Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

Начальник УРОПСП
В.А. Мельникова

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 01ff058c007bae2c8149e7712c28ce8469
Владелец: Мельникова Виктория Александровна
Действителен: с 18.04.2022 по 18.04.2023

Рабочая программа практики

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА – ПРЕДДИПЛОМНАЯ ПРАКТИКА

основной профессиональной образовательной программы высшего образования
программы специалитета по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	Институт цифровых технологий
ВЫПУСКАЮЩАЯ КАФЕДРА	Кафедра информационной безопасности
РАЗРАБОТЧИК	УРОПСП

1 ТИП И ФОРМА ПРОВЕДЕНИЯ, БАЗЫ И ЦЕЛЬ ПРОХОЖДЕНИЯ ПРАКТИКИ

Вид и тип практики:

производственная практика – эксплуатационная практика;

производственная практика – научно-исследовательская работа;

производственная практика – преддипломная практика.

Форма проведения практики: дискретно.

Базы практики: профильные организации, учреждения и предприятия, связанные по роду своей производственной, научно-проектной, научно-исследовательской деятельностью с проблематикой в области защиты информации, а также-подразделения университета.

Цель производственных практик – закрепление и углубление теоретической подготовки обучающихся, формирование компетенций и их индикаторов, приобретение практических навыков, профессиональных умений и опыта самостоятельной профессиональной деятельности, включающей в себя освоение практических навыков по специализации: «Безопасность открытых информационных систем».

2 РЕЗУЛЬТАТЫ ПРОХОЖДЕНИЯ ПРАКТИКИ

Прохождение производственных практик направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по специализации подготовки: «Безопасность открытых информационных систем».

Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения ОПОП, представлен в таблице 1.

Таблица 1 – Планируемые результаты обучения по практикам, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Наименование практики	Результаты обучения, соотнесенные с компетенциями/индикаторами достижения компетенции
УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни; ПКС-2: Разработка проектных решений по защите информации в автоматизированных системах; ПКС-4: Проведение анализа структурных и функциональных схем, защищённых автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; ПКС-5: Способен к разработке моделей автоматизированных систем и под-	УК-6.7: Составляет план распределения личного времени для выполнения задач на дипломное проектирование; ПКС-2.5: Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации открытых информационных систем; ПКС-4.3: Применяет меры по защите информации от основных угроз информации в автоматизированных системах и способы выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; ПКС-5.4: Формирует перечень мероприятий по разработке систем защиты информации автоматизированных систем;	Преддипломная практика	*Знать:* - технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; - источники и классификацию угроз информационной безопасности; - программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. *Уметь:* - формировать перечень мероприятий по разработке систем защиты информации автоматизированных систем; - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем. *Владеть:* - навыками выборки меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; - способностью к составлению плана распределения личного времени для выполнения задач на дипломное проектирование;

Код и наименование компетенции	Индикаторы достижения компетенции	Наименование практики	Результаты обучения, соотнесенные с компетенциями/индикаторами достижения компетенции
систем безопасности автоматизированных систем; ПКС-6: Способен к анализу защищённости информационной инфраструктуры автоматизированной системы.	ПКС-6.9: Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем.		- способностью определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации открытых информационных систем. Должен приобрести опыт: - в выборке мер защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; - определения структуры системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации открытых информационных систем.

При прохождении практики обеспечивается развитие у студентов-практикантов навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

3 МЕСТО ПРАКТИК В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ОБЪЕМ (ТРУДОЕМКОСТЬ) И ПРОДОЛЖИТЕЛЬНОСТЬ ПРАКТИК, ФОРМЫ АТТЕСТАЦИИ ПО НИМ

Производственная практика – преддипломная практика входит в состав обязательной части основной профессиональной образовательной программы специалитета и проводится после теоретического обучения и экзаменационной сессии в одиннадцатом семестре, при очной форме обучения.

