

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное автономное образовательное учреждение
высшего образования «Балтийский федеральный университет имени Иммануила
Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Учебная практика (учебно-лабораторная)»

Шифр: 10.05.01

Специальность: «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Квалификация (степень) выпускника: специалист

Калининград
2022 г.

Лист согласования

Составитель: Киршанова Е.А., PhD., доцент.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета ИФМНиИТ
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент А.А.Шпилевой

СОДЕРЖАНИЕ

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.
3. Место практики в структуре образовательной программы.
4. Содержание практики.
5. Сведения о местах проведения практики
6. Указание форм отчетности по практике.
7. Фонд оценочных средств
8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики
10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для проведения практики.

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения

Вид практики: Учебная

Тип практики: Учебно-лабораторная

Способ проведения практики: стационарная

Форма проведения практики: дискретно, путем выделения в календарном учебном графике непрерывного периода учебного времени для ее проведения.

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Цель практики – ознакомление студентов с распределенными системами управления версиями на примере GIT, системой верстки LaTeX и использование этих систем для создания презентации о выполненном задании одного из списка задач с сайта cryptohack.org в системе компьютерной алгебры Sage.

Код компетенции	Результаты освоения образовательной программы (ИДК)	Перечень планируемых результатов
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.	Знать: основы систем управления версиями GIT, синтаксис GIT команд, синтаксис основных команд верстки LaTeX. Уметь: работать с системой управления версиями на примере GitHub/GitLab, оформлять презентации в пакете Beamer от LaTeX. Владеть: навыками использования систем управления версиями Git, навыками верстки в LaTeX и создания презентаций с помощью пакета Beamer.
ОПК-7 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный	ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня. ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.	Знать: базовый синтаксис языка Python (Sage) для решения криптоаналитической задачи по курсу типа CTF. Уметь: моделировать криптоаналитическую задачу формата CTF на языке Python Владеть: навыками решения задач формата CTF на языке Python.

выбор инструментария программирования и способов организации программ.		
--	--	--

3. Место практики в структуре образовательной программы

Учебная практика (учебно-лабораторная) практика представляет собой практику Обязательной части Блока 2 «Практика» подготовки обучающихся.

4. Содержание практики

Этапы практики, их содержание	Виды деятельности обучающихся	Формы текущего контроля
Подготовительный этап	1.Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 2.Обязательный инструктаж по охране труда, инструктаж по технике безопасности, пожарной безопасности. 3.Инструктаж по установке Git, LaTeX и TexStudio. 4. Выбор задания типа CTF с сайта cryptihack.org	Загруженный на Git аккаунт корректно компилирующийся шаблон презентации в Beamer
Производственный этап	Выполнение выбранного задания с сайта cryptihack.org задания на языке Python/Sage	Проверка работоспособности программы
		Заполнение разделов дневника
Заключительный этап	Оформление презентации.	Оформление отчета
	Представление результатов в виде презентации и демонстрации работы программы.	Представление презентации, демонстрация корректности решения (флага)

Примеры задач, инструкций и указаний к установке необходимого ПО можно найти на страницах курса

https://crypto-kantiana.com/elena.kirshanova/teaching/science_tools_2020/

https://crypto-kantiana.com/elena.kirshanova/teaching/scientific_tools_2021.html

5. Сведения о местах проведения практики

Практика проводится непосредственно в образовательной организации, в том числе в ее структурном подразделении, предназначенном для проведения практической подготовки.

Для обучающихся с ограниченными возможностями здоровья и инвалидов практика планируется и организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

6. Указание форм отчетности по практике

Формой отчетности по практике является:

1. Дневник практики;
2. Отчет по практике с приложениями;
3. Презентация и исходный код программы, выложенные в открытый доступ на одну из доступных систем контроля версий.

Указанные документы представляются руководителю практики.

Дневник практики.

С момента прибытия и до конца пребывания на практике студент обязан вести «Дневник прохождения производственной практики», который является составной частью отчета о практике и используется при его написании. Записи в дневнике должны быть ежедневными. В дневнике фиксируются следующие виды работ:

1. учебная (сбор источников/литературы для решения выбранной криптоаналитической задачи);
2. научная (написание программы для решения задачи).

В дневнике необходимо также отразить встретившиеся в работе затруднения, их характер, какие меры были приняты для их устранения, отметить недостатки в теоретической подготовке. Дневники периодически проверяются руководителем практики, в нем делаются отметки по его ведению, качеству выполняемой студентом работы. В дневнике руководитель практики дает отзыв о прохождении обучающимся практики (выполнении программы практики, отношении к порученной работе, собранных материалов) и выставляет оценку практики.

Отзыв руководителя практики от университета должен отражать основные структурные элементы: степень реализации плана практики; грамотность и полнота изложения материала в отчете; уровень самостоятельности выполнения работы; недостатки и замечания, выявленные как в процессе практики, так и в представленном отчете; положительные стороны, выявленные как в процессе практики, так и в представленном отчете; общий вывод об отчете с заключением о проделанной работе.

Отзыв руководителя практики от профильной организации, на базе которой студент проходил практику, должен отражать: краткую характеристику предоставленной информации, с которой работал обучающийся; методы и технологии, уровень самостоятельности, степень ответственности, добросовестности при выполнении работы; недостатки и замечания, выявленные в процессе прохождения практики; положительные стороны, выявленные в процессе прохождения практики; общий вывод об отчете с заключением о проделанной работе.

Отчет о практике составляется индивидуально каждым студентом в соответствии с методическими рекомендациями по прохождению практики и должен отражать его деятельность в период практики. В отчете следует отразить все вопросы, изученные во время прохождения практики, представить аналитические результаты анализа, выводы и рекомендации. Отчет о практике должен состоять из титульного листа, содержания, введения, основной части, заключения, списка литературы (при необходимости) и приложений (при необходимости). В заключении обобщаются результаты проделанной

работы и делаются выводы и рекомендации. В конце отчета приводится список литературы и нормативных материалов, а также материалы приложений (графики, таблицы и т.д.).

Отчетная документация по практике (с приложениями) предоставляется в институт/школу не позднее 5 дней по окончании практики. Если практика проходит летом или в конце учебного семестра, то не позднее последнего рабочего (учебного) дня практики. За обучающихся заочной формы обучения отчетная документация предоставляется в период экзаменационной сессии (не позднее последнего учебного дня) соответствующего семестра.

7. Фонд оценочных средств

Текущий контроль прохождения практики производится руководителем практики в дискретные временные интервалы с использованием следующих оценочных средств:

- решение криптоаналитической задачи средствами языка Python/Sage. Проверка нахождения корректного флага (решения задачи) с агрегатора задач cryptohack.org

Промежуточная аттестация производится в форме зачета с оценкой с использованием следующих оценочных средств:

- оформление и устное представление презентации, выполненной в LaTeX, о задаче, выбранных методах ее решения, загрузка всех материалов (исходников кода и презентации) в одну из систем контроля версий GIT.

При оценке результатов практики принимается во внимание:

- соответствие отчета заданию на практику;
- степень полноты выполненных задач, достижения цели практики;
- соблюдение графика прохождения практики;
- характеристика на обучающегося, составленная руководителем практики от профильной организации;
- оформление отчета по практике;
- содержательность доклада, аргументированность и полнота ответов на вопросы при защите результатов практики.

Зачёт по практике (в виде защиты отчёта) принимает групповой руководитель в индивидуальном порядке.

Во время защиты обучающийся должен подтвердить уровень образовательных результатов практики в соответствии с требованиями, определенными программой практики.

При оценке итогов практики обучающегося принимается во внимание отзыв руководителя практики от профильной организации

По результатам защиты студенту выставляется зачет с оценкой.

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	<i>Включает нижестоящий уровень. Умение самостоятельно принимать решение, решать проблему/задачу</i>	отлично	86-100

		теоретического и прикладного характера на основе изученных методов, приемов, технологий		
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	<i>Включает нижестоящий уровень.</i> Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо	71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно	55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	Менее 55

8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики

Основная литература:

1. *Авдошин, С.М.* Дискретная математика. Модулярная алгебра, криптография, кодирование / С.М. Авдошин, А.А. Набебин. - Москва : ДМК Пресс, 2017. - 352 с. - ISBN 978-5-94074-408-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1027855>

Дополнительная литература:

2. *Алешников С.И., Козьминых Е.В.* Математические методы защиты информации. Ч. 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях: Практическое пособие. – Калининград: Изд-во РГУ им. И. Канта, 2006, . Переиздано: электронное издание, Изд-во БФУ, 2015 г

3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС

- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (<https://elib.kantiana.ru/>)

4. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе практики используются информационные технологии:

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security,
- LaTeX (+TexStudio), Python, GIT.

5. Описание материально-технической базы, необходимой для проведения практики

Для проведения отчетной конференции используются аудитории института/ школы; занятия проводятся с применением компьютера и видеопроектора. На всех компьютерах установлено необходимое программное обеспечение, требуемое в учебном процессе. Образовательная организация обеспечена необходимым комплектом лицензионного программного обеспечения, подлежащего ежегодному обновлению. Типовое программное обеспечение: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security, LaTeX (+TexStudio), Python, GIT.

При реализации практики в профильной организации на основании договора о практической подготовке обучающихся в качестве материально-технического обеспечения практики используется материальное оснащение профильной организации.

6. Методические рекомендации по прохождению практики

Этапы деятельности	Содержание деятельности	
	Преподаватель	Студент
Подготовка: определение цели и задач задания, установка необходимого ПО на ПК студента.	Выдает инструкцию по установке и работе с GIT, LaTeX. Предоставляет шаблон оформления презентации.	Согласно инструкциям устанавливает на свой ПК (или использует ПК университета) необходимое ПО.
Планирование: выбор криптоаналитической задачи с сайта cryptohack.org	Знакомит студентов с задачами формата CTF.	Выбирает задачу и разрабатывает план решения; обсуждает с

		преподавателем методы исследования
Решений задачи: решение выбранной задачи на языке Python кода	Консультирует студента по выбранным методам решения, методам программирования решения	Пишет код для решения выбранной задачи
Анализ информации: проверка полученного решения (флага)	Корректирует деятельность обучающегося, если полученный ответ или выбранный метод неверный	Проверка работоспособности/эффективности программы, корректности решения, дебаг
Оформление работы: подготовка и представление результатов	Консультирует в оформлении документов по практике	Оформляет конечные результаты в пакете Beamer (LaTeX)
Представление задания	Оценивает результаты исследования по заранее установленным критериям	Представляет результаты по заданию в форме письменного отчета и его устной защиты (презентации)
Подведение итогов: рефлексия, оценка	Оценивает усилия, использованные и неиспользованные возможности, творческий подход студента	Участствует в коллективном обсуждении итогов практики

При выборе базы практики целесообразно использовать оптимальное количество объективных критериев, оценивающих наиболее важные стороны организации или структурного подразделения университета как базы практики. К таким критериям относятся:

- соответствие профиля организации направлению обучения;
- обеспечение квалифицированными кадрами;
- оснащенность организации современным оборудованием и технологиями;
- наличие возможности дальнейшего трудоустройства и др.

Условия проведения практики в сторонних организациях регламентируются договорами о практической подготовке.

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное автономное образовательное учреждение высшего
образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Производственная практика (проектно-технологическая)»

Шифр: 10.05.01

Специальность: «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Квалификация (степень) выпускника: Специалист по защите информации

Калининград

2022

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНи-ИТ, к. ф.-м. н., доцент

Шпилевой А. А

Ведущий менеджер

Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.
3. Место практики в структуре образовательной программы.
4. Содержание практики.
5. Сведения о местах проведения практики
6. Указание форм отчетности по практике.
7. Фонд оценочных средств
8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики
10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для проведения практики.

