

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Сибирский государственный университет геосистем и технологий»

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

ПРОИЗВОДСТВЕННАЯ:  
ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА

НАПРАВЛЕНИЕ ПОДГОТОВКИ  
10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Профиль подготовки  
«Организация и технологии защиты информации  
(по отрасли или в сфере профессиональной деятельности)»

УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ  
БАКАЛАВРИАТ

Форма обучения  
очная

Новосибирск – 2024

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 (по отрасли или в сфере профессиональной деятельности)».

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



*А.В. Троеглазова*

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

Председатель ученого совета ИОиТИБ



*А.В. Шабурова*

«СОГЛАСОВАНО»

Зав. библиотекой СГУГиТ



*А.В. 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 ...	7
5.2	Самостоятельная работа обучающихся .....	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 освоения практики.....	9
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 .....	10
7.4	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.....	11
8	ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ.....	12
8.1	Основная литература .....	12
8.2	Дополнительная литература.....	13
8.3	Нормативная документация .....	14
8.4	Периодические издания.....	14
8.5	Электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы .....	14
9	ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ .....	15

## 1 ВИД ПРАКТИКИ, СПОСОБ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ

Вид практики - производственная практика.

Тип практики - технологическая 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

Целью производственной практики: технологической практики является закрепление на практике знаний, умений и навыков, полученных в процессе теоретического обучения, навыков применения систем защиты информации, проектирования систем защиты информации; формирование у обучающихся 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 «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

В результате проведения производственной практики должны быть решены следующие основные задачи:

- освоение обучающимися методик обеспечения организационных и инженерно-технических мер защиты информационных систем;
- формирование навыков разработки предложений по совершенствованию и повышению эффективности защиты объектов информатизации;
- совершенствование навыков применения контрольно-измерительной аппаратуры, применяемой для проверки и аттестации объектов информатизации;
- формирование навыков технического обслуживания средств защиты информации;
- ознакомление с процедурой проведения контрольных проверок работоспособности и эффективности действующих систем и технических средств защиты информации, составление и оформление актов контрольных проверок;
- подготовка и оформление отчета о выполнении индивидуального задания по учебной практике.

В результате освоения практики обучающийся должен обладать следующими профессиональными компетенциями:

Код компетенции	Содержание формируемой компетенции	Код и наименование индикатора достижения	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенции	
			Уровни сформированности компетенций	Образовательные результаты
ПК-3	Способен выявлять уязвимости в системах защиты	ПК-3.1 Осуществляет сбор и анализ исходных данных, необ-	ПОРОГОВЫЙ («удовлетворительно»)	Выпускник знает: – характеристики систем защиты информации автоматизированных систем. Выпускник умеет:

	информации автоматизированных систем, разрабатывать методики, предложения и процедуры совершенствования процесса защиты информации в автоматизированных системах	<p>ходимых для проектирования систем защиты информации автоматизированных систем.</p> <p>ПК-3.2</p> <p>Осуществляет поиск уязвимостей в параметрах автоматизированных систем.</p> <p>ПК-3.3</p> <p>Оформляет рабочую техническую документацию, в том числе программы и методики процесса защиты информации автоматизированных систем.</p>		<p>– анализировать действующие системы защиты информации в автоматизированных системах.</p> <p><i>Выпускник владеет:</i></p> <p>– навыками сбора и анализа исходных данных.</p>
			<p><b>БАЗОВЫЙ</b> («хорошо»)</p>	<p><i>Выпускник знает:</i></p> <p>– характеристики систем защиты информации автоматизированных систем;</p> <p>– виды возможных уязвимостей в существующих системах защиты информации.</p> <p><i>Выпускник умеет:</i></p> <p>– анализировать действующие системы защиты информации в автоматизированных системах;</p> <p>– выявлять уязвимости в действующих системах защиты информации.</p> <p><i>Выпускник владеет:</i></p> <p>– навыками сбора и анализа исходных данных;</p> <p>– навыками проектирования систем защиты информации.</p>
			<p><b>ПОВЫШЕННЫЙ</b> («отлично»)</p>	<p><i>Выпускник знает:</i></p> <p>– характеристики систем защиты информации автоматизированных систем;</p> <p>– виды возможных уязвимостей в существующих системах защиты информации;</p> <p>– порядок проектирования систем защиты информации автоматизированных систем.</p> <p><i>Выпускник умеет:</i></p> <p>– анализировать действующие системы защиты информации в автоматизированных системах;</p> <p>– выявлять уязвимости в действующих системах защиты информации.</p> <p><i>Выпускник владеет:</i></p> <p>– навыками сбора и анализа исходных данных;</p> <p>– навыками проектирования систем защиты информации;</p> <p>– навыками разработки рабочей технической документации на проектируемые средства защиты информации.</p>

