

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра информационной безопасности

## ПРОГРАММА ПРАКТИКИ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА:  
ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И  
ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

НАПРАВЛЕНИЕ ПОДГОТОВКИ  
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Профиль подготовки  
Организация и управление информационной безопасностью

УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ  
МАГИСТРАТУРА

Форма обучения  
очно-заочная

Новосибирск - 2021

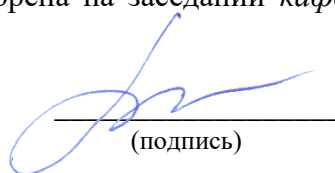
Программа практики составлена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.04.01 Информационная безопасность и учебного плана направления подготовки 10.04.01 Информационная безопасность, профиль «Организация и управление информационной безопасностью».

Программу составили *Троеглазова Анна Владимировна, доцент кафедры информационной безопасности, PhD*

Рецензент программы *Новиков Сергей Николаевич, профессор кафедры информационной безопасности, доктор технических наук, доцент*

Рабочая программа обсуждена и одобрена на заседании *кафедры информационной безопасности (ИБ)*

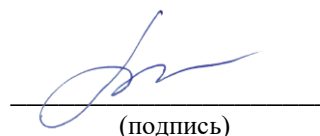
Зав. кафедрой ИБ

  
(подпись)

*А.В. Шабурова*

Программа одобрена ученым советом *института оптики и технологий информационной безопасности (ИОиТИБ)*

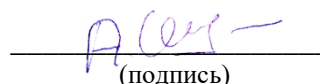
Председатель ученого совета ИОиТИБ

  
(подпись)

*А.В. Шабурова*

«СОГЛАСОВАНО»

Зав. научно-технической библиотекой

  
(подпись)

*А.В. Шпак*

## ОГЛАВЛЕНИЕ

1. ВИД И СПОСОБЫ ПРОВЕДЕНИЯ ПРАКТИКИ, РЕАЛИЗУЮЩЕЙ ПРАКТИЧЕСКУЮ ПОДГОТОВКУ.....	4
2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ РЕАЛИЗАЦИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ .....	4
3. МЕСТО ПРАКТИКИ ФОРМЕ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ .....	6
4. ОБЪЕМ ПРАКТИКИ .....	6
5. СОДЕРЖАНИЕ ПРАКТИКИ.....	6
5.1. Содержание этапов практики, реализующих практическую подготовку .....	6
5.2. Самостоятельная работа обучающегося по практике .....	6
6. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ .....	7
7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ .....	7
7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.....	7
7.2. Уровни сформированности компетенций, шкала и критерии оценивания освоения практики.....	8
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 .....	9
7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций .....	10
8. ПЕРЕЧЕНЬ УЧЕБНОЙ литературы и ресурсов сети «Интернет», необходимых для РЕАЛИЗАЦИИ ПРАКТИКИ .....	11
8.1. Основная литература .....	11
8.2. Дополнительная литература.....	11
8.3. Нормативная документация .....	13
8.4. Электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы .....	14
9. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ .....	14

## 1. ВИД И СПОСОБЫ ПРОВЕДЕНИЯ ПРАКТИКИ, РЕАЛИЗУЮЩЕЙ ПРАКТИЧЕСКУЮ ПОДГОТОВКУ

Вид практики – производственная.

Тип практики – практика по получению профессиональных умений и опыта профессиональной деятельности.

Способы проведения практики – стационарная, выездная.

Форма проведения производственной практики: практика по получению профессиональных умений и опыта профессиональной деятельности - реализация компонентов образовательной программы осуществляется путем чередования с реализацией иных компонентов образовательной программы в соответствии с календарным учебным графиком и учебным планом.

## 2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ РЕАЛИЗАЦИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Целью практики является закрепление теоретической подготовки и приобретение навыков и компетенций в сфере профессиональной деятельности, а также формирование у обучающихся профессиональных компетенций для решения научных и практических задач в области информационной безопасности и осуществления профессиональной деятельности по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры), направленность (профиль) – «Организация и управление информационной безопасностью».

Практика закладывает основы для дальнейшего осуществления научно-исследовательской работы в соответствии с профилем профессиональной деятельности.