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.

Вид практики: Производственная практика (проектно-технологическая) (далее **производственная практика** или **практика**).

Производственная практика проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения практики, указанного в календарном учебном графике.

Способы проведения преддипломной практики:

- стационарная на рабочем месте (в компании, с которой заключен договор на прохождение преддипломной практики).

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Целью практики является получение студентами профессиональных умений и опыта профессиональной деятельности.

Код компетенции	Результаты освоения образовательной программы (ИДК)	Перечень планируемых результатов
УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК.6.1. Определяет свои личные ресурсы, возможности и ограничения для достижения поставленной цели; УК.6.2. Создает и достраивает индивидуальную траекторию саморазвития при получении основного и дополнительного образования; УК.6.3. Умеет обобщать и транслировать свои индивидуальные достижения на пути реализации задач саморазвития; умеет рационально распределять временные и информационные ресурсы	- знать: свои личные ресурсы, возможности и ограничения для достижения поставленной цели; - уметь: обобщать и транслировать свои индивидуальные достижения на пути реализации задач саморазвития; рационально распределять временные и информационные ресурсы; - владеть: навыками создания индивидуальной траектории саморазвития при получении основного и дополнительного образования..
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей лично-	ОПК.1.1. Демонстрирует знания понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; ОПК.1.2. Демонстрирует	- знать: понятия информации, информационной безопасности, место и роли информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; - уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы информационной безопасности для объекта информатизации; - владеть: разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации.

сти, общества и государства	знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации; ОПК.1.3. Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации;	
ОПК – 4: Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации; ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации; ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации	<ul style="list-style-type: none"> – знать: физические законы и модели, необходимые при решении задач обеспечения защиты информации; – уметь: применять необходимые физические законы и модели для решения обеспечения защиты информации; – владеть: навыками моделирования для решения задач обеспечения защиты информации.
ОПК – 5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации; ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-	<ul style="list-style-type: none"> – знать: основные положения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации; – уметь: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; – владеть: анализом и разработкой проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.

	распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	
ОПК -6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ОПК-6.2. Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ОПК-6.3. Обладает навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	<ul style="list-style-type: none"> - знать: угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; - уметь: организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; - владеть: навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-11: Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты; ОПК-11.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению инфор-	<ul style="list-style-type: none"> - знать: меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты; - уметь: формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; - владеть: навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.

	<p>мационной безопасности; ОПК-11.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты</p>	
<p>ОПК-14: Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации</p>	<p>ОПК-14.1. Знает методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации;</p> <p>ОПК-14.2. Умеет проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;</p> <p>ОПК-14.3. Владеет навыками проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации</p>	<ul style="list-style-type: none"> – знать: методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации; – уметь: проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации; – владеть: навыками проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации.
<p>ОПК-15: Способен администрировать компьютерные сети и контролировать корректность их функционирования</p>	<p>ОПК-15.1. Знает устройство, порядок администрирования и контроля функционирования компьютерных сетей.</p> <p>ОПК-15.2. Умеет осуществлять администрирование и контроль корректности функционирования компьютерных сетей.</p> <p>ОПК-15.3. Владеет навыками администрирования и контроля функционирования компьютерных сетей</p>	<ul style="list-style-type: none"> – знать: устройство, порядок администрирования и контроля функционирования компьютерных сетей – уметь: осуществлять администрирование и контроль корректности функционирования компьютерных сетей. – владеть: навыками администрирования и контроля функционирования компьютерных сетей
<p>ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты</p>	<p>ОПК-16.1. Знает устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности</p>	<ul style="list-style-type: none"> – знать: устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях – уметь: осуществлять мониторинг работос-

информации в компьютерных системах и сетях	<p>средств защиты информации в компьютерных системах и сетях.</p> <p>ОПК-16.2. Умеет осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.</p> <p>ОПК-16.3. Владеет навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.</p>	<p>способности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p> <p>– <i>владеть</i>: навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях</p>
--	---	---

3. Место практики в структуре образовательной программы

Производственная практика относится к обязательной части блока 2 «Практики» ОПОП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Содержание практики

Студенты-практиканты выполняют программу практики в соответствии с планом-графиком практики, утверждаемым руководством базового предприятия и представителями Образовательно-научного кластера «Институт высоких технологий» БФУ им. И. Канта.

Ведется дневник практики и составляется заключительный отчет, который защищается после окончания практики и утверждается руководителями практики со стороны базового предприятия и института. В зависимости от специализации базового подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Студентам-практикантам должна быть предоставлена возможность ознакомиться с научно-технической документацией и научной литературой, которая касается предмета его исследований. В процессе прохождения практики студенты прослушивают лекции ведущих специалистов базовых предприятий, участвуют в научно-технических семинарах и конференциях при их наличии.

Студенты-практиканты проходят практику в отделах компьютерной безопасности, информационной и технической безопасности, компьютерных лабораториях, в которых работают их руководители и сотрудники подразделений. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для исследований, иметь возможность непосредственных консультаций во время работы со специалистами подразделений. Практиканты ежедневно работают в течение 3-4 часов в отделах предприятия. Объем теоретических занятий и семинаров определяется спецификой базового предприятия.

При прохождении производственной практики студенты изучают:

- административную и информационную структуру предприятия;
- основные нормативно-правовые положения в области информационной безопасности и защиты информации, на основании которых обеспечивается информационная безопасность предприятия;
- должностные инструкции сотрудников организации, отвечающих за безопасность;
- применяемые аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, используемых на предприятии;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности, современную технологию анализа потенциальных каналов утечки информации;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия, современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
- криптографические средства, стандарты в области криптографической защиты информации и криптографическую инфраструктуру, используемые на предприятии;
- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования
- структуру и методы построения современных моделей безопасности компьютерных систем;
- передовой опыт лучших специалистов подразделения;
- менеджмент в области программно-аппаратных и технических средств защиты информации.

При прохождении производственной практики студенты разрабатывают и исследуют:

- методы организации и управления деятельности служб защиты информации на предприятии;
- технологию проектирования, построения и эксплуатации систем и подсистем компьютерной безопасности;
- методы анализа уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- методы и схемы управления информационной безопасностью;
- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;

- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах
- методы оценки экономической эффективности применения программно-аппаратных и технических средств защиты информации.

При прохождении производственной практики возможен следующий перечень индивидуальных заданий:

- на основе стандартов в области информационной безопасности, нормативных документов и с помощью программно-аппаратных средств контроля вторжений произвести анализ и оценку уровня информационной защищённости предприятия или его компьютерной системы.
- разработать математические модели защищаемых информационных процессов, исследовать их свойства и приложения для создания средств защиты информации и систем, обеспечивающих информационную безопасность объектов.
- обосновать и выбрать рациональное решение по уровню обеспечения информационной безопасности предприятия с учетом заданных требований и стандартов информационной безопасности; разработать и обосновать рекомендации по совершенствованию существующей системы информационной безопасности предприятия или его компьютерной системы.
- разработать модификацию системы информационной безопасности предприятия или его компьютерной системы, или адаптировать существующую для обеспечения требуемого уровня безопасности; разработать необходимое программное обеспечение для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
- принять участие в разработке технических заданий на проектирование, разработку эскизных, технических и рабочих проектов систем и подсистем защиты информации, с учетом действующих нормативных и методических документов; подробно описать методику и этапы разработки технического задания.
- принять участие в разработке проектов систем и подсистем управления информационной безопасностью предприятия в соответствии с техническим заданием; подробно описать методику и этапы проектирования.
- принять участие в экспериментально-исследовательских работах по сертификации средств защиты информации и анализу результатов; подробно описать методику сертификации и порядок проведения соответствующих работ.

Задание на практику определяется вместе со студентом руководителями практики со стороны института и предприятия в начале практики. В конце практики студент должен представить результаты практики в виде отчета и сдать его руководителю от института. Руководитель практики от института организует защиту отчетов, по результатам которой на основании решения комиссии выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении производственной практики на предприятии, учреждении, организации, студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка;

- посещать все мероприятия по месту практики;
- подчиняться действующим на предприятии, в учреждении, организации правилам внутреннего трудового распорядка;
- изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить внедрению результатов, полученных практикантом, по месту практики, а также анализу возможности их применения и / или внедрения в учебный процесс при освоении дальнейших дисциплин.

Содержание практики

№ п/п	Этапы практики, их содержание	Виды деятельности обучающихся	Формы текущего контроля
1	Подготовительный этап	1. Определение базы прохождения практики. 2. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 3. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 4. Ознакомление с правилами внутреннего распорядка на базе прохождения практики. 5. Получение и согласование индивидуального задания по прохождению практики. 6. Разработка и утверждение индивидуальной программы практики и графика выполнения исследования. 7. Получение документации по практике (программы практики, индивидуального задания на практику, плана-графика прохождения практики и дневника практики с направлением на практику) в сроки, определенные программой. 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики.	Письменный отчет. Индивидуальное задание на практику.
2	Производственный	1. Выполнение производственных заданий. <ul style="list-style-type: none"> • Ознакомление с конкретными видами деятельности в соответствии с положениями структурных подразделений и должностными инструкциями. • Ознакомление с задачами отдела/службы организации базы практики. • Сбор информации и материалов в соответствии с заданием на практику. • Выполнение заданий, поставленных руководителями практики. • Обработка, систематизация и анализ фактического и теоретического материала. 2. Введение дневника практики.	Письменный отчет. Дневник практики
3	Заключительный этап	1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию существующего порядка работы, а также по внедрению но-	Зачет с оценкой.

№ п/п	Этапы практики, их содержание	Виды деятельности обучающихся	Формы текущего контроля
		вых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практики и прилагаемых документов для защиты.	

5. Сведения о местах проведения практики

Местами обеспечения производственной практики служат в организации, осуществляющие деятельность по профилю образовательной программы, в том числе ее структурном подразделении, предназначенном для проведения практической подготовки, на основании договора. Для обучающихся с ограниченными возможностями здоровья и инвалидов практика планируется и организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

1.	ООО «Центр Защиты Информации»
2.	ГАУ КО «КГНИЦ»
3.	АО «Янтарьэнерго»
4.	ООО «Алгоритм»
5.	АО «ЦентрИнформ»
6.	ООО «СКА и К»
7.	ООО «Сократ»
8.	АО «33 судоремонтный завод»
9.	“Elite Games Limited”
10.	ООО «Альпея»
11.	ООО «Е-Легион»
12.	ФГБК «Федеральный центр высоких медицинских технологий» Министерства здравоохранения Российской Федерации
13.	ООО «Хирокрафт»

6. Указание форм отчетности по практике

Формы отчетности студентов по производственной практике (заверенные подписью и печатью руководителя базы практики и / или руководителя практики от ОНК):

- индивидуальное задание на практику, заверенное руководителями практики от института и организации;
- план-график прохождения практики, заверенный руководителями практики от института и организации;
- дневник практики, заверенный руководителем практики от организации;
- отчет о результатах прохождения практики.

Формы отчетности руководителей практики:

- руководитель практики от ОНК не позднее 1 месяца после окончания практики предоставляет в институт отчет о проведенной преддипломной практике;
- руководитель практики от организации предоставляет отзыв о работе каждого студента-практиканта на практике.

Указанные документы представляются руководителю практики.

Дневник практики.

С момента прибытия и до конца пребывания на практике студент обязан вести «Дневник прохождения производственной практики», который является составной частью отчета о практике и используется при его написании. Записи в дневнике должны быть ежедневными. В дневнике фиксируются следующие виды работ: виды работ, их объем, краткое содержание, затраченное время.