ПК-4	Способен оптимизировать параметры программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	<p>ПК-4.1 Осуществляет оптимизацию параметров автоматизированных систем для повышения степени защиты информации.</p> <p>ПК-4.2 Принимает участие в подготовке технико-экономического обоснования разработанных проектных решений</p>	<p><b>ПОРОГОВЫЙ</b> («удовлетворительно»)</p>	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>– характеристики систем защиты информации автоматизированных систем.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>– анализировать действующие системы защиты информации в автоматизированных системах.</li> </ul> <p><i>Выпускник владеет:</i></p> <ul style="list-style-type: none"> <li>– навыками сбора и анализа исходных данных.</li> </ul>
			<p><b>БАЗОВЫЙ</b> («хорошо»)</p>	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>– характеристики систем защиты информации автоматизированных систем;</li> <li>– виды возможных уязвимостей в существующих системах защиты информации.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>– анализировать действующие системы защиты информации в автоматизированных системах;</li> <li>– выявлять уязвимости в действующих системах защиты информации.</li> </ul> <p><i>Выпускник владеет:</i></p> <ul style="list-style-type: none"> <li>– навыками сбора и анализа исходных данных;</li> <li>– навыками проектирования систем защиты информации.</li> </ul>
			<p><b>ПОВЫШЕННЫЙ</b> («отлично»)</p>	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>– характеристики систем защиты информации автоматизированных систем;</li> <li>– виды возможных уязвимостей в существующих системах защиты информации;</li> <li>– порядок проектирования систем защиты информации автоматизированных систем.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>– анализировать действующие системы защиты информации в автоматизированных системах;</li> <li>– выявлять уязвимости в действующих системах защиты информации.</li> </ul> <p><i>Выпускник владеет:</i></p> <ul style="list-style-type: none"> <li>– навыками сбора и анализа исходных данных;</li> <li>– навыками проектирования систем</li> </ul>

				защиты информации; – навыками разработки рабочей технической документации на проектируемые средства защиты информации.
--	--	--	--	---

### 3 МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Производственная практика: технологическая практика входит в Блок 2 «Практики» и относится к части, формируемой участником образовательного процесса 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 технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

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, том числе реализуемой в форме практической подготовки

№ п/п	Наименование раздела (этапа) практики	Трудоемкость работы (часы) в т.ч. в форме практической подготов- ки		Формы контроля
		Контактная работа	СРО	
1	Организационно-методический этап	-	4/4	Собеседование (устно)
2	Выполнение практических работ	-	94/94	Собеседование (устно)
3	Заключительный этап	-	8/8	Собеседование (устно)
Всего		-	108/108	

#### 5.2 Самостоятельная работа обучающихся

№	Содержание СРО	Порядок реализации	Трудоем- кость (часы)	Формы кон- троля
1	Организационно-методический этап	Обучающийся присутствует на инструктаже по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего	4/4	Собеседование (устно)

		трудового распорядка (вводный инструктаж). Обучающийся оформляет индивидуальное задание и документы для похождения практической подготовки, визирует у руководителя практики и заведующего кафедрой.		
	Выполнение практических работ	Обучающийся прорабатывает теоретические вопросы, осуществляет информационный поиск по теме. Обучающийся самостоятельно выполняет практическую работу с применением системы защиты информации от утечки согласно индивидуальному заданию	94/94	Собеседование (устно)
	Заключительный этап	Обучающийся готовит отчет по практике в соответствии с требованиями стандарта СТО СМК СГУГиТ 8-06-2021	8/8	Собеседование (устно)
	<i>Всего</i>		<i>108/108</i>	

## 6 ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

По завершению практики должен быть сформирован следующий пакет документов.

1 При прохождении практики на базе СГУГиТ:

- отчет, где излагаются вопросы, рассмотренные в соответствии с индивидуальным заданием;

- заявление о направлении на практику;

- индивидуальное задание на практику;

- рабочий график (план) проведения практики;

- контрольный лист инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка;

- оценочный лист от руководителя практики;

2 При прохождении практики в профильной организации:

- отчет, где излагаются вопросы, рассмотренные в соответствии с индивидуальным заданием;

- заявление о направлении на практику;

- индивидуальное задание на практику;

- совместный рабочий график (план) проведения практики;

- характеристика от руководителя профильной организации;

- оценочный лист от руководителя практики от СГУГиТ;

- договор о практической подготовке обучающихся, направление на практику

- приказ о прохождении производственной практики от профильной организации;

- выписка из журнала вводного инструктажа.