Трудоемкость производственной практики – преддипломной практики составляет 12 зачетных единиц (ЗЕТ), 432 академических часа (324 астр. часа) контактной работы, продолжительность практики – 8 недель.

Форма аттестации по практике - дифференцированный зачет (зачёт с оценкой).

4 СОДЕРЖАНИЕ ПРАКТИКИ

Содержание практики формируется на основе планируемых результатов обучения, соотнесённых с планируемыми результатами освоения ОПОП, и представлено в таблице 2.

Таблица 2 – Содержание и примерный рабочий график (план) производственной практики – преддипломной практики

Разделы (этапы) практики и их содержание	**Продолжительность раздела (этапа)**
	акад.ч.
1. Организационные вопросы оформления в организации, инструктаж по охране труда и технике безопасности. Изучение инструкции по охране труда. Изучение инструкции по технике безопасности и пожаробезопасности, схем аварийных проходов и выходов, пожарного инвентаря. Изучение правил внутреннего распорядка. Изучение правил и норм охраны труда, техники безопасности при работе с вычислительной техникой.	**20**
2. Ознакомление со структурой и характером деятельности организации. Определение статуса, структуры и системы управления функциональных подразделений и служб организации. Изучение положения об их деятельности и правовой статус. Ознакомление с перечнем и строением сети. Ознакомление перечня и назначения оборудования. Изучение должностных инструкций технических работников среднего звена в соответствии с подразделением организации.	**40**
3. Сбор материалов по теме ВКР. Изучение исходной информации по заданной теме ВКР. Исследование предметной области дипломной работы. Определение общей цели ВКР. Определение соста-	**100**

Разделы (этапы) практики и их содержание	Продолжительность раздела (этапа)
	акад.ч.
ва ВКР и функциональных задач. Разработка и обоснование требований к ВКР. Определение этапов ВКР и сроков их выполнения.	
4. Анализ технических и программных средств защиты информации организации. Изучение принятой в организации системы защиты информации, комплекса проводимых организационно-профилактических мероприятий по предупреждению несанкционированной утечки конфиденциальной информации.	**80**
5. Постановка задачи по разработке/совершенствованию методов, средств и/или систем информационной безопасности. Обоснование целесообразности проектирования (внедрения, модернизации и т.п.) системы информационной безопасности организации.	**62**
6. Обработка и анализ полученной информации. Сбор, систематизация и обработка собранного материала.	**70**
7. Подготовка отчета по практике Оформление и представление (каждого индивидуально) рабочих материалов и результатов практической работы в форме отчетов о практике, а также отзывы с оценками работы со стороны руководителей от предприятий (организаций).	**60**
Итого по практике	**432**

5 ФОРМЫ И ТРЕБОВАНИЯ К ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Форма отчетности по преддипломной практике - отчет по практике.

Прохождение практики является учебной работой студентов. Учебная работа состоит из двух основных частей: теоретической и практической.

Первая часть заключается в изучении теоретического материала по результатам проведенных наблюдений. Вопросы, порядок их изучения и выполнения практической работы выдаются на установочном занятии к учебной практике и указаны в разрабатываемых методических указаниях по прохождению практики.

Во второй части практики производится изучение установленных программой практики вопросов (выполнению индивидуального задания, задания на научно-исследовательскую работу). Выполнение практики на предприятии осуществляется в сроки, указанные в учебном плане. По результатам практики составляется отчет и производится его защита.

Аттестация по итогам практики осуществляется на основании оформленного в соответствии с установленными требованиями письменного отчета с отзывом руководителя практики от организации, заверенным печатью. Сдача отчета по практике производится в сроки, установленные учебным планом. Отчет по практике составляется в соответствии с требованиями программы и с учетом индивидуального задания.

По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно). Оценка по итогам практики заносится в зачетную книжку.

После окончания практики отчет по практике предоставляется на кафедру. В отчет входят индивидуальные задания (при наличии), выполненные в период прохождения учебных практик.