В результате выполнения практики должны быть решены следующие задачи:

- формирование у обучающихся профессиональных компетенций, направленных на решение научных и практических задач в области информационной безопасности;
- формулирование цели, задач, плана научного исследования в области информационной безопасности на основе проведения библиографической работы, анализа состояния научно-технической проблемы, технического задания и поставка цели и задач проектирования систем информационного типа на основе подбора и изучения литературных и патентных источников;
- выбор общенаучных и специальных методов исследования для выполнения магистерской диссертации;
- построение математических моделей объектов исследования, выбор численных методов их моделирование, разработка новых или выбор готовых алгоритмов решения задачи;
- разработка структурных, функциональных и алгоритмических схем систем информационного типа с определением их физических принципов действия, структур и установлением технических требований на отдельные блоки, элементы и программные модули;
- разработка программного обеспечения систем информационного типа с использованием средств компьютерного моделирования;
- выявление новизны полученных результатов для охраны интеллектуальной собственности;
- выбор оптимального метода и разработка программы экспериментальных исследований, проведение требуемых физических измерений с выбором технических средств и обработкой результатов;
- подготовка и оформление рефератов, докладов и научных статей для участия в научных семинарах и конференциях; представление результатов выполненных исследований на научных семинарах или конференциях;
- подготовка промежуточного и заключительного отчетов о выполнении обучающимся индивидуального задания по практике.

В результате прохождения практики обучающийся должен обладать следующими профессиональными компетенциями:

<i>Код компетенции</i>	<i>Содержание формируемой компетенции</i>	<i>Образовательные результаты</i>
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>- основные направления развития информационных технологий, принципы и методы формирования политики безопасности объектов защиты с учетом специфики этих объектов.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>- прогнозировать эффективность функционирования информационных технологий, оценивать затраты и риски в сфере информационной безопасности с учетом специфики этих объектов.</li> </ul> <p><i>Выпускник владеет:</i></p> <ul style="list-style-type: none"> <li>- навыками и опытом оценки затрат и рисков при использовании информационных технологий, формирования политики безопасности объектов защиты с учетом специфики этих объектов.</li> </ul>
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>- системы, комплексы, средства и технологии обеспечения информационной безопасности.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>- разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.</li> </ul> <p><i>Выпускник владеет:</i></p> <ul style="list-style-type: none"> <li>- навыками и опытом разработки систем, комплексов, средств и технологий обеспечения информационной безопасности системы защиты информации техническими средствами.</li> </ul>
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>- состав, характеристики и функциональные возможности систем и средств обеспечения информационной безопасности;</li> <li>- российские и международные стандарты в сфере информационной безопасности.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>- проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.</li> </ul> <p><i>Выпускник владеет:</i></p> <ul style="list-style-type: none"> <li>- навыком и опытом обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.</li> </ul>
ПК-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопас-	<p><i>Выпускник знает:</i></p> <ul style="list-style-type: none"> <li>- методы и способы разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики.</li> </ul> <p><i>Выпускник умеет:</i></p> <ul style="list-style-type: none"> <li>- разрабатывать программы и методики испытаний</li> </ul>

	ности	средств и систем обеспечения информационной безопасности с учетом их специфики. <i>Выпускник владеет:</i> - навыком и опытом разработки программ и методик испытаний средств и систем обеспечения информационной безопасности с учетом их специфики.
--	-------	--

### 3. МЕСТО ПРАКТИКИ ФОРМЕ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Практическая подготовка организуется при проведении практики, которая входит в Блок 2 «Практики, в том числе НИР» и относится к вариативной части основной образовательной программы (далее – ООП) высшего образования – программ магистратуры федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и управление информационной безопасностью».

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

### 4. ОБЪЕМ ПРАКТИКИ

Общая трудоемкость практики составляет 432 часа / 12 з.е., в том числе в форме практической подготовки – 432 часа. Продолжительность практики – 8 недель.

### 5. СОДЕРЖАНИЕ ПРАКТИКИ

#### 5.1. Содержание этапов практики, реализующих практическую подготовку

<i>№ n/n</i>	<i>Наименование этапа практики</i>	<i>Трудоемкость (часы)</i>	<i>Формы контроля</i>
1	Организационно-методический этап	24/24	Собеседование
2	Экспериментальные исследования (или практические разработки)	400/400	Собеседование
3	Заключительный этап	8/8	Собеседование
	<i>Всего</i>	<i>432/432</i>	

#### 5.2. Самостоятельная работа обучающегося по практике

<i>№ n/n</i>	<i>Содержание СРО</i>	<i>Порядок реализации</i>	<i>Трудоемкость (часы)</i>	<i>Формы контроля</i>
1	Организационно-методический этап	Информационный поиск по теме задания. Составление плана работ. Обучающийся присутствует на инструктаже по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка (вводный инструктаж). Обучающийся оформляет индивидуальное задание и документы для похождения	24/ 24	Собеседование

		практики, визирует у руководителя практики и заведующего кафедрой		
2	Экспериментальные исследования (или практические разработки)	Обучающийся проводит экспериментальные исследования или практические разработки, составление и отладку программного обеспечения. По результатам экспериментальных исследований или практических разработок обучающийся готовит раздел магистерской диссертации и раздел отчета по практике. Обучающийся формулирует актуальность, новизну и практическую значимость объекта исследования	400/ 400	Собеседование
3	Заключительный этап	Обучающийся оформляет отчет по практике, готовится к защите отчета по практике и получению зачета	8/8	Собеседование
	<i>Всего</i>		432/ 432	