Для аттестации обучающийся должен полностью выполнить все разделы индивидуального задания на учебную практику, оформить отчет по учебной практике.

В отчёте должны быть представлены:

1. Индивидуальное задание на практику в форме практической подготовки.

2. Рабочий график (план) проведения практики в форме практической подготовки.

3. Титульный лист.

4. Оглавление

5. Введение.



6. Основная часть отчета.

Основная часть отчета пишется по результатам выполнения индивидуального задания на практику.

7. Заключение.

8. Список используемой литературы.

9. Приложения (обязательные и справочные). При наличии.

Отчет должен быть оформлен согласно СТО СМК СГУГиТ 8-06-2021. По окончании учебной практики организуется защита отчета, где учитывается: оценка качества выполнения и индивидуальные оценки по каждому этапу учебной практики в форме практической подготовки. По результатам защиты отчета по учебной практике в форме практической подготовки руководитель выставляет зачет с оценкой. Зачет с оценкой по учебной практике в форме практической подготовки приравнивается к оценкам (зачетам) по теоретическому обучению и учитывается при подведении итогов общей успеваемости обучающихся. Обучающийся, не выполнивший программу учебной практики в форме практической подготовки или не предоставивший её результаты в установленные сроки, считается не аттестованным.

## 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-3	Способен выявлять уязвимости в системах защиты информации автоматизированных систем, разрабатывать методики, предложения и процедуры совершенствования процесса защиты информации в автоматизированных системах	3 этап из 4	2 – аудит информационных систем
ПК-4	Способен оптимизировать параметры программных, программно-аппаратных и технических средств защиты информации автоматизированных систем	2 этап из 3	1 – встраиваемые системы и их программирование, технологии мультимедиа в виртуальной реальности

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

### 7.2 Уровни сформированности компетенций, шкала и критерии оценивания освоения практики

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

	стрируется недоста- точный уровень само- стоятельности прак- тического навыка	стрируется доста- точный уровень са- мостоятельности устойчивого практи- ческого навыка	стрируется высокий уровень самостоя- тельности, высокая адаптивность научных знаний и практиче- ского навыка
--	--	---	---

В качестве основного критерия оценивания освоения производственной практики обуча-  
ющимися 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 компе-  
тенций 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-3, ПК-4

ВОПРОСЫ ДЛЯ ЗАЩИТЫ ОТЧЕТА ПО ПРАКТИКЕ

1. Исследование причин возникновения, форм проявления, возможности параметриза-  
ции и оценки опасности физических явлений, увеличивающих вероятность нежелательного  
воздействия на информационные процессы в защищаемом объекте.

2. Изучение возможных источников и каналов утечки информации, составление методик  
расчетов и программ экспериментальных исследований по технической защите информации,  
выполнение рас четов в соответствии с разработанными методиками и программами.

3. Исследования с целью нахождения и выбора наиболее целесообразных практических  
решений в пределах поставленной задачи обеспечения инженерно-технической защиты инфор-  
мации, в том числе с обеспечением требований соблюдения государственной тайны.

4. Подбор, изучение и обобщение научно-технической литературы, нормативных и ме-  
тодических материалов по инженерно-технической защите объектов информатизации.

5. Проектирование и внедрение комплексных систем и отдельных специальных техни-  
ческих и программно-математических средств защиты информации на объектах информатиза-  
ции, в том числе сравнительного анализа типовых криптосхем.

6. Сбор и анализ материалов учреждений, организаций и предприятий отрасли с целью  
выработки и принятия решений и мер по обеспечению защиты информации и эффективному  
использованию средств автоматического контроля, обнаружения возможных каналов утечки  
сведений, представляющих государственную, военную, служебную и коммерческую тайну.

7. Анализ существующих методов и средств, применяемых для контроля и защиты ин-  
формации и разработка предложений по их совершенствованию и повышению эффективности  
этой защиты.

8. Обследование объектов защиты, их аттестации и категорирования, разработка и под-  
готовка к утверждению проектов нормативных и методических материалов, регламентирующих  
работу по защите информации, а также положений, инструкций и других организационно-  
распорядительных документов.

9. Организация и своевременное представление предложений для включения в соответ-  
ствующие разделы перспективных и текущих планов работ и программ мер по контролю и за-  
щите информации.

