

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)
Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

**ПРОИЗВОДСТВЕННАЯ ПРАКТИКА:
ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА**

**НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**Профиль подготовки
«Организация и технология защиты информации»**

**УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ
БАКАЛАВРИАТ**

**Форма обучения
очно-заочная**

Программа практики составлена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 Информационная безопасность и учебного плана направления подготовки 10.03.01 Информационная безопасность, профиль «Организация и технологии защиты информации».

Программу составила Троеглазова Анна Владимировна, PhD, доцент *кафедры информационной безопасности*.

Рецензент программы: Титов Дмитрий Николаевич, к.т.н., доцент *кафедры информационной безопасности*.

Программа практики обсуждена и одобрена на заседании *кафедры информационной безопасности*

Зам. зав. кафедрой ИБ

A.V. Троеглазова

Программа одобрена ученым советом *Института оптики и технологий информационной безопасности*

Председатель ученого совета ИОиТИБ

A.V. Шабурова

«СОГЛАСОВАНО»

Зав. библиотекой СГУГиТ

A.V. Шнак

ОГЛАВЛЕНИЕ

1	ВИД ПРАКТИКИ, СПОСОБ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ	4
2	ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	4
3	МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	7
4	ОБЪЕМ ПРАКТИКИ	7
5	СОДЕРЖАНИЕ ПРАКТИКИ	7
5.1	Содержание этапов практики, том числе реализуемой в форме практической подготовки.....	6
5.2	Самостоятельная работа обучающегося.....	7
6	ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ	8
7	ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ.....	9
7.1	Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы	9
7.2	Уровни сформированности компетенций, шкала и критерии оценивания результатов прохождения практики	10
7.3	Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.....	11
7.4	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.....	12
8	ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ.....	13
8.1	Основная литература.....	13
8.2	Дополнительная литература	14
8.3	Нормативная документация	15
8.4	Периодические издания	15
8.5	Электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы.....	15
9	ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ.....	16

1 ВИД ПРАКТИКИ, СПОСОБ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ

Вид: производственная практика.

Тип: эксплуатационная практика.

Способы проведения практики: стационарная, выездная.

Форма проведения производственной практики: реализация компонентов образовательной программы в форме практической подготовки осуществляется путем чередования с реализацией иных компонентов образовательной программы в соответствии с календарным учебным графиком и учебным планом

2 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Целями производственной практики являются: формирование профессиональных компетенций для решения научных и практических задач в сфере, осуществления профессиональной деятельности в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, профиль подготовки «Организации и технология защиты информации», и сбор материалов для выпускной квалификационной работы; в области воспитания: нравственное, патриотическое, общекультурное, профессионально-трудовое, гражданско-правовое, профессионально-трудовое, нравственно-эстетическое, эколого-оздоровительное.

Задачами прохождения производственной практики являются:

–приобрести первичные навыки практической работы с вычислительной техникой, существующими в организации программными средствами обработки и защиты информации;

–приобрести навыки эксплуатации программных, технических средств защиты информации,

– приобрести первоначальные практические навыки выполнения работ по обслуживанию технических средств защиты информации.

В результате прохождения практики обучающийся должен обладать следующими компетенциями

профессиональные компетенции

<i>Код компетенции</i>	<i>Содержание формируемой компетенции</i>	<i>Образовательные результаты</i>
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Выпускник знает: - принципы построения, функционирования, основные характеристики, элементную базу аппаратных средств вычислительной техники; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации; Выпускник умеет: - использовать программные и аппаратные средства персонального компьютера; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и

		<p>аппаратных средств защиты;</p> <ul style="list-style-type: none"> - осуществлять удаленный доступ к базам данных; - проводить анализ показателей качества сетей и систем связи. <p>Выпускник владеет:</p> <ul style="list-style-type: none"> - профессиональной терминологией; - навыками настройки и обслуживания программно-аппаратных средств защиты информации; - навыками настройки локальных вычислительных сетей.
ПК-2	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	<p>Выпускник знает:</p> <ul style="list-style-type: none"> - профессиональную терминологию; - основные принципы построения защищенных систем обработки и хранения информации. <p>Выпускник умеет:</p> <ul style="list-style-type: none"> - применять на практике программные средства системного и прикладного назначения; - проводить оценочные расчёты основных параметров телекоммуникационных систем; - выполнять первоначальную настройку параметров работы программных средств системы; - настраивать системы обнаружения вторжений в соответствии с требованиями системы. <p>Выпускник владеет:</p> <ul style="list-style-type: none"> - навыками практического использования программных СЗИ.
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	<p>Выпускник знает:</p> <ul style="list-style-type: none"> - принципы организации информационных систем в соответствии с требованиями по защите информации. <p>Выпускник умеет:</p> <ul style="list-style-type: none"> - разрабатывать и оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов. <p>Выпускник владеет:</p> <ul style="list-style-type: none"> - методами анализа степени угроз объекту защиты; - навыками поиска информации о параметрах и характеристиках программных СЗИ; - навыками разработки и оформления рабочей технической документации.
ПК-4	Способностью участвовать в работах по реализации политики информационной	<p>Выпускник знает:</p> <ul style="list-style-type: none"> - принципы формирования политики информационной безопасности в информационных системах.

	безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	<p>Выпускник умеет:</p> <ul style="list-style-type: none"> - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем. <p>Выпускник владеет:</p> <ul style="list-style-type: none"> - первичными навыками находить организационно-управленческие решения в нестандартных ситуациях; - навыками в эксплуатации подсистем управления информационной безопасностью предприятия; - первичными навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	<p>Выпускник знает:</p> <ul style="list-style-type: none"> - организацию работы и нормативные правовые акты по аттестации объектов информатизации; - типовые методики испытаний объектов информатизации по требованиям защиты информации; - типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации; - специальные защитные знаки и их классификацию. <p>Выпускник умеет:</p> <ul style="list-style-type: none"> - анализировать и оценивать угрозы информационной безопасности объекта; - проводить аудит информационной безопасности предприятий, организаций вне зависимости от их формы собственности и сферы деятельности. <p>Выпускник владеет:</p> <ul style="list-style-type: none"> - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - навыками использования нормативной базы РФ, международных, зарубежных стандартов, лучших практик по обеспечению информационной безопасности предприятий, организаций; - навыками организации мероприятий по защите информации на объекте информатизации.
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок	<p>Выпускник знает:</p> <ul style="list-style-type: none"> - методы и средства контроля эффективности программных и программно-аппаратных средств защиты информации;

	<p>работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p>	<p>- методы и средства контроля эффективности технических средств защиты информации.</p> <p>Выпускник умеет:</p> <p>- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем.</p> <p>Выпускник владеет:</p> <p>- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем;</p> <p>- навыками участия в экспертизе состояния защищенности информации на объекте защиты.</p>
--	---------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3 МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная практика: эксплуатационная практика входит в Блок 2 «Практики» и относится к вариативной образовательной организацией части основной образовательной программы (далее ООП) высшего образования – программ бакалавриата федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, профиль «Организация и технология защиты информации».

Матрица поэтапного формирования компетенций, отражающая междисциплинарные связи, приведена в общей характеристике ООП по направлению подготовки.

4 ОБЪЕМ ПРАКТИКИ

Общая трудоемкость производственной практики - согласно образовательной программе практики составляет 108 часов/3 з.е., в том числе в форме практической подготовки – 108 часов. Продолжительность практики – 2 недели

5 СОДЕРЖАНИЕ ПРАКТИКИ

5.1 Содержание этапов практики, в том числе реализуемой в форме практической подготовки

<i>№ п/п</i>	<i>Наименование раздела (этапа) практики</i>	<i>Трудоемкость работы (часы)</i>	<i>Наименование оценочного средства</i>
1	Получение индивидуального задания по прохождению производственной практики.	2	Собеседование
2	Прибытие на предприятие, прохождение инструктажа обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка	4	Собеседование
3	Составление совместного рабочего графика (плана) проведения практики	12	Собеседование
4	Ознакомиться с тематикой работы базы прохождения практики	12	Собеседование

5	Сбор материала по тематике задания. Выполнение практического задания.	18	Собеседование
6	Анализ полученных результатов.	20	Собеседование
7	Защита отчета, включая оформление отчёта по практике	40	Собеседование
Всего		108	

