

**МИНОБРНАУКИ РОССИИ**  
**Ярославский государственный университет им. П.Г. Демидова**

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

**Рабочая программа производственной практики**  
**«Преддипломная практика»**

Направление подготовки (специальности)  
10.05.01 Компьютерная безопасность

Направленность (профиль)  
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2023 г.

## 1. Способ и формы практической подготовки при проведении практики

Организация, способ и форма проведения практики определяется положением "О проведении практики как компонента образовательной программы, реализуемого в форме практической подготовки, для студентов, осваивающих образовательные программы высшего образования", утвержденного приказом ректора ФГБОУ ВО ЯрГУ им. П.Г. Демидова от 25.02.2021 г. № 149. Данное положение распространяется на образовательные программы (далее - ОП) высшего образования – программы бакалавриата, специалитета, магистратуры и программы подготовки кадров высшей квалификации, – реализуемые в соответствии с федеральными государственными образовательными стандартами высшего образования, и на все формы получения высшего образования, включая очную, очно-заочную и заочную. Данная учебная практика строится на основании ФГОС ВО № 1459 от 26.11.2020 г. на специальность 10.05.01 «Компьютерная безопасность», по профилю «Математические методы защиты информации».

**Вид практики** - производственная практика.

**Тип практики** – преддипломная практика.

**Способ проведения практики** - стационарная.

**Место проведения практики:** практика проводится в структурных подразделениях ЯрГУ либо в профильных организациях, расположенных на территории города Ярославля.

## 2. Место практики в структуре образовательной программы

Преддипломная практика относится к базовой части образовательной программы. В течение преддипломной практики студенты применяют знания и умения, полученные при изучении профессиональных дисциплин ООП. В ходе преддипломной практики закрепляется и завершается формирование у обучающихся универсальных, общепрофессиональных и профессиональных компетенций. В период преддипломной практики студент набирает теоретический и практический материал, который может быть использован при выполнении ВКР, в т.ч. сведения о производственной деятельности организации, являющейся базой практики, проводит эксперимент по избранной теме. Практика должна подтвердить, что студент умеет организовать свой труд, владеет необходимыми методами сбора, хранения, обработки информации, применяемых в сфере его профессиональной деятельности; а также является грамотным специалистом в области защиты информации и способен успешно работать по выбранному направлению.

## 3. Планируемые результаты обучения при прохождении учебной (ознакомительной, стационарной) практики, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
<b>Общекультурные компетенции</b>	
<b>ОК-8</b> Обладает способностью к самоорганизации и самообразованию	<b>Умеет:</b> - грамотно распределять время при решении профессиональных задач <b>Владеет навыками:</b> - самоорганизации

	- выстраивания траектории для самостоятельного развития в профессиональной области
<b>Профессиональные компетенции</b>	
<b>ПК-8</b> Обладает способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	<b>Знает:</b> - современные математические методы решения задач обеспечения защиты информации. <b>Умеет:</b> - применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. - осуществлять выбор современных математических методов защиты информации для решения задач профессиональной деятельности. <b>Владеет навыками:</b> - применения совокупности необходимых математических методов для решения задач обеспечения защиты информации. - разработки алгоритмов, реализующих современные математические методы защиты информации, используя современные программные комплексы.
<b>ПК-9</b> Обладает способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	<b>Знает:</b> - стандартные математические модели механизмов защиты информации и критерии их оценки. <b>Умеет:</b> - анализировать существующие модели, корректировать их в соответствии с практической задачей и разрабатывать новые математические модели механизмов защиты информации. <b>Владеет навыками:</b> - математического моделирования механизмов защиты информации и их применения для решения задач в профессиональной деятельности.
<b>ПК-12</b> Обладает способностью проводить инструментальный мониторинг защищенности компьютерных систем	<b>Знает:</b> - современные программные и программно-аппаратные средства защиты информации, в том числе отечественного производства, реализованные в них математические методы защиты информации и области их применения. <b>Умеет:</b> - проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации, в том числе отечественного производства, с учетом реализованных в них математических методов для решения задач профессиональной деятельности. <b>Владеет навыками:</b> - применения программных и программно-аппаратных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.
<b>ПК-13</b> Обладает способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	<b>Знать:</b> - понятия «группа» и «команда», их основные характеристики; - типологию групп в организациях; - основные социально-психологические закономерности взаимоотношений в группе (команде); - теорию, признаки, этапы и факторы развития команды; <b>Уметь:</b> - учитывать мнение и особенности партнера при работе в команде; - применять полученные знания на практике. - определять и реализовывать свою роль в команде, учитывая особенности поведения и общения разных людей в совместной деятельности; - планировать и организовывать командную работу; - устанавливать различные виды коммуникации для работы в команде;