**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>№ n/n</i>	<i>Наименование этапа практики</i>	<i>Код контролируемой компетенции (или ее части)</i>	<i>Формы контроля</i>	<i>Наименование оценочных материалов</i>
1.	Организационно-методический этап	ПК-3, ПК-4	Собеседование (устно)	Вопросы для защиты отчета по практике
2.	Выполнение практических работ	ПК-3, ПК-4	Собеседование (устно)	Вопросы для защиты отчета по практике
3.	Заключительный этап	ПК-3, ПК-4	Собеседование (устно)	Вопросы для защиты отчета по практике

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

### 8.1 Основная литература

<i>№ n/n</i>	<i>Библиографическое описание</i>	<i>Количество экземпляров в библиотеке СГУТ</i>
1.	Советов, Б. Я. Информационные технологии: теоретические основы : учебное пособие / Б. Я. Советов, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2017. — 444 с. — ISBN 978-5-8114-1912-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/93007">https://e.lanbook.com/book/93007</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2.	Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/114688">https://e.lanbook.com/book/114688</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3.	Гребешков, А. Ю. Вычислительная техника, сети и телекоммуникации : учебное пособие / А. Ю. Гребешков. — Москва : Горячая линия-Телеком, 2017. — 190 с. — ISBN 978-5-9912-0492-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111047">https://e.lanbook.com/book/111047</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
4.	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 // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/105842">https://e.lanbook.com/book/105842</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

5.	Операционные системы. Основы UNIX : учебное пособие / А.Б. Вавренюк, О.К. Курышева, С.В. Кутепов, В.В. Макаров. — Москва : ИНФРА-М, 2021. — 160 с. + Доп. материалы [Электронный ресурс]. — (Среднее профессиональное образование). - ISBN 978-5-16-013981-4. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1189336">https://znanium.com/catalog/product/1189336</a> (дата обращения: 05.04.2021). — Режим доступа: по подписке.	Электронный ресурс
----	---	--------------------

## 8.2 Дополнительная литература

<i>№ n/n</i>	<i>Библиографическое описание</i>	<i>Количество экземпляров в библиотеке СГУГиТ</i>
1.	Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/50578">https://e.lanbook.com/book/50578</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2.	Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111075">https://e.lanbook.com/book/111075</a> (дата обращения: 05.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3.	Мельников, В. П. Информационная безопасность и защита информации : 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, [6] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - ISBN 978-5-7695-7738-3 (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	30
4.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов, Э. Р. Газизова ; под редакцией А. А. Шелупанова [и др.]. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2012. — 550 с. — ISBN 978-5-9912-0257-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/5114">https://e.lanbook.com/book/5114</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
5.	Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем : монография / А. В. Благодаров, В. С. Зияутдинов, П. А. Корнев, В. Н. Малыш. — Москва : Горячая линия-Телеком, 2015. — 116 с. — ISBN 978-5-9912-0307-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111019">https://e.lanbook.com/book/111019</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
6.	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. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/5194">https://e.lanbook.com/book/5194</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

	02.04.2021). — Режим доступа: для авториз. пользователей.	
7.	Международные и российские нормативные акты и стандарты по информационной безопасности: основы стандартизации и сертификации : учебно - метод. пособие / И. В. Минин, О. В. Минин ; СГГА. - Новосибирск : СГГА, 2013. - 34, [1] с. - ISBN 978-5-87693-589-2: (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей	Электронный ресурс
8.	Петренко, С. А. Аудит безопасности Intranet : учебное пособие / С. А. Петренко, А. А. Петренко. — Москва : ДМК Пресс, 2010. — 386 с. — ISBN 5-94074-183-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/1113">https://e.lanbook.com/book/1113</a> (дата обращения: 02.04.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

### 8.3 Нормативная документация

1. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне".
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция).
4. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне".
5. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
6. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
7. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
8. Положение от 27 октября 1995 г. N 199 О сертификации средств защиты информации по требованиям безопасности информации.
9. 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 помещения, представляющие собой учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде 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 AceCop 16200; бескорпусная цветная видеокамера ACV-452СНА; бескорпусная черно-белая видеокамера ACV-322L; черно-белая купольная видеокамера ACV-922; видеокамера СВ-28038; объектив с автодиофрагмой и регулируемым фо-

кусным 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 ради шума 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 ради шума RNR-02; широкополосный генератор ради шума SP-21; полосовой генератор ради шума RNR-02.2; персональный компьютер.

- комплект оборудования ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ И ВИБРОАКУСТИЧЕСКИМ КАНАЛАМ: направленные микрофоны BOYA 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).