5.2 Самостоятельная работа обучающегося

<i>№ n/n</i>	<i>Содержание СРО</i>	<i>Порядок реализации</i>	<i>Трудоемкость (часы)</i>	<i>Формы контроля</i>
1	Получение индивидуального задания по прохождению производственной практики	Обучающийся получает индивидуальное задание на практику, изучает его	2	Собеседование
2	Прибытие на предприятие, прохождение инструктажа обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка	Обучающийся проходит инструктаж по технике безопасности, изучает все необходимые инструкции	4	Собеседование
3	Составление совместного рабочего графика (плана) проведения практики	Обучающийся разрабатывает рабочий график практики на основании индивидуального задания на практику и в соответствии с планом выполнения выпускной квалификационной работы	12	Собеседование
4	Проработка теоретического материала по теме: «Информационные системы и средства их защиты»	Обучающийся прорабатывает теоретические вопросы, осуществляет информационный поиск по теме.	54	Собеседование
5	Описание выполняемой практической работы с использованием средства защиты информации	Обучающийся самостоятельно изучает вопросы подготовки к практической работе, изучает технические требования и характеристики по применению СЗИ.	54	Собеседование
Всего			108	

6 ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

По завершению практики должен быть сформирован следующий пакет документов.

1 При прохождении практики на базе СГУГиТ:

- заявление о направлении на практику;
- индивидуальное задание на практику;
- отчет, где излагаются вопросы, рассмотренные в соответствии с индивидуальным заданием;
- рабочий график;
- дневник по практике;
- контрольный лист инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка;
- аттестационный лист от руководителя практики.

2 При прохождении практики в Профильной организации:

- заявление о направлении на практику;
- индивидуальное задание на практику;
- отчет, где излагаются вопросы, рассмотренные в соответствии с индивидуальным заданием;
- рабочий график;
- дневник по практике;
- контрольный лист инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка;
- аттестационный лист от руководителя практики;
- характеристика от Профильной организации
- приказ о назначении руководителя практики от Профильной организации;
- документ, подтверждающий прохождение инструктажа по технике безопасности (копия журнала страницы с вашей фамилией).
- договор о практической подготовке обучающихся, направление на практику, перечень помещений (экземпляр СГУГиТ).

7 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

<i>Код компетенции</i>	<i>Содержание компетенции</i>	<i>Этап формирования</i>	<i>Предшествующий этап (с указанием дисциплин)</i>
ПК-1	Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	4 этап из 4	3- Программно-аппаратные средства защиты информации
ПК-2	Способностью применять программные средства	6 этап из 6	5 - Технологии и системы искусственного

	системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач		интеллекта
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты	3 этап из 3	2 – Технические средства охраны и видеонаблюдения
ПК-4	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	2 этап из 2	1 - Безопасность автоматизированных систем; Основы управления информационной безопасностью
ПК-5	Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	3 этап из 3	2 - Техническая защита информации
ПК-6	Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	3 этап из 3	2 - Программно-аппаратные средства защиты информации

Матрица формирования компетенций, наглядно иллюстрирующая последовательность этапов процесса формирования компетенций, содержится в общей характеристике ООП.

7.2 Уровни сформированности компетенций, шкала и критерии оценивания результатов прохождения практики.

<i>Уровни сформированности компетенций</i>	<i>Пороговый</i>	<i>Базовый</i>	<i>Повышенный</i>
<i>Шкала оценивания</i>	Оценка «удовлетворительно» / «зачтено»	Оценка «хорошо» / «зачтено»	Оценка «отлично»/«зачтено»
<i>Критерии оценивания</i>	Компетенция сформирована. Демонстрируется	Компетенция сформирована. Демонстрируется	Компетенция сформирована. Демонстрируется

	недостаточный уровень самостоятельности практического навыка	достаточный уровень самостоятельности устойчивого практического навыка	высокий уровень самостоятельности, высокая адаптивность научных знаний и практического навыка
--	-----------------------------------------------------------------------	---------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------

В качестве основного критерия оценивания освоения производственной практики обучающимся используется наличие сформированных компетенций.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Паспорт оценочных материалов (фонда оценочных средств) по практике

<i>№ п/п</i>	<i>Наименование оценочного средства</i>	<i>Виды контроля</i>	<i>Код контролируемой компетенции</i>
1.	Вопросы для защиты отчета по практике	Промежуточная аттестация	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6

ВОПРОСЫ ДЛЯ ЗАЩИТЫ ОТЧЕТА ПО ПРАКТИКЕ

1. Виды и объемы работ, выполненные за время прохождения практики.
2. Требования, инструкции и нормативные документы, использованные при выполнении работ.
3. Обоснованность целесообразность разработки темы.
4. Определение целей и задач производственной практики.
5. Анализ, систематизация и обобщение данных по теме производственной практики.
6. Используемое оборудование, аппаратура за время прохождения практики.