Отчет должен быть подписан руководителем практики. Отчет принимается руководителем практики от кафедры. Защита отчета проводится студентами по окончании практики.

Форма отчетности по производственной – преддипломной практике - отчет по практике, допускается предоставление завершенной и оформленной выпускной квалификационной работы взамен отчета по практике.

6 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ ПО ПРАКТИКЕ

Результаты работы, выполненной в процессе прохождения производственной практики, представляются в виде отчета. Содержание отчета определяется, прежде всего, индивидуальным заданием на производственную практику.

В первой части отчета кратко излагаются общие сведения о предприятии, учреждении, организации, на котором проходила производственная практика. Приводится структурная схема предприятия (или его подразделения), дается описание организации управления его деятельностью. Описывается состав и основные характеристики средств вычислительной техники, используемые в подразделении. Приводится обзор технических средств защиты информации и организационных мер обеспечения информационной безопасности. Отражаются результаты самостоятельной работы, использованные литературные материалы, содержание лекций, экскурсий, консультаций.

Во второй части отчета приводится анализ собранной информации, необходимой для выполнения практической работы, оговоренной третьим разделом индивидуального задания. Анализируются информационные потоки, возможные угрозы, способы защиты от них.

В третьей части отчета излагается методика решения конкретной задачи, сформулированной в третьем разделе индивидуального задания, и полученные результаты решения этой задачи.

Отчет оформляется в виде пояснительной записки. На титульном листе отчета указываются все подразделения, в которых студент проходил учебную практику, фамилии и должности руководителей. Каждый руководитель визирует соответствующую часть отчета на титульном листе. Вторым листом в отчет подшивается направление на учебную практику с от-

меткой предприятия о сроках прохождения практики и характеристикой студента-практиканта. Третьим листом идет индивидуальное задание.

В отчете обязательно должен быть список использованных литературных источников со ссылками на них в тексте, приведены расчетные формулы и расчеты по ним, необходимые графики и рисунки. Листинги программ, чертежи, подготовленные доклады оформляются в виде приложений к отчету.

Студенты должны строго соблюдать действующие на предприятии, учреждении, организации правила оформления, хранения и обращения с документацией.

Типовые контрольные вопросы, необходимые для оценки результатов прохождения производственной-преддипломной практики

1. Принципы построения и особенности использования шифрованной файловой системы EFS.
2. Перечислите и охарактеризуйте основные встроенные механизмы защиты ОС.
3. Виды файловых систем. Контроль доступа к файлам.
4. Виртуальные частные сети (VPN): определение, назначение, способы организации.
5. Методы обеспечения защиты системы WWW и электронной почты.
6. Средства обеспечения защиты базовых протоколов и служб Internet семейства TCP/IP и службы поиска.
7. Классификация сетей, сравнительная характеристика различных типов сетей.
8. Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности.
9. Понятие и виды защищаемой информации по законодательству РФ.
10. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
11. Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.
12. Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности.
13. Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации.
14. Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.
15. Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права.

16. Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).

17. Основное содержание разработки Политики безопасности предприятия (организации).

18. Принципы, основные задачи и функции обеспечения информационной безопасности.

19. Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации.

20. Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну.

21. Ответственность за нарушение законодательства в информационной сфере.

22. Основные мероприятия по защите информации при проведении совещаний и переговоров.

23. Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных).

24. Виды компьютерных преступлений. Классификация компьютерных злоумышленников.

25. Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП).

26. Раскрыть основной порядок проведения аттестации и контроля объектов информатизации.

27. Сформулировать основные правила безопасной работы в компьютерной системе.

28. Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД.

29. Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.

30. Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам.

31. Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения.

32. Раскрыть понятие «компьютерный вирус». Привести виды компьютерных вирусов. Раскрыть жизненный цикл вирусов и механизмы сокрытия вредоносных программ.

33. Назначение и основные особенности применения системы защиты конфиденциальной информации «Aura».

34. Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.

35. Рассмотреть особенности разграничения доступа и аудита в СЗИ (на примере СЗИ «Аура»).

36. Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа.

37. Раскрыть особенности организации технического противодействия лазерному подслушиванию.

38. Раскрыть особенности образования электромагнитных каналов утечки информации.

39. Раскрыть особенности образования и съема информации по электрическим каналам утечки информации.

40. Сформулировать основные особенности построения периметровой охраны особо важных объектов.

Аттестация результатов производственной практики. Производственная практика завершается защитой отчета научному руководителю. К защите представляется оформленный и подписанный студентом отчет по производственной практике. Аттестация по итогам производственной практики осуществляется после сдачи документов по практике на кафедру информационной безопасности и фактической защиты представленного студентом отчета с учетом ответов студента на вопросы, заданные научным руководителем, полноты и качества оформления отчета по практике, а также отзыва руководителя практики об уровне знаний и квалификации студента. По результатам аттестации выставляется дифференцированная оценка по 4-хбалльной шкале «отлично – хорошо – удовлетворительно – неудовлетворительно».

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 3).

Таблица 3 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно	Обладает минимальным набором знаний, необходимым для системного взгляда	Обладает набором знаний, достаточным для системного взгляда на изу-	Обладает полнотой знаний и системным взглядом на изучаемый объект

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	связывать между собой (только некоторые из которых может связывать между собой)	на изучаемый объект	чаемый объект	
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3.Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4. Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

7 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Нормативно-правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ) // «Собрание законодательства РФ», 14.04.2014, N 15, ст. 1691.

2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (выписка в части вопросов защиты информации).

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (выписка в части вопросов защиты информации).

4. Гражданский кодекс Российской Федерации. Часть четвертая. Интеллектуальная собственность.

5. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности".

6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»

9. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 5 декабря 2016 г. № 646.

10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

11. Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

12. Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

13. Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных».

14. Руководящий документ. «АС. Защита от НСД к информации. Классификация АС и требования по защите информации», Гостехкомиссия России, 1998.

15. Руководящий документ. «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1998.

16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Гостехкомиссия России, 2001.

17. ГОСТ 29339-92. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Общие технические требования».

18. ГОСТ Р 50739-95. «СВТ. Защита от несанкционированного доступа к информации. Общие технические требования».

19. ГОСТ Р 50752-95. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний».

20. ГОСТ Р 50922-96. «ЗИ. Основные термины и определения».

21. ГОСТ 7.32–2017. Отчет о научно-исследовательской работе. Структура и правила оформления. Введен 2018–07–01. Москва: Стандартинформ, 2017. - 32 с

Основная учебная литература:

1. Ищейнов, В. Я. Защита конфиденциальной информации: учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – М. : ФОРУМ, 2013. – 256 с. (наличие в библиотеке БГАРФ - 15 экз.)

2. Кузнецов, А. В. Основы защиты информации: учеб. пособие / В. А. Иванов, О.П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с. (наличие в библиотеке БГАРФ - 110 экз.)

3. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – М. : Издательский центр «Академия», 2008. – 256 с. (наличие в библиотеке БГАРФ - 15 экз.)

4. Б.И. Герасимов [и др.] Основы научных исследований: учебное пособие – М.: ФОРУМ:М.: ИНФРА-М, 2015 (3 экз.)

5. Баранов, А.П. Основы научных исследований: учебник для курсантов (студентов) вузов, обучающихся по специальности 26.06.07 "Эксплуатация судового электрооборудования и средств автоматики" / А. П. Баранов ; ГУМРФ им. адм. С.О. Макарова. - СПб. : Изд-во ГУМРФ им. адм. С.О. Макарова, 2015. - 104 с. - (Библиотека Совкомфлот). - Библиогр.: с. 103. - ISBN 978-5-9509-0156-0 : 431.00 р., 450.00 р. (15 экз.)

6. И.Б. Рыжков Основы научных исследований и изобретательства: учебное пособие – СПб.: Лань, 2013, - 400 с. (5 экз.)