В дневнике необходимо также отразить встретившиеся в работе затруднения, их характер, какие меры были приняты для их устранения, отметить недостатки в теоретической подготовке. Дневники периодически проверяются руководителем практики, в нем делаются отметки по его ведению, качеству выполняемой студентом работы. В дневнике руководитель практики дает отзыв о прохождении обучающимся практики (выполнении программы практики, отношении к порученной работе, собранных материалов) и выставляет оценку практики.

Отзыв руководителя практики от университета должен отражать основные структурные элементы: степень реализации плана практики; грамотность и полнота изложения материала в отчете; уровень самостоятельности выполнения работы; недостатки и замечания, выявленные как в процессе практики, так и в представленном отчете; положительные стороны, выявленные как в процессе практики, так и в представленном отчете; общий вывод об отчете с заключением о проделанной работе.

Отзыв руководителя практики от профильной организации, на базе которой студент проходил практику, должен отражать: краткую характеристику предоставленной информации, с которой работал обучающийся; методы и технологии, уровень самостоятельности, степень ответственности, добросовестности при выполнении работы; недостатки и замечания, выявленные в процессе прохождения практики; положительные стороны, выявленные в процессе прохождения практики; общий вывод об отчете с заключением о проделанной работе.

Отчет о практике составляется индивидуально каждым студентом в соответствии с методическими рекомендациями по прохождению практики и должен отражать его деятельность в период практики. В отчете следует отразить все вопросы, изученные во время прохождения практики, представить аналитические результаты анализа, выводы и рекомендации. Отчет о практике должен состоять из титульного листа, содержания, введения, основной части, заключения, списка литературы (при необходимости) и приложений (при необходимости). В заключении обобщаются результаты проделанной работы и делаются выводы и рекомендации. В конце отчета приводится список литературы и нормативных материалов, а также материалы приложений (графики, таблицы и т.д.).

Отчетная документация по практике (с приложениями) предоставляется в институт/школу не позднее 5 дней по окончании практики. Если практика проходит летом или в конце учебного семестра, то не позднее последнего рабочего (учебного) дня практики. За обучающихся заочной формы обучения отчетная документация предоставляется в период экзаменационной сессии (не позднее последнего учебного дня) соответствующего семестра.

7. Фонд оценочных средств

Текущий контроль прохождения практики производится руководителем практики в дискретные временные интервалы с использованием следующих оценочных средств:

- проверка ведения дневника производственной практики;

Промежуточная аттестация производится в форме зачета с оценкой с использованием следующих оценочных средств:

- Примерные контрольные вопросы к дифференцированному зачету по производственной практике:
 1. Какие нормативные документы по охране труда, технике безопасности и пожарной безопасности вам были предоставлены для изучения?
 2. В чем заключались Ваши права и обязанности в соответствии с должностной инструкцией?
 3. Какие нормативные документы для составления отчетности используются на предприятии?
 4. Суть порученных Вам производственных задач.
 5. Какие методы, технологии были предложены вами для решения поставленных производственных задач?
 6. Какие информационные системы/технологии используются на предприятии?
 7. Описать административную и информационную структуру предприятия.
 8. Описать цели и задачи, решаемые предприятием, направление деятельности предприятия.
 9. Описать используемые на предприятии технические и программные средства вычислительной техники.
 10. Описать организацию информационных систем с точки зрения информационной защищенности и защиты государственной тайны.
 11. Описать технические устройства хранения, обработки и передачи информации, используемые на предприятии.
 12. Представить анализ потенциальных каналов утечки информации и уязвимостей информационных процессов.
 13. Описать схему инженерно-технической защиты информации.
 14. Описать используемые методы и средства противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
 15. Представить перечень правовых положений в области информационной безопасности и защиты информации, регламентирующих уровень защищенности базового предприятия.
 16. Описать проведённые экспериментально-исследовательские работы по сертификации средств защиты информации и анализ их результатов.
 17. Представить и обосновать рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы.
 18. Представить эскизный проект модификации системы информационной безопасности предприятия или его компьютерной системы.
 19. Описать структуру и функции разработанного программного обеспечения для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
 20. Каковы выводы и предложения по внедрению рекомендаций по совершенствованию системы информационной безопасности на предприятии?
- дневник производственной практики;

- отзыв руководителя практики от предприятия;
- отчет студента о прохождении практики.

При оценке результатов практики принимается во внимание:

- соответствие отчета заданию на практику;
- степень полноты выполненных задач, достижения цели практики;
- соблюдение графика прохождения практики;
- характеристика на обучающегося, составленная руководителем практики от профильной организации;
- оформление отчета по практике;
- содержательность доклада, аргументированность и полнота ответов на вопросы при защите результатов практики.

Зачёт по практике (в виде защиты отчёта) принимает групповой руководитель в индивидуальном порядке.

Во время защиты обучающийся должен подтвердить уровень образовательных результатов практики в соответствии с требованиями, определенными программой практики.

При оценке итогов практики обучающегося принимается во внимание отзыв руководителя практики от профильной организации

По результатам защиты студенту выставляется зачет с оценкой.

Уровни	Содержательно е описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалль ная шкала (академиче ская) оценка	БРС, % освоения (рейтингов ая оценка)
Повышен ный	Творческая деятельность	<i>Включает нижестоящий уровень.</i> Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональ ной деятельности,	<i>Включает нижестоящий уровень.</i> Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или	хорошо	71-85

	нежели по образцу с большей степени самостоятельности и инициативы	обосновывать практику применения		
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно	55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	Менее 55

8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики

8.1. Основная литература

1. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета) №1459. утвержден 26 ноября 2020 г.
2. Приказ Минобрнауки России от 27.11.2015 №1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования» (зарегистрировано в Минюсте России 18.12.2015 №40168).
3. Положение о практической подготовке обучающихся в федеральном государственном автономном образовательном учреждении высшего образования «Балтийский федеральный университет имени Иммануила Канта (принято решением ученого совета БФУ им. И. Канта 23 декабря 2021 года, протокол №2).

8.2. Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информац. потоками: Учебное пособие для вузов/П.Н.Девянин-2-е изд., испр. и доп.- Москва :Гор.линия-Телеком,2013-338с.:ил.;. - (Специальность). ISBN 978-5-9912-0328-9, 100 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/436878> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Москва :Гор. линия-Телеком, 2013. - 214 с.: . - (Во-

- просы управления информационной безопасностью) ISBN 978-5-9912-0274-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/560783> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Костин, В. Н. Методы и средства защиты компьютерной информации: законодательные и нормативные акты по защите информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2017. - 26 с. - ISBN 978-5-906846-87-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232204> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 4. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Гор. линия-Телеком, 2012. - 184 с.: ил.; . ISBN 978-5-9912-0246-6, 500 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/367555> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 5. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1167736> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 6. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1210523> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 7. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189326> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 8. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1178150> (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для выполнения практики

1. НЭБ Национальная электронная библиотека, диссертации и прочие издания
2. eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
3. Гребенников Электронная библиотека ИД журналы
4. ЭБС Лань книги, журналы
5. ЭБС Консультант студента
6. ПРОСПЕКТ ЭБС
7. ЭБС ZNANIUM.COM

8. РГБ Информационное обслуживание по МБА
9. БЕН РАН
10. Электронно-библиотечная система (ЭБС) Кантитана (<https://elib.kantiana.ru/>)
11. http://lib.mexmat.ru/catalogue.php?dir=02_06 - Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография
12. http://booklid.org/g/mt_number+theory - Библиотека научной литературы. Раздел «Теория чисел».
13. <https://www.coursehero.com/file/p7t1rf7/External-links-Certicom-ECC-Tutorial-http-www-certicom-com-index-php-ecc/> - Online Elliptic Curve Cryptography Tutorial, Certicom Corp.
14. [MathWorld](http://mathworld.wolfram.com/). – математический сайт, созданный *Weisstein, Eric W.* (англ.).
15. <http://mathworld.wolfram.com/> - сайт по эллиптическим кривым.
16. <http://mathemlib.ru/> - библиотека по математике.
17. <http://www.math.uiuc.edu/~r-ash/ANT.html> - курс по алгебраической теории чисел Robert B. Ash.
18. <http://www1.spms.ntu.edu.sg/~frederique/Teaching.html> - электронные курсы лекций: алгебра, алгебраическая теория чисел, дискретная математика, группы и симметрии.
19. <http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf> - Лекции по алгебраической теории чисел F.Oggier.
20. <http://www.math.wisc.edu/~mmwood/748Fall2014/weston.pdf> - лекции по алгебраической теории чисел Tom Weston.
21. <http://www2.warwick.ac.uk/fac/sci/math/undergrad/ughandbook/year3/ma3a6/> - электронные лекции по алгебраической теории чисел университета Warwick.
22. <http://arxiv.org/list/math.AG/recent> - архив новых публикаций по алгебраической геометрии.
23. <http://www.jmilne.org/math/CourseNotes/ag.html> - веб-сайт J.Miln'a с публикациями по алгебраической геометрии.
24. <http://www.fen.bilkent.edu.tr/~franz/LN/LN-algeo.html> - собрание лекций по алгебраической геометрии.
25. http://www.math.utah.edu/~yplee/teaching/LN_ag.html - собрание лекций по алгебраической геометрии.
26. <http://www.math.byu.edu/~jarvis/alg-geom.html> - информация о веб-сайтах по алгебраической геометрии.
27. <http://ocw.mit.edu/courses/mathematics/18-726-algebraic-geometry-spring-2009/lecture-notes/> - открытый курс лекций по алгебраической геометрии.
28. <http://www.freebookcentre.net/Mathematics/Algebraic-Geometry-Books.html> - лекции по алгебраической геометрии в свободном доступе.

10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе практики используются информационные технологии:

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Программа для ЭВМ Wolfram Mathematica 10.2 Education Bundled Price (Количество лицензий – 3, Номер акта / накладной – Tr053766, Дата акта – 02.11.15);
- IBM SPSS Statistics Base Campus Edition (Количество лицензий – 25, Номер акта / накладной – Tr031923, Дата акта – 10.06.15);
- Intel Cluster Studio for Linux (Количество лицензий – 2, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Maple 11 (Количество лицензий – 30, Номер акта / накладной – Tr068983, Дата акта – 19.12.07);
- Mathematica (Количество лицензий – 15, Номер акта / накладной – Tr066706, Дата акта – 18.11.13);
- Mathworks Gauges Blockset Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Mathworks Simulink 3d animation Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Tr063168, Дата акта – 24.11.14);
- Microsoft Visio Professional 2010 (Количество лицензий – 25, Номер акта / накладной – Tr070182, Дата акта – 15.12.11);
- Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Parallel Computing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Signal Processing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Statistica Base (Количество лицензий – 20, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Statistics Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- System Identification Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11).

11. Описание материально-технической базы, необходимой для проведения

практики

Для проведения отчетной конференции используются аудитории института/ школы; занятия проводятся с применением компьютера и видеопроектора. На всех компьютерах установлено необходимое программное обеспечение, требуемое в учебном процессе. Образовательная организация обеспечена необходимым комплектом лицензионного программного обеспечения, подлежащего ежегодному обновлению. Типовое программное обеспечение: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

При реализации практики в профильной организации на основании договора о практической подготовке обучающихся в качестве материально-технического обеспечения практики используется материальное оснащение профильной организации.