Шкала и критерии оценивания

<i>Шкала оценивания</i>	<i>Критерии оценки (содержательная характеристика)</i>
1 (неудовлетворительно) Повторное выполнение работы	Работа выполнена полностью. Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.
2 (неудовлетворительно) Повторная подготовка к защите	Работа выполнена полностью. Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы.
3 (удовлетворительно)	Работа выполнена полностью. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы.

4 (хорошо)	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы.
5 (отлично)	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, представляет полные и развернутые ответы на дополнительные вопросы.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Текущий контроль представляет собой проверку уровня формирования компетенций, регулярно осуществляемую в процессе и после завершения каждого этапа практики.

К основным формам текущего контроля относятся материалы по этапам практики и собеседование по результатам прохождения практики.

Промежуточная аттестация осуществляется по завершению всех этапов практики. Промежуточная аттестация помогает оценить уровень формирования. Компетенций Форма промежуточной аттестации – зачет с оценкой.

Текущий контроль и промежуточная аттестация служат основным средством обеспечения в учебном процессе «обратной связи» между руководителем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики проведения практики.

Во время процедуры оценивания обучающиеся могут пользоваться РПП, а также, с разрешения преподавателя, справочной и нормативной литературой.

Инвалиды и обучающиеся с ограниченными возможностями здоровья могут допускаться на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Привязка оценочных материалов к контролируемым компетенциям и этапам производственной практики приведена в таблице.

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы в рамках практики

<i>№ п/п</i>	<i>Наименование этапа практики</i>	<i>Код контролируемой компетенции (или ее части)</i>	<i>Формы контроля</i>	<i>Наименование оценочных материалов</i>
1.	Получение индивидуального задания по прохождению производственной практики.	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике
2.	Прибытие на предприятие, прохождение инструктаж обучающихся по	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике

	ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка			
3.	Составление совместного рабочего графика (плана) проведения практики	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике
4.	Ознакомиться с тематикой работы базы прохождения практики	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике
5.	Сбор материала по тематике задания. Выполнение практического задания.	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике
6.	Анализ полученных результатов.	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике
7.	Защита отчета, включая оформление отчёта по практике	ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6	Собеседование	Вопросы для защиты отчета по практике

8 ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

8.1 Основная литература

<i>№ п/п</i>	<i>Библиографическое описание</i>	<i>Количество экземпляров в библиотеке СГУГиТ</i>
1.	Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279 (дата обращения: 05.04.2023). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2.	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 05.04.2023). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3.	Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А.С. Масалков. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 226 с. — Режим доступа: https://e.lanbook.com/book/105842 . — Загл. с экрана.	Электронный ресурс

8.2 Дополнительная литература

<i>№ n/n</i>	<i>Библиографическое описание</i>	<i>Количество экземпляров в библиотеке СГУГиТ</i>
1.	Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: http://e.lanbook.com/book/5170 . — Загл. с экрана.	Электронный ресурс
2.	Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 442 с. — Режим доступа: http://e.lanbook.com/book/5155 . — Загл. с экрана.	Электронный ресурс
3.	Зайцев, А.П. Технические средства и методы защиты информации. [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: http://e.lanbook.com/book/5154 . — Загл. с экрана.	Электронный ресурс
4.	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] — Электрон. дан. — М.: ДМК Пресс, 2012. — 592 с. — Режим доступа: http://e.lanbook.com/book/3032 . — Загл. с экрана.	Электронный ресурс
5.	Экономическая эффективность системы защиты информации [Текст]: учебно - метод. пособие / Ю. А. Голиков, Л. Ю. Сульгина; СГГА. - Новосибирск: СГГА, 2012 – 40 с.	30
6.	Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для вузов, допущено УМО / В.П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С. А. Клейменов. - 5-е изд., стереотип. - М.: Академия, 2011. – 330 с.	30
7.	Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С.Н. Никифоров. — Электрон. дан. — Санкт-Петербург: Лань, 2018. — 96 с. — Режим доступа: https://e.lanbook.com/book/107306 . — Загл. с экрана.	Электронный ресурс
8.	Гребешков, А.Ю. Вычислительная техника, сети и телекоммуникации. Учебное пособие для вузов. [Электронный ресурс] — Электрон. дан. — М.: Горячая линия-Телеком, 2015. — 190 с. — Режим доступа: http://e.lanbook.com/book/90140 . — Загл. с экрана.	Электронный ресурс
9.	Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — М.: ФОРУМ : ИНФРА-М, 2017. — 240 с. — Режим доступа: http://znanium.com/bookread2.php?book=914480 . — Загл. с экрана.	Электронный ресурс
10.	Информатика, автоматизированные информационные технологии и системы: Учебник [Электронный ресурс] / В.А. Гвоздева. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 544 с. – Режим доступа: http://znanium.com/catalog.php?bookinfo=207105 – Загл. с экрана	Электронный ресурс
11.	Петренко, С.А. Аудит безопасности Intranet. [Электронный ресурс] / С.А. Петренко, А.А. Петренко. — Электрон. дан. — М. : ДМК Пресс, 2010. — 386 с. — Режим доступа: http://e.lanbook.com/book/1113 — Загл. с экрана.	Электронный ресурс