## 6. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Для аттестации обучающийся должен полностью выполнить все разделы индивидуального задания на практику и оформить отчет по практике. В отчете должны быть представлены:

- индивидуальное задание на практику;
- рабочий график (план) проведения практики;
- оглавление;
- введение;
- основная часть отчета. Основная часть отчета оформляется по результатам выполнения индивидуального задания на практику;
- заключение;
- список используемой литературы;
- приложения (обязательные и справочные). При наличии.

Отчет должен быть оформлен согласно СТО СГУГиТ 8-06-2021.

По окончании практики организуется защита отчета, где учитывается: оценка качества выполнения и индивидуальные оценки по каждому этапу практики. По результатам защиты отчета по практике руководитель выставляет зачет с оценкой.

Зачет с оценкой по практике приравнивается к оценкам (зачетам) по теоретическому обучению и учитывается при подведении итогов общей успеваемости обучающегося.

Обучающийся, не выполнивший программу практики или не предоставивший ее 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

Код компетенции	Содержание компетенции	Этап формирования	Предшествующий этап (с указанием дисциплин)
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, про-	4 этап из 5	3 – теория систем и системный анализ в информационной безопасности

	гнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты		
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	4 этап из 5	3 – контроль защищенности информации от несанкционированного доступа, контроль защищенности информации от утечки по техническим каналам
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	3 этап из 4	2 – технологии обеспечения информационной безопасности
ПК-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	4 этап из 5	3 – аттестация объектов информатизации по требованиям безопасности информации

Матрица формирования компетенций, наглядно иллюстрирующая этапность процесса формирования компетенций, содержится в Общей характеристике ООП.

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

<i>Уровни сформированности компетенций</i>	Пороговый	Базовый	Повышенный
<i>Шкала оценивания</i>	Оценка «удовлетворительно» / «зачтено»	Оценка «хорошо» / «зачтено»	Оценка «отлично» / «зачтено»
<i>Критерии оценивания</i>	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка	Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность научных знаний и практического навыка

В качестве основного критерия оценивания освоения дисциплины обучающимся используется наличие сформированных компетенций (компетенции).



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 в форме практической подготовке

<i>№ п/п</i>	<i>Наименование оценочных материалов</i>	<i>Виды контроля</i>	<i>Код контролируемой компетенции (или ее части)</i>
1	Вопросы для защиты отчета по практике в форме практической подготовке	Промежуточная аттестация	ПК-1, ПК-2, ПК-3, ПК-4

### ВОПРОСЫ ДЛЯ ЗАЩИТЫ ОТЧЕТА ПО ПРАКТИКЕ

#### 1. Организационно-методический этап:

- Виды и объемы работ, выполняемые за время прохождения практики?
- Какие основные работы должны быть запланированы магистранту на практику?
- Какие вопросы магистерской диссертации следует рассмотреть в рамках практики?
- Кто проводит вводный инструктаж в СГУГиТ?
- Как проводится литературный обзор и патентный поиск?
- Как оценить достоверность полученной информации?
- Как оценить стоимость полученной информации?
- Какие разделы должны быть в общем плане работ по теме практики?
- Как проводится детализация и уточнение плана работ?
- Какие вопросы плана работ согласовываются с руководителем практики?
- Зачем уточняются формулировки плана работ?
- Кто утверждает план работ по практике?

#### 2. Экспериментальные исследования (или практические разработки):

- В чем заключается выбор оптимального метода и разработка программ экспериментальных исследований?
- В чем заключается новизна и актуальность исследования, решаемые задачи и методы их решения?
- Что лежит в основе обоснования выбора экспериментальных установок, требуемых физических измерений, выбора технических средств и оценки достоверности полученных результатов?
- Как проводилась проработка выбранных решений по системотехническому проектированию систем информационной безопасности с использованием современных программных средств компьютерного моделирования?

#### 3. Заключительный этап:

- Какие компетенции были освоены за время прохождения практики?
- Каковы результаты прохождения практики?

#### Шкала и критерии оценивания

<i>Балл</i>	<i>Критерии оценки (содержательная характеристика)</i>
2 (неудовлетворительно) Повторная подготовка к защите	Работа выполнена полностью. Магистрант 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. Магистрант 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. Магистрант владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки, отвечая на дополнительные вопросы
5 (отлично)	Работа выполнена полностью. Магистрант 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 получения первичных умений и навыков профессиональной деятельности, 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 получение первичных профессиональных умений и навыков, в том числе первичных умений и навыков профессиональной деятельности и формирование 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 программой практики, 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 практики приведена в таблице.