	<b>Владеть:</b> - основными понятиями теории командообразования; - методами определения роли каждого члена команды. - навыками лидерского поведения; - навыками принятия эффективных командных решений для достижения поставленной цели; - соблюдением этических норм взаимодействия.
--	--

#### 4. Объем практики составляет 21 зачетную единицу, 14 недель

#### 5. Содержание практической подготовки при проведении практики

№ п/п	Тип(ы) практики, этапы прохождения практики	Формы отчетности
1	Установочная конференция	Отчет руководителя практики
2	Подготовительный этап	Отметки в дневниках практики студентов
3	Научно-исследовательский этап	Отметки в дневниках практики студентов
4	Этап выполнения исследовательских работ по индивидуальному плану	Отметки в дневниках практики студентов
5	Этап оформления отчёта по итогам практики	Отметки в дневниках практики студентов
6	Защита отчетов по результатам преддипломной практики комиссии на заседании кафедры КБ и ММОИ	Отметки в дневниках практики студентов
7	Итоговая конференция по преддипломной практике	Отметки в дневниках практики студентов

Содержание этапов практики:

##### 1. Установочная конференция

**2. Подготовительный этап:** инструктаж по общим вопросам; инструктаж по технике безопасности. Составление первоначального плана работ.

##### 3. Научно-исследовательский этап:

Выбор темы исследования. Определение проблемы, объекта и предмета исследования. Формулирование цели и задач исследования. Составление математической модели.

Анализ литературы и исследований по проблеме. Подбор специальных источников по теме (нормативно-правовые акты, рекомендации ФСТЭК и ФСБ России, базы данных уязвимостей, техническая документация, патентные материалы, научные отчеты, и др.). Составление библиографии. Корректировка плана работ.

Углубленное изучение вопросов информационной безопасности в соответствии с поставленной практической задачей, в том числе возможно изучение встроенных механизмов безопасности операционных систем (ОС) Windows и Linux; приобретение навыков администрирования ОС Windows и Linux; углубленное изучение Active Directory (AD), а также других программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов. Приобретение навыков настройки безопасной работы домена Windows.

##### 4. Этап выполнения исследовательских работ по индивидуальному плану

Проведение обзора существующих математических моделей и методов защиты информации, используемых для решения поставленной задачи. Сравнительный анализ математических моделей и методов защиты информации, выбор наиболее подходящей модели, ее

корректировка или разработка алгоритма, реализующего современные математические методы защиты информации, анализ результатов. Выбор программных и программно-аппаратных средств защиты информации, в том числе отечественного производства, с учетом реализованных в них математических методов для решения поставленной задачи.

Одной из задач задачей проектно-технологической практики является приобретение опыта в правильной с точки зрения безопасности настройке современных ОС и их сетевого взаимодействия. В рамках этой задачи могут выполнены такие работы: создание домена Windows из нескольких рабочих станций и контроллера домена, моделирующего сеть некоторой организации; создание учетных записей для работы на рабочих станциях, для администрирования рабочих станций, для контроллера домена; выполнение анализа защищенности домена: возможность получения прав локального администратора на рабочих станциях, возможность повышения привилегий на рабочих станциях и т. д.; проанализировать уязвимость к современным эксплоитам.

#### **5. Этап оформления отчёта по итогам практики**

Ведение дневника практики. Описание проделанной работы. Составление отчета по практике. Формулирование выводов и предложений по организации практики. Представление отчета и дневника практики.