8.3 Нормативная документация

- 1 Федеральный закон от 27 июля 2006 г. N 149-ФЗ.
- 2 Федеральный закон от 27 июля 2006 г. N 152-ФЗ.
- 3 Закон Российской Федерации от 21 июля 1993 г. N 5485-1.
- 4 Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- 5 Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера».
- 6 Указ Президента Российской Федерации от 30 ноября 1995 г. N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».
- 7 Постановление Правительства Российской Федерации от 04.09.95 № 870 “Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности”.
- 8 Приказ ФСТЭК России от 15 февраля 2017 г. N 27.
- 9 Приказ ФСТЭК России от 14 марта 2014 г. N 31.
- 10 Приказ ФСТЭК России от 18 февраля 2013 г. N 21.
- 11 Приказ ФСТЭК России от 11 февраля 2013 г. N 17.
- 12 Приказ ФСТЭК России от 31 августа 2010 г. N 489.
- 13 Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. Меры защиты информации в государственных информационных системах.
- 14 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год.
- 15 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2021 год.
- 16 Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. N 187 Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.
- 17 Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- 18 Государственная итоговая аттестация выпускников СГУГиТ. Структура и правила оформления [Электронный ресурс]: СТО СМК СГУГиТ 8-06-2021. - Новосибирск : СГУГиТ, 2021. - 69 с. – Режим доступа: <http://lib.sgugit.ru> – Загл. с экрана.

8.4 Периодические издания

1. Журнал «Защита информации. Инсайд»;
2. Журнал «Information Security»;
3. Журнал «Информация и безопасность»;
4. Журнал «Информационная безопасность регионов».

8.5 Электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Каждому обучающемуся в течение всего периода прохождения практики из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», обеспечен индивидуальный неограниченный доступ к следующим электронно-библиотечным системам (электронным библиотекам), современным

профессиональным базам данных и информационным справочным системам, к электронной информационно-образовательной среде СГУГиТ, включая:

1. Сетевые локальные ресурсы (авторизованный доступ для работы с полнотекстовыми документами, свободный доступ в остальных случаях). – Режим доступа: <http://lib.sgugit.ru>.

2. Сетевые удалённые ресурсы:

– электронно-библиотечная система издательства «Лань». – Режим доступа: <http://e.lanbook.com> (получение логина и пароля с компьютеров СГУГиТ, дальнейший авторизованный доступ с любого компьютера, подключенного к интернету);

– электронно-библиотечная система Znanium. – Режим доступа: <http://znanium.com> (доступ по логину и паролю с любого компьютера, подключенного к интернету);

– научная электронная библиотека eLibrary. – Режим доступа: <http://www.elibrary.ru> (доступ с любого компьютера, подключенного к интернету).

– компьютерная справочная правовая система «Консультант-Плюс». – Режим доступа: <http://www.consultant.ru/> (доступ с любого компьютера, подключенного к интернету);

– электронная информационно-образовательная среда СГУГиТ.

9 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

СГУГиТ располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской деятельности обучающихся, предусмотренных учебным планом.

СГУГиТ имеет специальные помещения для проведения занятий лекционного типа, занятий семинарского типа (практических и лабораторных занятий), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, объединенной в локальную сеть, с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду СГУГиТ.