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

<i>№ п/п</i>	<i>Наименование этапа практики в форме практической подготовки</i>	<i>Код контролируемой компетенции (или ее части)</i>	<i>Формы контроля</i>	<i>Наименование оценочных материалов</i>
1	Организационно-методический этап	ПК-1, ПК-2, ПК-3, ПК-4	Собеседование	Вопросы для защиты отчета по практике
2	Экспериментальные исследования (или практические разработки)	ПК-1, ПК-2, ПК-3, ПК-4	Собеседование	Вопросы для защиты отчета по практике
3	Заключительный этап	ПК-1, ПК-2, ПК-3, ПК-4	Собеседование	Вопросы для защиты отчета по практике

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

### 8.1. Основная литература

<i>№ n/n</i>	<i>Библиографическое описание</i>	<i>Количество экземпляров в библиотеке СГУГуТ</i>
1	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учебное пособие / Т. В. Гвоздева, Б. А. Баллод. — Санкт-Петербург : Лань, 2019. — 252 с. — ISBN 978-5-8114-3517-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/115515">https://e.lanbook.com/book/115515</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2	Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111057">https://e.lanbook.com/book/111057</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
3	Новиков, С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С. Н. Новиков. — Москва : Горячая линия-Телеком, 2018. — 128 с. — ISBN 978-5-9912-0410-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/119836">https://e.lanbook.com/book/119836</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
4	Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 124 с. — ISBN 978-5-8114-4041-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/114698">https://e.lanbook.com/book/114698</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

### 8.2. Дополнительная литература

<i>№ n/n</i>	<i>Библиографическое описание</i>	<i>Количество экземпляров в библиотеке СГУГуТ</i>
1	Малюк, А. А. Защита информации в информационном обществе : учебное пособие / А. А. Малюк. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111078">https://e.lanbook.com/book/111078</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
2	Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Лань, 2018. — 96 с. — ISBN 978-5-8114-3099-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/110935">https://e.lanbook.com/book/110935</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс

3	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: 10.07.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
4	Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие / В. К. Новиков. — Москва : Горячая линия-Телеком, 2017. — 176 с. — ISBN 978-5-9912-0525-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111084">https://e.lanbook.com/book/111084</a> (дата обращения: 10.06.2021). — Режим доступа: для авториз. пользователей.	Электронный ресурс
5	Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Инв. № 891. ДСП	1
6	Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждено ФСТЭК России 25.12.2006. ДСП	1
7	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
8	Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
9	Основные мероприятия по организации и обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
10	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено ФСТЭК России 15.02.2008. ДСП	1
11	Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. ДСП	1
12	Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119. ДСП	1
13	Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса. Утверждены приказом ФСТЭК России от 28 февраля 2017 г. № 31. ДСП	1
14	Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87. ДСП	1
15	Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9. ДСП	1
16	Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19 августа 2016 г. № 119. ДСП	1
17	Требования по безопасности информации, устанавливающие уровни до-	1

	верия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76. ДСП	
18	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К). Утвержден приказом ФСТЭК России от 15 марта 2012 г. № 27. ДСП	1
19	Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России. Москва: 2002 – 74 с. ДСП	1
20	Методика выявления уязвимостей и недеklarированных возможностей в программном обеспечении. Утверждена ФСТЭК России 11 февраля 2019 г. ДСП	1
21	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. ДСП	1

### 8.3. Нормативная документация

1) ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

2) ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

3) ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

4) ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

5) ГОСТ Р ИСО/МЭК 27003-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации.

6) ГОСТ Р ИСО/МЭК 27004-2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание.

7) ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007).

8) Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры).

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.

Полнотекстовая база данных учебных и методических пособий СГУГиТ для обеспечения практики доступна по ссылке: <http://lib.sgugit.ru>.

#### 8.4. Электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Каждому обучающемуся в течение всего периода обучения 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.com. – 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);
  - – электронная информационно-справочная система «Техэксперт». – Режим доступа: <http://bnd2.kodeks.ru/kodeks01/> (доступ по логину и паролю с любого компьютера, подключенного к интернету).
3. Электронная справочно-правовая система (база данных) «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>
4. Национальная электронная библиотека (НЭБ). – Режим доступа: <http://www.rusneb.ru> (доступ с любого компьютера, подключенного к интернету).

#### 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.

Для реализации программы магистратуры в СГУГиТ имеется специально оборудованное помещение для проведения учебных занятий - лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

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 обеспечени-

ем 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; 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-452CNA; бескорпусная черно-белая видеокамера ACV-322L; черно-белая купольная видеокамера ACV-922; видеокамера СВ-28038; объектив с автодиафрагмой 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 – физическая 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 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).