1. Методические рекомендации по прохождению практики

Этапы деятельности	Содержание деятельности	
	Преподаватель	Студент
Подготовка: определение цели и задач задания	Мотивирует, помогает обучающемуся в постановке задач	Определяет и обсуждает с преподавателем актуальность проблемы; выдвигает совместно с преподавателем гипотезу исследования
Планирование: определение источников, способов сбора, анализа информации, способов представления результатов, установление критериев оценки результата и процесса	Корректирует в случае необходимости деятельность обучающегося, предлагает идеи, высказывает предположения	Формулирует задачи и разрабатывает план действий; обсуждает с преподавателем методы исследования
Сбор информации: наблюдение, работа со справочной литературой, нормативно-правовой, учебной, научной и др. литературы	Наблюдает за деятельностью обучающегося, косвенно руководит его исследовательской деятельностью	Собирает и систематизирует информацию
Анализ информации: формулирование выводов	Корректирует деятельность обучающегося, наблюдает, советует	Анализирует собранную информацию
Оформление работы: подготовка и представление результатов	Консультирует в оформлении документов по практике	Оформляет конечные результаты
Представление задания	Оценивает результаты исследования по заранее установленным критериям	Представляет результаты по заданию в форме письменного отчета и его устной защиты
Подведение итогов: рефлексия, оценка	Оценивает усилия, использованные и неиспользованные возможности, творческий подход студента	Участствует в коллективном обсуждении итогов практики

При выборе базы практики целесообразно использовать оптимальное количество объективных критериев, оценивающих наиболее важные стороны организации или структурного подразделения университета как базы практики. К таким критериям относятся:

- соответствие профиля организации направлению обучения;
- обеспечение квалифицированными кадрами;
- оснащенность организации современным оборудованием и технологиями;
- наличие возможности дальнейшего трудоустройства и др.

Условия проведения практики в сторонних организациях регламентируются договорами о практической подготовке.

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное автономное образовательное учреждение
высшего образования «Балтийский федеральный университет имени Иммануила
Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Производственная практика (научно-исследовательская работа)»

Шифр: 10.05.01

Специальность: «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Квалификация (степень) выпускника: Специалист по защите информации

Калининград

2022 г.

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора
ИФМНиИТ, к. ф.-м. н., доцент

Шпилевой А. А

Ведущий менеджер

Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.
3. Место практики в структуре образовательной программы.
4. Содержание практики.
5. Сведения о местах проведения практики
6. Указание форм отчетности по практике.
7. Фонд оценочных средств
8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики
10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для проведения практики.

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.

Вид практики: Производственная практика (научно-исследовательская работа) (далее научно-исследовательская работа или НИР).

НИР проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения НИР, указанного в календарном учебном графике.

Способы проведения НИР:

- стационарная на рабочем месте. Включает в себя самостоятельную работу студентов.

Итогом НИР является представление отчета по НИР об основных результатах проведенной научно-исследовательской работы.

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.

Целью НИР является освоение студентом методики проведения всех этапов научно-исследовательской работы – от постановки задачи исследования; через исследование и разработку средств и систем защиты информации, доказательный анализ защищённости компьютерных систем от вредоносных программно-технических воздействий в условиях существования угроз в информационной сфере; через рациональное планирование эксплуатации систем управления и обеспечения информационной безопасности; до подготовки отчётов по теме или её разделу.

Код компетенции	Результаты освоения образовательной программы (ИДК)	Перечень планируемых результатов
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	знать: - необходимые математические методы для решения задач обеспечения защиты информации; уметь: - применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; владеть: разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации
ОПК – 7: Способен	ОПК-7.1. Разрабатывает	знать:

<p>создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования</p>	<p>программы на языках высокого и низкого уровня. ОПК-7.1. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.1. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.</p>	<p>- методику разработки программ на языках высокого и низкого уровня уметь: - применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач владеть: - обоснованным выбором инструментария программирования и способов организации программ.</p>
<p>ОПК – 8: Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p>	<p>ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации. ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов. ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.</p>	<p>знать: - принципы работы с научной литературой, методы поиска научно-технической информации уметь: - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов владеть: навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы</p>
<p>ОПК – 9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты</p>	<p>ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты</p>	<p>знать: - методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации уметь: - решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. владеть: - навыками решения задач профессиональной</p>

<p>информации от утечки по техническим каналам, сетей и систем передачи информации</p>	<p>информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.3. Владеет навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p>	<p>деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p>
<p>ОПК – 11: Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p>	<p>ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты. ОПК-11.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. ОПК-11.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной</p>	<p>знать: - меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты уметь: - формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности владеть: - навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.</p>

	безопасности на объекте защиты.	
--	---------------------------------	--

3. Место практики в структуре образовательной программы

Научно-исследовательская работа относится к обязательной части блока 2 «Практики» ОПОП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Содержание практики

Студенты выполняют программу НИР в соответствии с индивидуальным планом проведения НИР, утверждаемым руководителем НИР.

Ведется дневник НИР и составляется заключительный отчет, который защищается после окончания практики и утверждается руководителем НИР.

Студентам должна быть предоставлена возможность ознакомиться с научно-технической документацией и научной литературой, которая касается предмета его исследований. В процессе выполнения НИР студенты прослушивают лекции ведущих специалистов, участвуют в научно-технических семинарах и конференциях при их наличии.

Студенты проходят НИР в лабораториях образовательно-научного кластера «Института высоких технологий», относящихся к специальности «Компьютерная безопасность» и компьютерных классах. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для исследований, иметь возможность непосредственных консультаций во время проведения НИР с руководителями ВКР.

В результате выполнения НИР студент готовит материалы для написания ВКР в рамках ее предполагаемой тематики и в соответствии со специализацией «Математические методы защиты информации».

При проведении НИР студенты **изучают**:

- научную литературу по теме ВКР (монографии, статьи, патентные материалы, научные отчёты, техническую документацию, авторефераты и диссертации);
- современную технологию анализа потенциальных каналов утечки информации;
- структуру и методы построения современных моделей безопасности компьютерных систем;
- современную технологию защиты информации в компьютерных системах;
- современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования.

При проведении НИР студенты разрабатывают и **исследуют**:

- алгоритмы быстрых вычислений в алгебраических структурах, их компьютерную реализацию;
- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;

- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах;

При выполнении НИР возможен следующий перечень **индивидуальных заданий**:

- Разработка методик анализа и оценки уровней защищённости компьютерных систем.
- Проектирование защищённых компьютерных систем, в частности систем автоматизированной обработки персональных данных.
- Разработка систем защиты информации и систем управления информационной безопасностью, основанных на новых логических и математических принципах;
- Разработка методов контроля эффективности защиты информации, основанных на новых математических моделях и методах;
- Анализ эффективности, модификация и построение криптографических алгоритмов, основанных на новых математических принципах.
- Разработка и анализ систем помехоустойчивого кодирования на алгебраических кривых над конечными полями с большим числом точек.
- Проектирование и статистический анализ качества потоковых шифров и генераторов псевдослучайных чисел.
- Компьютерное моделирование эффективных алгоритмов: вычислительных, криптографических, кодирования, сжатия и восстановления информации при её передаче и хранении.
- Анализ и разработка криптографической инфраструктуры для конкретных систем защиты информации; алгоритмическое обеспечение инфраструктуры.
- Анализ стойкости и разработка схем и защищённых протоколов обмена информацией в компьютерных системах и сетях общего назначения.
- Анализ стойкости и разработка защищённых протоколов обмена информацией в специализированных компьютерных системах и сетях: банковских, корпоративных, системах электронного голосования и т.д.

Задание на НИР определяется вместе со студентом руководителями НИР в начале работы. В конце выполнения НИР студент должен представить результаты НИР в виде отчета и сдать его руководителю от института. Руководитель НИР организует защиту отчетов, по результатам которой на основании решения комиссии выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении НИР в лабораториях и компьютерных классах студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка, принятого в лабораториях ОНК «Института высоких технологий»;
- посещать все мероприятия научного характера по теме НИР, проводимые в ОНК «Института высоких технологий»;
- подчиняться действующим в лабораториях правилам внутреннего трудового распорядка;
- изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить анализу возможности публичного представления результатов НИР, возможности внедрения результатов исследования в проектную деятельность, инженерную практику и в производство.

Содержание практики

№ п/п	Этапы (периоды) НИР	Вид работ	Форма текущего контроля
1	Подготовительный этап	1. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения НИР. 2. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 3. Ознакомление с правилами внутреннего распорядка на базе прохождения НИР. 4. Получение и согласование индивидуального задания по прохождению НИР. 5. Составление индивидуального плана НИР совместно с научным руководителем: выбор и обоснование текущей темы исследования; составление рабочего плана и графика выполнения исследования. 6. Получение документации по НИР (программа НИР и дневник НИР) в сроки, определенные программой.	Письменный отчёт. Индивидуальное задание на НИР.
2	Производственный этап	1. Подготовка к проведению научного исследования: ознакомление со структурой и принципами работы исследуемых компьютерных систем, взаимосвязей между информационными потоками; постановка целей и конкретных задач; формулировка рабочих гипотез; обзор и анализ литературы по теме исследования, сбор информации. 2. Проведение экспериментального исследования: компьютерное моделирование и статистический анализ уровней защищённости компьютерных систем, вычислительной эффективности алгоритмов, качества псевдослучайных последовательностей. 3. Проведение теоретического исследования: разработка структурных схем, математических моделей,	Письменный отчет. Дневник НИР

№ п/п	Этапы (периоды) НИР	Вид работ	Форма текущего контроля
		протоколов обмена информацией; анализ свойств математических моделей; анализ и разработка алгоритмов; планирование компьютерных экспериментов; компьютерное моделирование алгоритмов. 4. Обработка, систематизация и анализ полученных теоретических результатов и результатов компьютерного моделирования, проверка корректности разработанных алгоритмов; проверка работоспособности комплекса программ. 5. Анализ возможности публичного представления результатов НИР, возможности внедрения результатов исследования в проектную деятельность, инженерную практику, в производство.	
3	Заключительный этап	1. Подготовка отчета о НИР, представления отчета по НИР и прилагаемых документов для защиты.	Зачет с оценкой.

5. Сведения о местах проведения практики

Практика проводится в ОНК «Институт высоких технологий» БФУ им. И. Канта. Для обучающихся с ограниченными возможностями здоровья и инвалидов практика планируется и организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья

Материально-техническим обеспечением производственной (научно-исследовательская работа) практики служат учебные (специальные) классы и лаборатории ОНК «Института высоких технологий» БФУ им. И. Канта, а также читальные залы Университета.

6. Указание форм отчетности по практике

Формы отчетности студентов по НИР:

- Дневник практики;
- Отчет по практике с приложениями.

Формы отчетности руководителей НИР:

- не позднее 1 месяца после окончания НИР предоставляет в институт отчет о проведенной НИР;
- предоставляет отзыв о научно-исследовательской работе каждого студента, заверенный также подписью руководителя ВКР.

Указанные документы представляются руководителю практики.
Дневник практики.

С момента прибытия и до конца пребывания на практике студент обязан вести «Дневник прохождения производственной практики», который является составной частью отчета о практике и используется при его написании. Записи в дневнике должны быть ежедневными. В дневнике фиксируются следующие виды работ: обработка данных, их анализ, краткие выводы в соответствии с тематикой ВКР.

В дневнике необходимо также отразить встретившиеся в работе затруднения, их характер, какие меры были приняты для их устранения, отметить недостатки в теоретической подготовке. Дневники периодически проверяются руководителем практики, в нем делаются отметки по его ведению, качеству выполняемой студентом работы. В дневнике руководитель практики дает отзыв о прохождении обучающимся практики (выполнении программы практики, отношении к порученной работе, собранных материалов) и выставляет оценку практики.

Отзыв руководителя практики от университета должен отражать основные структурные элементы: степень реализации плана практики; грамотность и полнота изложения материала в отчете; уровень самостоятельности выполнения работы; недостатки и замечания, выявленные как в процессе практики, так и в представленном отчете; положительные стороны, выявленные как в процессе практики, так и в представленном отчете; общий вывод об отчете с заключением о проделанной работе.