Для успешного освоения практики обучающимися, необходимо наличие следующего оборудования и лицензионного или свободно распространяемого программного обеспечения:

1) компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду;

2) программное обеспечение: Electronics Workbench; OpenOffice; T-FLEX CAD Учебная версия; Sheriff 7m для полиграфа Риф; Adobe Acrobat Reader DC; MATLAB; AnyLogic PLE; КристоАРМ ГОСТ (Академическая); СКЗИ "КристоПро CSP" версии 5.0; СКЗИ "КристоПро CSP" версии 5.0 на сервере; СКЗИ "КристоПро NGate" версии 1.0; ПАК "Удостоверяющий центр "КристоПро УЦ" версии 2.0 класс KC2; Docsvision (для учебных целей); КОМПАС-3D Учебная версия; Wireshark; Cisco Packet Tracer.

3) технические средства обучения, служащие для представления учебной информации большой аудитории мультимедийное оборудование; компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду;

4) лабораторное оборудование:

- учебно-методический программно-аппаратный комплекс криптографической защиты ViPNetCoordinator HW1000 4.x - тип 1; программно-аппаратный комплекс криптографической защиты ViPNetCoordinator HW100 С 4.x - тип 2; программное обеспечение комплекса криптографической защиты и межсетевого экранирования ViPNetCoordinatorforWindows 4.x (KC2) – тип 1; программное обеспечение программного комплекса криптографической защиты и межсетевого экранирования ViPNetCoordinatorforLinux 4.x (KC2) – тип 2; программное обеспечение программного комплекса криптографической защиты и межсетевого экранирования ViPNetClientforWindows 4.x (KC2) – тип 3.

- комплект оборудования ЭЛЕМЕНТЫ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ: компьютерный комплекс видеонаблюдения на основе платы AceCor 16200; бескорпусная цветная видеокамера ACV-452CNA; бескорпусная черно-белая видеокамера ACV-322L; черно-белая купольная видеокамера ACV-922; видеокамера СВ-28038; объектив с автодиофрагмой и регулируемым фокусным расстоянием SCV2810G; термокожух K17/3-220-220.

- комплект оборудования ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ И ОСОБЕННОСТЕЙ ПРИМЕНЕНИЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА РАДИОМОНИТОРИНГА: радиосканер AR8200; Анализатор электромагнитного спектра Атаком АКС-1201; измеритель мощности СВЧ; генератор радишума RNR-02; приемная измерительная биконическая активная антенна диапазон 30 МГц - 1,5 ГГц.

- ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ: анализатор Protek-3201; генератор сигналов; переходник-согласователь генератора с линией 220 В; поисковый приемник анализатор проводных коммуникаций RRL-02; генератор шума по сети 220 В RNC-02; фильтр сетевой помехоподавляющий RFT-02; осциллограф;

- ПОЛИГРАФ «РИФ» в составе: сенсорный блок (евро); фотоплетизмограмма (частота пульса); КГР – фазическая и тоническая составляющие; дыхание верхнее (грудное); дыхание нижнее (брюшное); регистрация изменения давления (АД) (модерн) регистрация противодействия тестированию (тремор-подушка); регистрация речевого сигнала; психологическая составляющая обследуемого лица (ПС).

- комплект оборудования ТЕОРИЯ И ПРАКТИКА ПРИМЕНЕНИЯ НЕЛИНЕЙНОГО ЛОКАТОРА: нелинейный локатор «Катран»; зарядное устройство; набор пронумерованных имитаторов; измерительная установка; экранированный бокс.

- комплект оборудования ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ (ПЭМИ): анализатор спектра PROTEK 3201; штатная антенна к анализатору; антенна приемо-передающая магнитного и электрического поля комбинированная диапазон 9 кГц - 30 МГц, приемная измерительная биконическая активная антенна диапазон 30 МГц - 1,5 ГГц П-6-221, широкополосный генератор радишума RNR-02; широкополосный генератор радишума SP-21; полосовой генератор радишума RNR-02.2; персональный компьютер.

- комплект оборудования ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРОАКУСТИЧЕСКИМ КАНАЛАМ: направленные микрофоны VOYA BY-PVM1000, устройство формирования тестового акустического сигнала (УФТС); генератор гармонических сигналов (или «белого» шума) с усилителем мощности; акустический излучатель 20 Вт; генератор акустического и виброакустического шума с тремя независимыми каналами формирования шума и встроенными 5-октавными эквалайзерами; виброизлучатели в комплекте с элементами крепления; тестовое устройство - проводной стетоскоп с усилителем; измеритель шума и вибраций в комплекте с измерительным микрофоном и акселерометром (ВШВ-003М); модуль АЦП (Е14-40); цифровой диктофон RR-850; измерительный микрофон СМ-100).