Дополнительная учебная литература:

1. Астахов А.А. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

2. Электроника и схемотехника : учебное пособие для студентов, обучающихся по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем" / А. И. Кучумов. - 4-е изд., стер. - М.: Гелиос АРВ, 2011. - 336 с. (наличие в библиотеке БГАРФ - 39 экз.)

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ИД «Форум», 2013. – 416 с. (наличие в библиотеке БГАРФ - 20 экз.)

4. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А. Клейменов. – Москва: Академия, 2008. – 336 с. (наличие в библиотеке БГАРФ - 31 экз.)

5. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - М. : ЮНИТИ-ДАНА, 2017. - 287 с.

6. Электроника и схемотехника. Мультимедийный практикум с использованием компьютерного моделирования в программной среде «TINA» [Электронный ресурс] : учебное пособие / В. А. Алехин. - Саратов : Вузовское образование, 2017. - 290 с.

7. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для студентов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев. - СПб. : Питер, 2008. - 272 с. (наличие в библиотеке БГАРФ - 15 экз.)

8. Информатика. Базовый курс: учебное пособие / ред. С. В. Симонович. - 3-е изд. Стандарт третьего поколения. - СПб. : Питер, 2013. - 640 с. (наличие в библиотеке БГАРФ - 21 экз.)

9. В.В. Кукушкина Организация научно-исследовательской работы студентов (магистров) : учебное пособие - М.: ИНФРА-М, 2015 (3 экз.)

8 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНТЕРНЕТ-РЕСУРСЫ

Студент при прохождении практики, в ходе выполнения индивидуального задания, подготовке аналитических материалов по практике и формировании отчета использует лицензионное программное обеспечение: программное обеспечение Microsoft, получаемое по программе "Open Value Subscription";

Электронные образовательные ресурсы

- Российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков - https://stepik.org

- Образовательная платформа - https://openedu.ru/

Состав современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС):

«Консультант Плюс» - www.consultant.ru

«Гарант» - www.garant.ru

Нормативные-правовые акты РФ - http://www.rg.ru

Сайт ФСТЭК России. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации - http://fstec.ru

Электронная интернет библиотека - http://www.iqlib.ru

Полнотекстовая электронная библиотека - http://www.biblioclub.ru

Научная электронная библиотека - http://www.elibrary.ru

Сайты библиотек вузов в каталоге ИС «Единое окно» - http://window.edu.ru

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА ПРАКТИКИ

Перечень соответствующих помещений и их оснащения приведен в таблице 4.

.

Таблица 4 – Материально-техническое обеспечение практики

Наименование практики	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений для самостоятельной работы
Преддипломная практика	г. Калининград, Советский проспект, 1, ГУК, ауд. 353, компьютерный класс - учебная аудитория для прохождения практики, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная (учебная) мебель - учебная доска, стол преподавателя, парты, стулья. 13 компьютеров с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации, мультимедийный проектор; inter doska; комплект лицензионного программного обеспечения.
	г. Калининград, Советский проспект, 1, ГУК, ауд. 352, компьютерный класс - учебная аудитория для прохождения практики, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная (учебная) мебель - учебная доска, стол преподавателя, парты, стулья. 14 компьютеров с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации, комплект лицензионного программного обеспечения.
	г. Калининград, Советский проспект, 1, ГУК, ауд. 261/13 - помещение для хранения и профилактического обслуживания учебного оборудования	Шкафы, стеллажи, оборудование и аппаратура для ремонта и профилактики

10 СВЕДЕНИЯ О ПРОГРАММЕ ПРАКТИКИ И ЕЕ СОГЛАСОВАНИИ

Рабочая программа преддипломной практики представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Безопасность открытых информационных систем»).

Рабочая программа практики рассмотрена и одобрена на заседании кафедры информационной безопасности 20.04.2022 г. (протокол № 7).

Заведующая кафедрой  Н.Я. Великите

Директор института  А.Б. Тристанов