Отзыв руководителя практики от профильной организации, на базе которой студент проходил практику, должен отражать: краткую характеристику предоставленной информации, с которой работал обучающийся; методы и технологии, уровень самостоятельности, степень ответственности, добросовестности при выполнении работы; недостатки и замечания, выявленные в процессе прохождения практики; положительные стороны, выявленные в процессе прохождения практики; общий вывод об отчете с заключением о проделанной работе.

Отчет о практике составляется индивидуально каждым студентом в соответствии с методическими рекомендациями по прохождению практики и должен отражать его деятельность в период практики. В отчете следует отразить все вопросы, изученные во время прохождения практики, представить аналитические результаты анализа, выводы и рекомендации. Отчет о практике должен состоять из титульного листа, содержания, введения, основной части, заключения, списка литературы (при необходимости) и приложений (при необходимости). В заключении обобщаются результаты проделанной работы и делаются выводы и рекомендации. В конце отчета приводится список литературы и нормативных материалов, а также материалы приложений (графики, таблицы и т.д.).

Отчетная документация по практике (с приложениями) предоставляется в институт/школу не позднее 5 дней по окончании практики. Если практика проходит летом или в конце учебного семестра, то не позднее последнего рабочего (учебного) дня практики. За обучающихся заочной формы обучения отчетная документация предоставляется в период экзаменационной сессии (не позднее последнего учебного дня) соответствующего семестра.

7. Фонд оценочных средств

Порядок аттестации студентов по результатам НИР

По окончании НИР проводится ***дифференцированный зачет***. При проведении зачета используются следующие критерии итоговой оценки за НИР:

- грамотный обзор и анализ литературы по теме исследования;
- наличие постановок конкретных задач исследования;
- наличие планов и результатов предварительного компьютерного моделирования, результаты статистического анализа его итогов;
- ясное и логичное описание рабочих гипотез, структурных схем, математических моделей, протоколов обмена информацией, вычислительных алгоритмов;
- обоснованные результаты исследования и анализа свойств математических моделей;
- обоснованные результаты анализа эффективности разработанных алгоритмов;
- достаточно полное описание разработанного комплекса программ;
- наличие планов и результатов компьютерного моделирования в соответствии с разработанными моделями и алгоритмами, результаты анализа адекватности разработанных математических моделей, корректности алгоритмов, работоспособности комплекса программ;
- правильные ответы студента на вопросы преподавателя, касающиеся предмета НИР.

Текущий контроль прохождения практики производится руководителем практики в дискретные временные интервалы с использованием следующих оценочных средств:

- контроль выполнения задания на НИР согласно индивидуальному плану;
- проверка ведения дневника практики.

Промежуточная аттестация производится в форме зачета с оценкой с использованием следующих оценочных средств:

- индивидуальное задание на НИР;
- контрольные вопросы к дифференцируемому зачету;
- отзыв руководителя НИР;
- отчет студента о НИР.

Вопросы для дифференцированного зачёта:

1. Сформулировать научную задачу (проблему), решаемую в рамках НИР.
2. Описать актуальность и научную значимость решения поставленной задачи (проблемы).
3. Описать результаты анализа эффективности и защищённости исследуемой компьютерной системы (предприятия, организации).
4. Описать частичные задачи, к решению которых сводится главная задача (проблема).
5. По результатам обзора литературы описать состояние решения поставленной задачи (проблемы) на сегодняшний день.

6. Описать планы и результаты проведённых компьютерных экспериментов по определению эффективности и уровней защищённости исследуемой компьютерной системы (предприятия, организации).
7. Описать основные идеи и математические модели, лежащие в основе теоретического исследования.
8. Описать результаты исследования свойств разработанных (используемых) математических моделей.
9. Описать разработанные вычислительные алгоритмы и оценки их эффективности.
10. Описать структуру программного комплекса, реализующего разработанные алгоритмы.
11. Описать планы и результаты компьютерных экспериментов, подтверждающих работоспособность комплекса программ.
12. Произвести сравнительный анализ результатов вычислительных экспериментов.
13. Описать перспективы практического использования результатов решения поставленной задачи (проблемы).

При оценке результатов практики принимается во внимание:

- соответствие отчета заданию на практику;
- степень полноты выполненных задач, достижения цели практики;
- соблюдение графика прохождения практики;
- характеристика на обучающегося, составленная руководителем практики от профильной организации;
- оформление отчета по практике;
- содержательность доклада, аргументированность и полнота ответов на вопросы при защите результатов практики.

Зачёт по практике (в виде защиты отчёта) принимает групповой руководитель в индивидуальном порядке.

Во время защиты обучающийся должен подтвердить уровень образовательных результатов практики в соответствии с требованиями, определенными программой практики.

При оценке итогов практики обучающегося принимается во внимание отзыв руководителя практики от профильной организации

По результатам защиты студенту выставляется зачет с оценкой.

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	<i>Включает нижестоящий уровень.</i> Умение самостоятельно принимать решение, решать	отлично	86-100

		проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий		
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	<i>Включает нижестоящий уровень.</i> Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо	71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно	55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	Менее 55

8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики

8.1. Основная литература

1. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета) №1459. утвержден 26 ноября 2020 г.
2. Приказ Минобрнауки России от 27.11.2015 №1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования» (зарегистрировано в Минюсте России 18.12.2015 №40168);
3. Положение о практической подготовке обучающихся в федеральном государственном автономном образовательном учреждении высшего образования

«Балтийский федеральный университет имени Иммануила Канта (принято решением ученого совета БФУ им. И. Канта 23 декабря 2021 года, протокол №2).

8.2. Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информац. потоками: Учебное пособие для вузов/П.Н.Девянин-2-е изд., испр. и доп.-Москва :Гор.линия-Телеком,2013-338с.:ил.; - (Специальность). ISBN 978-5-9912-0328-9, 100 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/436878> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Москва :Гор. линия-Телеком, 2013. - 214 с.: . - (Вопросы управления информационной безопасностью)ISBN 978-5-9912-0274-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/560783> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Костин, В. Н. Методы и средства защиты компьютерной информации: законодательные и нормативные акты по защите информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2017. - 26 с. - ISBN 978-5-906846-87-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232204> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
4. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Гор. линия-Телеком, 2012. - 184 с.: ил.; . ISBN 978-5-9912-0246-6, 500 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/367555> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
5. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1167736> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
6. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1210523> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
7. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189326> (дата обращения: 13.01.2022). – Режим доступа: по подписке.

8. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1178150> (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики

1. НЭБ Национальная электронная библиотека, диссертации и прочие издания
2. eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
3. Гребенников Электронная библиотека ИД журналы
4. ЭБС Лань книги, журналы
5. ЭБС Консультант студента
6. ПРОСПЕКТ ЭБС
7. ЭБС ZNANIUM.COM
8. РГБ Информационное обслуживание по МБА
9. БЕН РАН
10. Электронно-библиотечная система (ЭБС) Кантитана (<https://elib.kantiana.ru/>)
11. http://lib.mexmat.ru/catalogue.php?dir=02_06 - Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография
12. http://booklid.org/g/mt_number+theory - Библиотека научной литературы. Раздел «Теория чисел».
13. <https://www.coursehero.com/file/p7t1rf7/External-links-Certicom-ECC-Tutorial-http-www-certicom-com-index-php-ecc/> - Online Elliptic Curve Cryptography Tutorial, Certicom Corp.
14. [MathWorld](http://mathworld.wolfram.com/). – математический сайт, созданный *Weisstein, Eric W.* (англ.).
15. <http://mathworld.wolfram.com/> - сайт по эллиптическим кривым.
16. <http://mathemlib.ru/> - библиотека по математике.
17. <http://www.math.uiuc.edu/~r-ash/ANT.html> - курс по алгебраической теории чисел Robert B. Ash.
18. <http://www1.spms.ntu.edu.sg/~frederique/Teaching.html> - электронные курсы лекций: алгебра, алгебраическая теория чисел, дискретная математика, группы и симметрии.
19. <http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf> - Лекции по алгебраической теории чисел F.Oggier.
20. <http://www.math.wisc.edu/~mmwood/748Fall2014/weston.pdf> - лекции по алгебраической теории чисел Tom Weston.
21. <http://www2.warwick.ac.uk/fac/sci/maths/undergrad/ughandbook/year3/ma3a6/> - электронные лекции по алгебраической теории чисел университета Warwick.
22. <http://arxiv.org/list/math.AG/recent> - архив новых публикаций по алгебраической геометрии.

23. <http://www.jmilne.org/math/CourseNotes/ag.html> - веб-сайт J.Miln'a с публикациями по алгебраической геометрии.
24. <http://www.fen.bilkent.edu.tr/~franz/LN/LN-algeo.html> - собрание лекций по алгебраической геометрии.
25. http://www.math.utah.edu/~yplee/teaching/LN_ag.html - собрание лекций по алгебраической геометрии.
26. <http://www.math.byu.edu/~jarvis/alg-geom.html> - информация о веб-сайтах по алгебраической геометрии.
27. <http://ocw.mit.edu/courses/mathematics/18-726-algebraic-geometry-spring-2009/lecture-notes/> - открытый курс лекций по алгебраической геометрии.
28. <http://www.freebookcentre.net/Mathematics/Algebraic-Geometry-Books.html> - лекции по алгебраической геометрии в свободном доступе.

10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе практики используются информационные технологии:

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Программа для ЭВМ Wolfram Mathematica 10.2 Education Bundled Price (Количество лицензий – 3, Номер акта / накладной – Tr053766, Дата акта – 02.11.15);
- IBM SPSS Statistics Base Campus Edition (Количество лицензий – 25, Номер акта / накладной – Tr031923, Дата акта – 10.06.15);
- Intel Cluster Studio for Linux (Количество лицензий – 2, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Maple 11 (Количество лицензий – 30, Номер акта / накладной – Tr068983, Дата акта – 19.12.07);
- Mathematica (Количество лицензий – 15, Номер акта / накладной – Tr066706, Дата акта – 18.11.13);
- Mathworks Gauges Blockset Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Mathworks Simulink 3d animation Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);

- Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Tr063168, Дата акта – 24.11.14);
- Microsoft Visio Professional 2010 (Количество лицензий – 25, Номер акта / накладной – Tr070182, Дата акта – 15.12.11);
- Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Parallel Computing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Signal Processing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- Statistica Base (Количество лицензий – 20, Номер акта / накладной – Tr063374, Дата акта – 19.12.07).
- Statistics Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11);
- System Identification Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Tr072207, Дата акта – 16.12.11).

11. Описание материально-технической базы, необходимой для проведения практики

Для проведения отчетной конференции используются аудитории института/школы; занятия проводятся с применением компьютера и видеопроектора. На всех компьютерах установлено необходимое программное обеспечение, требуемое в учебном процессе. Образовательная организация обеспечена необходимым комплектом лицензионного программного обеспечения, подлежащего ежегодному обновлению. Типовое программное обеспечение: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

При реализации практики в профильной организации на основании договора о практической подготовке обучающихся в качестве материально-технического обеспечения практики используется материальное оснащение профильной организации.

