита ТЗ | 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 |
| Поиск и аналитико-синтетическая обработка информации по проблеме | Электронные ресурсы НБ ЮУрГУ | 40 |
| Изучение стандартов по обеспечению ИБ | Комплекс БР ИББС, PCI DSS и др. нормативных документов | 48 |

## 6. Инновационные образовательные технологии, используемые в учебном процессе

| Инновационные формы учебных занятий | Вид работы (Л, ПЗ, ЛР) | Краткое описание | Кол-во ауд. часов |
|---|---|---|---|
| Проектные технологии обучения | Практические занятия и семинары | Проектирование системы защиты информации в организации N. | 64 |

## 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 ИБ и путей их решения в России и за рубежом (1 раздел) |

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 |
|---|---|---|---|
| Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность) | ПК-3 способностью проводить анализ защищенности автоматизированных систем | Защита отчета о выполнении задания | 1-11 |
| Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность) | ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | Защита отчета о выполнении задания | 1-11 |
| Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность) | ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы | Защита отчета о выполнении задания | 1-11 |
| Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность) | ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | Защита отчета о выполнении задания | 12-22 |
| Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность) | ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем | Защита отчета о выполнении задания | 12-22 |
| Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность) | ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности | Защита отчета о выполнении задания | 12-22 |
| Все разделы | ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | Посещение занятий | 1-22 |
| Все разделы | ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | Бонус-рейтинг: Участие в научной конференции | 1-22 |

### 7.2. Виды контроля, процедуры проведения, критерии оценивания

| Вид контроля | Процедуры проведения и оценивания | Критерии оценивания |
|---|---|---|
| Защита отчета о выполнении задания | Защита отчета о выполнении задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 2 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 складывается из следующих показателей (за каждое задание): - приведены методики выполнения работы – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 1 балл Максимальное количество баллов – 5. Весовой коэффициент мероприятия (за каждое задание) – 0,1. | Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %. |
| Посещение занятий | Отмечается присутствие студента на занятиях. За каждое посещение прибавляется 0,4 балла. Максимальное количество баллов за семестр равно 51,2 | Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %. |
| Бонус-рейтинг: Участие в научной конференции | Студент представляет копии документов, подтверждающие победу или участие в научных конференциях по тематике дисциплины При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %. | Зачтено: +15 % за победу в научной конференции международного уровня +10 % за победу в научной конференции российского уровня +5 % за победу в научной конференции университетского уровня +1 % за участие в научной конференции. Не зачтено: - |

## 7.3. Типовые контрольные задания

| Вид контроля | Типовые контрольные задания |
|---|---|
| Защита отчета о выполнении задания | |
| Посещение занятий | . |
| Бонус-рейтинг: Участие в научной конференции | |

## 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:*

Не предусмотрены

*г) методические указания для студентов по освоению дисциплины:*

1. Баринов А.Е. Методические указания по практикуму по научно-исследовательской деятельности(в локальной сети кафедры)
2. Астахова Л.В._Практикум_Методическое пособие

*из них: учебно-методическое обеспечение самостоятельной работы студента:*

1. Баринов А.Е. Методические указания по практикуму по научно-исследовательской деятельности(в локальной сети кафедры)
2. Астахова Л.В._Практикум_Методическое пособие

**Электронная учебно-методическая документация**

| № | Вид литературы | Наименование ресурса в электронной форме | Библиографическое описание |
|---|---|---|---|
| 1 | Основная литература | Электронно-библиотечная система издательства Лань | Тумбинская, М.В. Защита информации на предприятии : учебное пособие / М.В. Тумбинская, М.В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. https://e.lanbook.com/book/130184 |
| 2 | Основная литература | Электронно-библиотечная система издательства Лань | Петренко, В.И. Защита персональных данных в информационных системах. Практикум : учебное пособие / В.И. Петренко, И.В. Мандрица. — Санкт-Петербург : Лань, 2019. — 108 с. — ISBN 978-5-8114-3311-7. https://e.lanbook.com/book/111916 |
| 3 | Основная литература | Электронно-библиотечная система издательства Лань | Персональные данные в государственных информационных ресурсах / М.Ю. Брауде-Золотарёв, Е.С. Сербина, В.С. Негородов, И.Г. Волошкин. — Москва : Дело РАНХиГС, 2016. — 56 с. — ISBN 978-5-7749-1121-9. https://e.lanbook.com/book/74913 |
| 4 | Дополнительная литература | Электронно-библиотечная система издательства Лань | Сабанов, А.Г. Защита персональных данных в организациях здравоохранения : учебное пособие / А.Г. Сабанов, В.Д. Зыков, Р.В. Мещеряков. — Москва : Горячая линия-Телеком, 2012. — 206 с. — ISBN 978-5-9912-0243-5. https://e.lanbook.com/book/5194 |
| 5 | Дополнительная литература | Электронно-библиотечная система издательства Лань | Каширская, Е. Н. Защита информации в информационно - управляющих системах : учебное пособие / Е. Н. Каширская, М. А. Макаров. — Москва : РТУ МИРЭА, 2020. — 67 с. https://e.lanbook.com/book/167621 |

## 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. -База данных polpred (обзор СМИ)(бессрочно)
2. -Стандартинформ(бессрочно)
3. -База данных ВИНИТИ РАН(бессрочно)
4. -Информационные ресурсы ФИПС(бессрочно)

## 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 (3б) | Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows 10, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2 |