12. Методические рекомендации по прохождению практики

Этапы деятельности	Содержание деятельности	
	Преподаватель	Студент
Подготовка: определение цели и задач задания	Мотивирует, помогает обучающемуся в постановке задач	Определяет и обсуждает с преподавателем актуальность проблемы; выдвигает совместно с преподавателем гипотезу

		исследования
Планирование: определение источников, способов сбора, анализа информации, способов представления результатов, установление критериев оценки результата и процесса	Корректирует в случае необходимости деятельность обучающегося, предлагает идеи, высказывает предположения	Формулирует задачи и разрабатывает план действий; обсуждает с преподавателем методы исследования
Сбор информации: наблюдение, работа со справочной литературой, нормативно-правовой, учебной, научной и др. литературы	Наблюдает за деятельностью обучающегося, косвенно руководит его исследовательской деятельностью	Собирает и систематизирует информацию
Анализ информации: формулирование выводов	Корректирует деятельность обучающегося, наблюдает, советует	Анализирует собранную информацию
Оформление работы: подготовка и представление результатов	Консультирует в оформлении документов по практике	Оформляет конечные результаты
Представление задания	Оценивает результаты исследования по заранее установленным критериям	Представляет результаты по заданию в форме письменного отчета и его устной защиты
Подведение итогов: рефлексия, оценка	Оценивает усилия, использованные и неиспользованные возможности, творческий подход студента	Участствует в коллективном обсуждении итогов практики

При выборе базы практики целесообразно использовать оптимальное количество объективных критериев, оценивающих наиболее важные стороны организации или структурного подразделения университета как базы практики. К таким критериям относятся:

- соответствие профиля организации направлению обучения;
- обеспечение квалифицированными кадрами;
- оснащенность организации современным оборудованием и технологиями;
- наличие возможности дальнейшего трудоустройства и др.

Условия проведения практики в сторонних организациях регламентируются договорами о практической подготовке.

Программно-аппаратные средства лаборатории программно-аппаратных средств защиты информации согласно имеющемуся перечню.

1. Маршрутизатор Cisco 2821. Коммутатор switch d-link des-3526. Стойка серверная 1000 мм 42u с дополнительным пассивным и организующим оборудованием.
2. АПКШ «Континент» (криптошлюз) в корпусе промышленного PC (1U), ЦУС «Континент» (центр управления сетью) в корпусе промышленного PC (1U) с сервером доступа, Абонентский пункт «Континент-АП».
3. «Аккорд-NT/2000» v. 2.0.1 на базе комплекса СЗИ НСД «Аккорд-АМДЗ» v.3.1 (PCI).
4. Средство криптографической защиты информации, включающее библиотеки шифрования и электронную цифровую подпись Верба-W.
5. Средство криптографической защиты информации КРИПТО-ПРО УЦ.
6. Система обеспечения безопасности информации в корпоративной сети «Secret Net» версии 5.0. (обновление) в составе: - Сервер безопасности Secret Net 5.0 -С (до 50 защищаемых серверов и рабочих станций); - «Secret Net» для Windows 2000/XP/2003 (клиенты сервера безопасности); - Системы обеспечения безопасности информации автономных компьютеров «Secret Net» версии 5.0. (обновление); - «Secret Net 5.0 – С» для Windows 2000|XP/2003.
7. Система обнаружения атак Real Secure Network 10/100.
8. Программный продукт для обеспечения сетевой безопасности Internet Scanner.
9. Программный продукт для обеспечения сетевой безопасности X Spider 7.
10. Средство контроля защищенности от несанкционированного доступа “Ревизор сети” (версия 1.2.1.0).
11. Средство контроля защищенности от несанкционированного доступа “Ревизор системы” (версия 1.0).
12. Средство контроля защищенности от несанкционированного доступа “TERRIER (версия 3.0).
13. Средство контроля защищенности от несанкционированного доступа “Ревизор 1 XP”.
14. Средство контроля защищенности от несанкционированного доступа “Ревизор 2 XP”.
15. Средство контроля защищенности от несанкционированного доступа ФИКС 3.0.
16. Персональное средство криптографической защиты информации ПСКЗИ ШИПКА-1.5.
17. Межсетевой экран ССПТ-1М, исполнение 54323649.401350.003-03 (корпус Iwill G478_XG(19” 1U).
18. Программное средство для защиты от несанкционированного доступа к информации в персональном компьютере с возможностью подключения аппаратных идентификаторов Dallas Lock 7.0.

Технические средства лаборатории технических средств защиты информации согласно имеющемуся перечню

1. Программно-аппаратный комплекс автоматического обнаружения, идентификации и нейтрализации подслушивающих устройств типа «Крона плюс».
2. Анализатор спектра типа "СК-4 Белан - 32".
3. Комплекс для проведения исследований на ПЭМИН типа «НАВИГАТОР».
4. Универсальный поисковый прибор типа «СРМ-700 Advancer + ВМР 1200.
5. Анализатор проводных линий типа «Отклик».
6. Портативный металло-детектор типа «ВМ311».
7. Блокиратор сотовых телефонов типа «Завеса».
8. Прибор ночного видения типа «Эдельвейс - МП».
9. Устройство защиты аналоговых АТС «Гранит».
10. Устройство защиты цифровых АТС «МП-1Ц».
11. Генератор вибро-акустического шума типа «Соната-АВ-1М».
12. Ручной измеритель частоты и мощности типа «РИЧ-8».
13. Аудио-излучатель типа «Соната-АВ-АИ-65».
14. Вибро-излучатель типа «Соната-АВ-ВИ-45».
15. Универсальный генератор шума типа «Гром-ЗИ-4».
16. Подавитель диктофонов типа «ЛГШ-104».
17. Генератор вибро-акустического шума ЛГШ-401.
18. Генератор радиопомех типа «ЛГШ-501».
19. Пьезо-излучатель типа «Соната-АВ-ПИ-45».
20. Антенна логопериодическая типа «ЕЛВ-26».
21. Сканирующий приемник типа AR-8200.
22. Нелинейный локатор типа «Лорнет».

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
**федеральное государственное автономное образовательное учреждение высшего
образования «Балтийский федеральный университет имени Иммануила Канта»**
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

«Производственная преддипломная практика»

Шифр: 10.05.01

Специальность: «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Квалификация (степень) выпускника: Специалист по защите информации

Калининград

2022 г.

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНи-ИТ, к. ф.-м. н., доцент

Шпилевой А. А

Ведущий менеджер

Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.
3. Место практики в структуре образовательной программы.
4. Содержание практики.
5. Сведения о местах проведения практики
6. Указание форм отчетности по практике.
7. Фонд оценочных средств
8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения практики.
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики
10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для проведения практики.

1. Указание вида практики, способа (при наличии) и формы (форм) ее проведения.

Вид практики: Производственная преддипломная практика (далее **преддипломная практика** или **практика**).

Преддипломная практика проводится в следующих **формах**:

- непрерывная – в период учебного времени для проведения практики, указанного в календарном учебном графике.

Способы проведения преддипломной практики:

- стационарная на рабочем месте (в компании, с которой заключен договор на прохождение преддипломной практики).

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Целью преддипломной практики является углубление профессиональных знаний и адаптация их к условиям конкретного производства, закрепление профессиональных компетенций, приобретение дополнительного опыта практической работы, сбор и обработка материала для написания ВКР.

Код компетенции	Результаты освоения образовательной программы (ИДК)	Перечень планируемых результатов
ОПК-2: Способен применять программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.	<ul style="list-style-type: none">– знать: современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности– уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности;– владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.
ОПК-3: Способен на основании со-	ОПК-3.1. Знает необходимые математические	– знать: необходимые математические методы для решения задач обеспечения защиты информа-

<p>вокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p>	<p>методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.</p>	<p>ции;</p> <ul style="list-style-type: none"> - уметь: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; - владеть: разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации
<p>ОПК – 7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования</p>	<p>ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня. ОПК-7.1. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.1. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.</p>	<ul style="list-style-type: none"> - знать: методику разработки программ на языках высокого и низкого уровня - уметь: применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач - владеть: обоснованным выбором инструментария программирования и способов организации программ.
<p>ОПК – 12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения</p>	<p>ОПК-12.1. Знает принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения ОПК-12.2. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения ОПК-12.3. Владеет навыками администрирования операционных систем и восстановления работоспособности прикладного и системного программного обеспечения ОПК-13.1. Знает принципы функционирования</p>	<ul style="list-style-type: none"> - знать: принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения - уметь: администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения - владеть: навыками администрирования операционных систем и восстановления работоспособности прикладного и системного программного обеспечения

	<p>программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.</p>	
<p>ОПК – 13: Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности</p>	<p>ОПК-13.2. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах</p> <p>ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах</p>	<ul style="list-style-type: none"> – знать: принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности. – уметь: разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах – владеть: способами анализа безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах
<p>ОПК-15: Способен администрировать компьютерные сети и контролировать корректность их функционирования</p>	<p>ОПК-15.1. Знает устройство, порядок администрирования и контроля функционирования компьютерных сетей.</p> <p>ОПК-15.2. Умеет осуществлять администрирование и контроль корректности функционирования компьютерных сетей.</p> <p>ОПК-15.3. Владеет навыками администрирования и контроля функционирования компьютерных сетей</p>	<ul style="list-style-type: none"> – знать: устройство, порядок администрирования и контроля функционирования компьютерных сетей – уметь: осуществлять администрирование и контроль корректности функционирования компьютерных сетей. – владеть: навыками администрирования и контроля функционирования компьютерных сетей
<p>ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>	<p>ОПК-16.1. Знает устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.</p> <p>ОПК-16.2. Умеет осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.</p> <p>ОПК-16.3. Владеет навы-</p>	<ul style="list-style-type: none"> – знать: устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях – уметь: осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях – владеть: навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях

	ками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.	
--	---	--

3. Место практики в структуре образовательной программы

Преддипломная практика относится к обязательной части блока 2 «Практики» ОПОП подготовки специалистов по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Содержание практики

Студенты-практиканты выполняют программу практики в соответствии с планом-графиком практики, утверждаемым руководством базового предприятия и представителями ОНК «Института высоких технологий» БФУ им. И. Канта.

Ведется дневник практики и составляется заключительный отчет, который защищается после окончания практики и утверждается руководителями практики со стороны базового предприятия и института. В зависимости от специализации базового подразделения, в котором студент проходит практику, осуществляется корректировка направления его деятельности.

Студентам-практикантам должна быть предоставлена возможность ознакомиться с научно-технической документацией и научной литературой, которая касается предмета его исследований. В процессе прохождения практики студенты прослушивают лекции ведущих специалистов базовых предприятий, участвуют в научно-технических семинарах и конференциях при их наличии.

Студенты-практиканты проходят практику в отделах компьютерной безопасности, информационной и технической безопасности, компьютерных лабораториях, в которых работают их руководители и сотрудники подразделений. Они должны иметь доступ к программно-техническим комплексам, программным комплексам, математическому обеспечению и техническим средствам, необходимым для исследований, иметь возможность непосредственных консультаций во время работы со специалистами подразделений. Практиканты ежедневно работают в течение 3-4 часов в отделах предприятия. Объем теоретических занятий и семинаров определяется спецификой базового предприятия.

При прохождении преддипломной практики студенты изучают:

- административную и информационную структуру предприятия;
- основные нормативно-правовые положения в области информационной безопасности и защиты информации, на основании которых обеспечивается информационная безопасность предприятия;
- должностные инструкции сотрудников организации, отвечающих за безопасность;
- применяемые аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;

- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, используемых на предприятии;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности, современную технологию анализа потенциальных каналов утечки информации;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия, современную технологию противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
- криптографические средства, стандарты в области криптографической защиты информации и криптографическую инфраструктуру, используемые на предприятии;
- математические модели и алгоритмы, используемые в современных криптографических системах и системах помехоустойчивого кодирования
- структуру и методы построения современных моделей безопасности компьютерных систем;
- передовой опыт лучших специалистов подразделения;
- менеджмент в области программно-аппаратных и технических средств защиты информации.

При прохождении преддипломной практики студенты разрабатывают и исследуют:

- методы организации и управления деятельности служб защиты информации на предприятии;
- технологию проектирования, построения и эксплуатации систем и подсистем компьютерной безопасности;
- методы анализа уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- методы и схемы управления информационной безопасностью;
- системы и алгоритмы шифрования информации, их свойства, оценки эффективности и их компьютерные модели;
- математические методы, модели и алгоритмы, используемые при разработке инфраструктуры современных криптосистем с открытым ключом, и их компьютерные модели;
- математические и компьютерные модели псевдослучайных генераторов, их свойства и методы статистического тестирования;
- системы и алгоритмы помехоустойчивого кодирования информации, их свойства, оценки эффективности и их компьютерные модели;
- структуру, принципы функционирования и управления современными системами защиты информации в компьютерных системах
- методы оценки экономической эффективности применения программно-аппаратных и технических средств защиты информации.

При прохождении преддипломной практики возможен следующий перечень индивидуальных заданий:

- На основе стандартов в области информационной безопасности, нормативных документов и с помощью программно-аппаратных средств контроля вторжений произведе-

сти анализ и оценку уровня информационной защищённости предприятия или его компьютерной системы.

- Разработать математические модели защищаемых информационных процессов, исследовать их свойства и приложения для создания средств защиты информации и систем, обеспечивающих информационную безопасность объектов.
- Обосновать и выбрать рациональное решение по уровню обеспечения информационной безопасности предприятия с учетом заданных требований и стандартов информационной безопасности; разработать и обосновать рекомендации по совершенствованию существующей системы информационной безопасности предприятия или его компьютерной системы.
- Разработать модификацию системы информационной безопасности предприятия или его компьютерной системы, или адаптировать существующую для обеспечения требуемого уровня безопасности; разработать необходимое программное обеспечение для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
- Принять участие в разработке технических заданий на проектирование, разработку эскизных, технических и рабочих проектов систем и подсистем защиты информации, с учетом действующих нормативных и методических документов; подробно описать методику и этапы разработки технического задания.
- Принять участие в разработке проектов систем и подсистем управления информационной безопасностью предприятия в соответствии с техническим заданием; подробно описать методику и этапы проектирования.
- Принять участие в экспериментально-исследовательских работах по сертификации средств защиты информации и анализу результатов; подробно описать методику сертификации и порядок проведения соответствующих работ.
- Осуществить сбор и первичную обработку материала для подготовки к написанию выпускной квалификационной работы; разработать и исследовать математические модели, провести компьютерные эксперименты по теме ВКР.

Задание на практику определяется вместе со студентом руководителями практики со стороны института и предприятия в начале практики. В конце практики студент должен представить результаты практики в виде отчета и сдать его руководителю от института. Руководитель практики от института организует защиту отчетов, по результатам которой на основании решения комиссии выставляется промежуточный контроль в виде зачета с оценкой.

Кроме того, при прохождении преддипломной практики на предприятии, учреждении, организации, студент обязан:

- пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, правилами внутреннего трудового распорядка;
- посещать все мероприятия по месту практики;
- подчиняться действующим на предприятии, в учреждении, организации правилам внутреннего трудового распорядка;
- изучить и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии.

Особое внимание следует уделить внедрению результатов, полученных практикантом, по месту практики, а также анализу возможности применения и / или внедрения в производство предполагаемых результатов исследований по теме ВКР.

Содержание преддипломной практики

№ п/п	Этапы (периоды) практики	Вид работ	Форма те- кущего кон- троля
1	Подгото- вительный этап	<ol style="list-style-type: none"> 1. Определение базы прохождения практики. 2. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 3. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 4. Ознакомление с правилами внутреннего распорядка на базе прохождения практики. 5. Получение и согласование индивидуального задания по прохождению практики. 6. Разработка и утверждение индивидуальной программы практики и графика выполнения исследования. 7. Получение документации по практике (программы практики, индивидуального задания на практику, плана-графика прохождения практики и дневника практики с направлением на практику) в сроки, определенные программой. 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики. 	Письменный отчёт. Индивиду- альное зада- ние на прак- тику.
2	Производ- ственный этап	<ol style="list-style-type: none"> 1. Выполнение производственных заданий. <ul style="list-style-type: none"> • Ознакомление с конкретными видами деятельности в соответствии с положениями структурных подразделений и должностными инструкциями. • Ознакомление с задачами отдела/службы организации базы практики. • Сбор информации и материалов в соответствии с заданием на практику. • Выполнение заданий, поставленных руководителями практики. • Обработка, систематизация и анализ фактического и теоретического материала. 2. Подготовка материалов для ВКР: <ul style="list-style-type: none"> • разработка и исследование математических моделей процессов и объектов, возникающих в системах компьютерной безопасности; • разработка и анализ эффективности вычислительных алгоритмов, реализующих процессы обработки информации в компьютерных системах; • проведение компьютерных экспериментов, демонстрирующих работоспособность компьютерных программ, и получение статистических оценок эффективности разработанных моделей и алгоритмов. 	Письменный отчет. Дневник практики

№ п/п	Этапы (периоды) практики	Вид работ	Форма текущего контроля
		3. Введение дневника практики.	
3	Заключительный этап	1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию существующего порядка работы, а также по внедрению новых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практике и прилагаемых документов для защиты.	Зачет с оценкой.

5. Сведения о местах проведения практики

Практика проводится:

- непосредственно в образовательной организации, в том числе в ее структурном подразделении, предназначенном для проведения практической подготовки;
- в организации, осуществляющей деятельность по профилю образовательной программы, в том числе ее структурном подразделении, предназначенном для проведения практической подготовки, на основании договора.

Для обучающихся с ограниченными возможностями здоровья и инвалидов практика планируется и организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Примеры организаций, с которыми заключены договоры о практической подготовке обучающихся.

1.	ООО «Центр Защиты Информации»
2.	ГАУ КО «КГНИЦ»
3.	АО «Янтарьэнерго»
4.	ООО «Алгоритм»
5.	АО «ЦентрИнформ»
6.	ООО «СКА и К»
7.	ООО «Сократ»
8.	АО «33 судоремонтный завод»
9.	“Elite Games Limited”
10.	ООО «Альпея»
11.	ООО «Е-Легион»
12.	ФГБК «Федеральный центр высоких медицинских технологий» Министерства здравоохранения Российской Федерации
13.	ООО «Хирокрафт»

6. Указание форм отчетности по практике

Формой отчетности по практике является:

1. Дневник практики;
2. Отчет по практике с приложениями;

Указанные документы представляются руководителю практики.

Дневник практики.

С момента прибытия и до конца пребывания на практике студент обязан вести «Дневник прохождения производственной практики», который является составной частью отчета о практике и используется при его написании. Записи в дневнике должны быть ежедневными. В дневнике фиксируются следующие виды работ: виды работ, их объем, краткое содержание, затраченное время, обработка данных, их анализ, краткие выводы в соответствии с тематикой ВКР.

В дневнике необходимо также отразить встретившиеся в работе затруднения, их характер, какие меры были приняты для их устранения, отметить недостатки в теоретической подготовке. Дневники периодически проверяются руководителем практики, в нем делаются отметки по его ведению, качеству выполняемой студентом работы. В дневнике руководитель практики дает отзыв о прохождении обучающимся практики (выполнении программы практики, отношении к порученной работе, собранных материалов) и выставляет оценку практики.

Отзыв руководителя практики от университета должен отражать основные структурные элементы: степень реализации плана практики; грамотность и полнота изложения материала в отчете; уровень самостоятельности выполнения работы; недостатки и замечания, выявленные как в процессе практики, так и в представленном отчете; положительные стороны, выявленные как в процессе практики, так и в представленном отчете; общий вывод об отчете с заключением о проделанной работе.

Отзыв руководителя практики от профильной организации, на базе которой студент проходил практику, должен отражать: краткую характеристику предоставленной информации, с которой работал обучающийся; методы и технологии, уровень самостоятельности, степень ответственности, добросовестности при выполнении работы; недостатки и замечания, выявленные в процессе прохождения практики; положительные стороны, выявленные в процессе прохождения практики; общий вывод об отчете с заключением о проделанной работе.

Отчет о практике составляется индивидуально каждым студентом в соответствии с методическими рекомендациями по прохождению практики и должен отражать его деятельность в период практики. В отчете следует отразить все вопросы, изученные во время прохождения практики, представить аналитические результаты анализа, выводы и рекомендации. Отчет о практике должен состоять из титульного листа, содержания, введения, основной части, заключения, списка литературы (при необходимости) и приложений (при необходимости). В заключении обобщаются результаты проделанной работы и делаются выводы и рекомендации. В конце отчета приводится список литературы и нормативных материалов, а также материалы приложений (графики, таблицы и т.д.).

Отчетная документация по практике (с приложениями) предоставляется в институт/школу не позднее 5 дней по окончании практики. Если практика проходит летом или в конце учебного семестра, то не позднее последнего рабочего (учебного) дня практики. За обучающихся заочной формы обучения отчетная документация предоставляется в период экзаменационной сессии (не позднее последнего учебного дня) соответствующего семестра.

Формы отчетности руководителей практики:

- руководитель практики от института не позднее 1 месяца после окончания практики предоставляет в институт отчет о проведенной преддипломной практике;
- руководитель практики от организации предоставляет отзыв о работе каждого студента-практиканта на практике.

7. Фонд оценочных средств

Текущий контроль осуществляется руководителем практики от базовой организации в дискретные временные интервалы с использованием следующих оценочных средств:

- выполнение индивидуального задания согласно плану-графику,
- оценивает каждый этап выполнения в дневнике практики.

Промежуточная аттестация производится в форме зачета с оценкой с использованием следующих оценочных средств:

- индивидуальное задание на практику, заверенное руководителями практики от института и организации;
- план-график прохождения практики, заверенный руководителями практики от института и организации;
- дневник практики, заверенный руководителем практики от организации;
- контрольные вопросы к дифференцируемому зачету;
- отзыв руководителя практики от предприятия;
- отчет студента о прохождении практики.

Примерные контрольные вопросы к дифференцированному зачету по преддипломной практике:

1. Какие нормативные документы по охране труда, технике безопасности и пожарной безопасности вам были предоставлены для изучения?
2. В чем заключались Ваши права и обязанности в соответствии с должностной инструкцией?
3. Какие нормативные документы для составления отчетности используются на предприятии?
4. Суть порученных Вам производственных задач.
5. Какие методы, технологии были предложены вами для решения поставленных производственных задач?
6. Какие информационные системы/технологии используются на предприятии?
7. Описать административную и информационную структуру предприятия.
8. Описать цели и задачи, решаемые предприятием, направление деятельности предприятия.
9. Описать используемые на предприятии технические и программные средства вычислительной техники.
10. Описать организацию информационных систем с точки зрения информационной защищенности и защиты государственной тайны.
11. Описать технические устройства хранения, обработки и передачи информации, используемые на предприятии.
12. Представить анализ потенциальных каналов утечки информации и уязвимостей информационных процессов.
13. Описать схему инженерно-технической защиты информации.
14. Описать используемые методы и средства противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

15. Представить перечень правовых положений в области информационной безопасности и защиты информации, регламентирующих уровень защищённости базового предприятия.
16. Описать проведённые экспериментально-исследовательские работы по сертификации средств защиты информации и анализ их результатов.
17. Представить и обосновать рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы.
18. Представить эскизный проект модификации системы информационной безопасности предприятия или его компьютерной системы.
19. Описать структуру и функции разработанного программного обеспечения для модифицированной системы информационной безопасности предприятия или его компьютерной системы.
20. Каковы выводы и предложения по внедрению рекомендаций по совершенствованию системы информационной безопасности на предприятии?
21. Какие работы проводились в рамках подготовки ВКР?
22. Какие математические модели были исследованы с целью подготовки ВКР? Каковы результаты исследований?
23. Какие материалы для прикладной части ВКР удалось собрать? Какие – не удалось?
24. Как соотносятся работы, выполненные на предприятии, с ВКР?

При проведении зачета используются следующие критерии итоговой оценки за преддипломную практику:

- полный и аккуратно оформленный в соответствии с требованиями отчет;
- глубокое и всестороннее знание существующей системы, методов и средств обеспечения информационной безопасности, применяемых на предприятии; знание основных документов, регламентирующих функционирование системы информационной безопасности на предприятии;
- грамотная оценка уровня информационной защищённости предприятия и его компьютерной системы;
- наличие разработанного и успешно протестированного программного продукта, реализующего безопасность отдельных компонент компьютерной системы предприятия, либо
- развёрнутые рекомендации по совершенствованию системы информационной безопасности предприятия или его компьютерной системы, либо
- наличие эскизного проекта модификации соответствующей системы информационной безопасности предприятия или его компьютерной системы;
- наличие всей необходимой для написания ВКР информации в соответствии с заданием на ВКР;
- правильные ответы студента на вопросы преподавателя, касающиеся предмета практики.

При оценке результатов практики принимается во внимание:

- соответствие отчета заданию на практику;
- степень полноты выполненных задач, достижения цели практики;
- соблюдение графика прохождения практики;

- характеристика на обучающегося, составленная руководителем практики от профильной организации;
- оформление отчета по практике;
- содержательность доклада, аргументированность и полнота ответов на вопросы при защите результатов практики.

Зачёт по практике (в виде защиты отчёта) принимает комиссия.

Во время защиты обучающийся должен подтвердить уровень образовательных результатов практики в соответствии с требованиями, определенными программой практики.

При оценке итогов практики обучающегося принимается во внимание отзыв руководителя практики от профильной организации

По результатам защиты студенту выставляется зачет с оценкой.

Уровни	Содержательно е описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалль ная шкала (академиче ская) оценка	БРС, % освоения (рейтингов ая оценка)
Повышен ный	Творческая деятельность	<i>Включает нижестоящий уровень.</i> Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональ ной деятельности, нежели по образцу с большой степени самостоятельно сти и	<i>Включает нижестоящий уровень.</i> Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо	71-85

	инициативы			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно	55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	Менее 55

8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики

8.1. Основная литература

1. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета) №1459. утвержден 26 ноября 2020 г.
2. Приказ Минобрнауки России от 27.11.2015 №1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования» (зарегистрировано в Минюсте России 18.12.2015 №40168);
3. Положение о практической подготовке обучающихся в федеральном государственном автономном образовательном учреждении высшего образования «Балтийский федеральный университет имени Иммануила Канта (принято решением ученого совета БФУ им. И. Канта 23 декабря 2021 года, протокол №2).

8.2. Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информац. потоками: Учебное пособие для вузов/П.Н.Девянин-2-е изд., испр. и доп.- Москва :Гор.линия-Телеком,2013-338с.:ил.;. - (Специальность). ISBN 978-5-9912-0328-9, 100 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/436878> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Москва :Гор. линия-Телеком, 2013. - 214 с.: . - (Вопросы управления информационной безопасностью)ISBN 978-5-9912-0274-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/560783> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Костин, В. Н. Методы и средства защиты компьютерной информации: законодательные и нормативные акты по защите информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2017. - 26 с. - ISBN 978-5-906846-87-7. - Текст :

- электронный. - URL: <https://znanium.com/catalog/product/1232204> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
4. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Гор. линия-Телеком, 2012. - 184 с.: ил.; . ISBN 978-5-9912-0246-6, 500 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/367555> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 5. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1167736> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 6. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1210523> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 7. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189326> (дата обращения: 13.01.2022). – Режим доступа: по подписке.
 8. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1178150> (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для выполнения НИР

1. НЭБ Национальная электронная библиотека, диссертации и прочие издания
2. eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
3. Гребенников Электронная библиотека ИД журналы
4. ЭБС Лань книги, журналы
5. ЭБС Консультант студента
6. ПРОСПЕКТ ЭБС
7. ЭБС ZNANIUM.COM
8. РГБ Информационное обслуживание по МБА
9. БЕН РАН
10. Электронно-библиотечная система (ЭБС) Кантитана (<https://elib.kantiana.ru/>)
11. http://lib.mexmat.ru/catalogue.php?dir=02_06 - Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография

12. http://booklid.org/g/mt_number+theory - Библиотека научной литературы. Раздел «Теория чисел».
13. <https://www.coursehero.com/file/p7t1rf7/External-links-Certicom-ECC-Tutorial-http-www-certicom-com-index-php-ecc/> - Online Elliptic Curve Cryptography Tutorial, Certicom Corp.
14. [MathWorld](http://mathworld.wolfram.com/). – математический сайт, созданный *Weisstein, Eric W.* (англ.).
15. <http://mathworld.wolfram.com/> - сайт по эллиптическим кривым.
16. <http://mathemlib.ru/> - библиотека по математике.
17. <http://www.math.uiuc.edu/~r-ash/ANT.html> - курс по алгебраической теории чисел Robert B. Ash.
18. <http://www1.spms.ntu.edu.sg/~frederique/Teaching.html> - электронные курсы лекций: алгебра, алгебраическая теория чисел, дискретная математика, группы и симметрии.
19. <http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf> - Лекции по алгебраической теории чисел F.Oggier.
20. <http://www.math.wisc.edu/~mmwood/748Fall2014/weston.pdf> - лекции по алгебраической теории чисел Tom Weston.
21. <http://www2.warwick.ac.uk/fac/sci/math/undergrad/ughandbook/year3/ma3a6/> - электронные лекции по алгебраической теории чисел университета Warwick.
22. <http://arxiv.org/list/math.AG/recent> - архив новых публикаций по алгебраической геометрии.
23. <http://www.jmilne.org/math/CourseNotes/ag.html> - веб-сайт J.Miln'a с публикациями по алгебраической геометрии.
24. <http://www.fen.bilkent.edu.tr/~franz/LN/LN-algeo.html> - собрание лекций по алгебраической геометрии.
25. http://www.math.utah.edu/~yplee/teaching/LN_ag.html - собрание лекций по алгебраической геометрии.
26. <http://www.math.byu.edu/~jarvis/alg-geom.html> - информация о веб-сайтах по алгебраической геометрии.
27. <http://ocw.mit.edu/courses/mathematics/18-726-algebraic-geometry-spring-2009/lecture-notes/> - открытый курс лекций по алгебраической геометрии.
28. <http://www.freebookcentre.net/Mathematics/Algebraic-Geometry-Books.html> - лекции по алгебраической геометрии в свободном доступе.

10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе практики используются информационные технологии:

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;

- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

Перечень программного обеспечения (используемое при необходимости)

- Программа для ЭВМ Wolfram Mathematica 10.2 Education Bundled Price (Количество лицензий – 3, Номер акта / накладной – Тг053766, Дата акта – 02.11.15);
- IBM SPSS Statistics Base Campus Edition (Количество лицензий – 25, Номер акта / накладной – Тг031923, Дата акта – 10.06.15);
- Intel Cluster Studio for Linux (Количество лицензий – 2, Номер акта / накладной – Тг072207, Дата акта – 16.12.11);
- Maple 11 (Количество лицензий – 30, Номер акта / накладной – Тг068983, Дата акта – 19.12.07);
- Mathematica (Количество лицензий – 15, Номер акта / накладной – Тг066706, Дата акта – 18.11.13);
- Mathworks Gauges Blockset Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Тг072207, Дата акта – 16.12.11);
- Mathworks Simulink 3d animation Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Тг072207, Дата акта – 16.12.11);
- Microsoft SQL Srv Standard Core 2014 (Количество лицензий – 4, Номер акта / накладной – Тг063168, Дата акта – 24.11.14);
- Microsoft Visio Professional 2010 (Количество лицензий – 25, Номер акта / накладной – Тг070182, Дата акта – 15.12.11);
- Microsoft Visual Studio 2005 (Количество лицензий – 30, Номер акта / накладной – Тг063374, Дата акта – 19.12.07).
- Parallel Computing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Тг072207, Дата акта – 16.12.11);
- Signal Processing Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Тг072207, Дата акта – 16.12.11);
- Statistica Base (Количество лицензий – 20, Номер акта / накладной – Тг063374, Дата акта – 19.12.07).
- Statistics Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Тг072207, Дата акта – 16.12.11);
- System Identification Toolbox Academic new Product Individual License (per License) (Количество лицензий – 5, Номер акта / накладной – Тг072207, Дата акта – 16.12.11).

11. Описание материально-технической базы, необходимой для проведения практики

Для проведения отчетной конференции используются аудитории института/ школы; занятия проводятся с применением компьютера и видеопроектора. На всех компьютерах установлено необходимое программное обеспечение, требуемое в учебном процессе. Обра-

зовательная организация обеспечена необходимым комплектом лицензионного программного обеспечения, подлежащего ежегодному обновлению. Типовое программное обеспечение: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

При реализации практики в профильной организации на основании договора о практической подготовке обучающихся в качестве материально-технического обеспечения практики используется материальное оснащение профильной организации.

14.	ООО «Центр Защиты Информации»
15.	ГАУ КО «КГНИЦ»
16.	АО «Янтарьэнерго»
17.	ООО «Алгоритм»
18.	АО «ЦентрИнформ»
19.	ООО «СКА и К»
20.	ООО «Сократ»
21.	АО «33 судоремонтный завод»
22.	“Elite Games Limited”
23.	ООО «Альпея»
24.	ООО «Е-Легион»
25.	ФГБК «Федеральный центр высоких медицинских технологий» Министерства здравоохранения Российской Федерации
26.	ООО «Хирокрафт»

12. Методические рекомендации по прохождению практики

Этапы деятельности	Содержание деятельности	
	Преподаватель	Студент
Подготовка: определение цели и задач задания	Мотивирует, помогает обучающемуся в постановке задач	Определяет и обсуждает с преподавателем актуальность проблемы; выдвигает совместно с преподавателем гипотезу исследования
Планирование: определение источников, способов сбора, анализа информации, способов представления результатов, установление критериев оценки результата и процесса	Корректирует в случае необходимости деятельность обучающегося, предлагает идеи, высказывает предположения	Формулирует задачи и разрабатывает план действий; обсуждает с преподавателем методы исследования
Сбор информации: наблюдение, работа со справочной литературой, нормативно-правовой, учебной, научной и др. литературы	Наблюдает за деятельностью обучающегося, косвенно руководит его исследовательской деятельностью	Собирает и систематизирует информацию
Анализ информации: формулирование выводов	Корректирует деятельность обучающегося, наблюдает,	Анализирует собранную информацию

	советует	
Оформление работы: подготовка и представление результатов	Консультирует в оформлении документов по практике	Оформляет конечные результаты
Представление задания	Оценивает результаты исследования по заранее установленным критериям	Представляет результаты по заданию в форме письменного отчета и его устной защиты
Подведение итогов: рефлексия, оценка	Оценивает усилия, использованные и неиспользованные возможности, творческий подход студента	Участвует в коллективном обсуждении итогов практики

При выборе базы практики целесообразно использовать оптимальное количество объективных критериев, оценивающих наиболее важные стороны организации или структурного подразделения университета как базы практики. К таким критериям относятся:

- соответствие профиля организации направлению обучения;
- обеспечение квалифицированными кадрами;
- оснащенность организации современным оборудованием и технологиями;
- наличие возможности дальнейшего трудоустройства и др.

Условия проведения практики в сторонних организациях регламентируются договорами о практической подготовке.