#### **6. Защита отчетов по результатам проектно-технологической практики комиссии на заседании кафедры КБ и ММОИ**

Защита отчета.

#### **7. Итоговая конференция по проектно-технологической практике**

Выступление на конференции.

### **6. Фонд оценочных средств**

#### **6.1 Формы оценки по преддипломной практике**

По результатам прохождения практики проводится итоговая конференция, студенты готовят в произвольной форме краткие индивидуальные письменные отчеты о выполнении в ходе практики выбранных ими заданий, полученных при этом знаниях, умениях и навыках.

#### **6.2 Критерии оценивания результатов практики**

Отчеты о выполнении индивидуальных заданий защищаются студентами на комиссии кафедры КБ и ММОИ с постановкой им, при положительном решении комиссии, дифференцированного зачета по учебной практике.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения проектно-технологической практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

#### **Список вопросов и (или) заданий для проведения промежуточной аттестации**

На защите практики обучающемуся могут быть заданы в том числе следующие вопросы:

1. Кратко расскажите о использованной Вами методике эффективной организации работы. Обоснуйте ответ, приведите ссылки на первоисточники.
2. Кратко расскажите об основах тайм-менеджмента. Приведите ссылки на первоисточники.

3. Каким образом вы нашли необходимые для работы источники информации и нормативные правовые документы. Как проверяли их актуальность?
4. Кратко расскажите о принципах оформления рабочей технической документации с учетом действующих нормативных и методических документов по информационной безопасности.
5. Кратко расскажите о принципах организации работы малого коллектива исполнителей в профессиональной деятельности в сфере информационной безопасности.
6. Назовите несколько математических методов решения задач обеспечения защиты информации.
7. Укажите стандартные математические модели механизмов защиты информации и критерии их оценки.
8. Приведите номера и названия нескольких основных правовых нормативных документов в сфере информационной безопасности, регламентирующих разработку политики управления доступом.
9. Кратко расскажите о методах разработки политик управления доступом и информационными потоками, предусмотренных действующими правовыми нормативными документами в сфере информационной безопасности.
10. Кратко расскажите о методах разработки политик управления информационными потоками в компьютерных системах, предусмотренных действующими правовыми нормативными документами в сфере информационной безопасности.
11. Назовите некоторые современные программные и программно-аппаратные средства защиты информации, в том числе отечественного производства, и идеи реализованных в них математических методов защиты информации и области их применения.
12. Назовите критерии для сравнительного анализа и осуществления выбора программных и программно-аппаратных средств защиты информации, в том числе отечественного производства, для решения задач профессиональной деятельности.
13. Приведите номера и названия нескольких основных правовых нормативных документов в сфере информационной безопасности, регламентирующих проведение работ по администрированию средств защиты информации в компьютерных системах и сетях.
14. Кратко расскажите о порядке проведения работ по администрированию средств защиты информации в компьютерных системах и сетях, предусмотренном действующими правовыми нормативными документами в сфере информационной безопасности.
15. Приведите номера и названия нескольких основных правовых нормативных документов в сфере информационной безопасности, регламентирующих администрирование системного программного обеспечения в компьютерных системах и сетях.
16. Кратко расскажите о содержании работ по администрированию системного программного обеспечения в компьютерных системах и сетях, предусмотренных действующими правовыми нормативными документами в сфере информационной безопасности.
17. Кратко расскажите о методике оценивания уровня безопасности компьютерных систем и сетей, предусмотренной действующими правовыми нормативными документами в сфере информационной безопасности. Приведите номера и названия этих документов.
18. Кратко расскажите о методике проведения экспериментальных исследований компьютерных систем с целью выявления уязвимостей, предусмотренной действующими правовыми нормативными документами в сфере информационной безопасности. Приведите номера и названия этих документов.

### **Критерии выставления оценки**

#### **1. Оценка, рекомендуемая руководителем практики от организации.**

Оценка руководителя, учитывающая качество выполненного задания, является основным критерием. Тем не менее она может быть изменена в большую или меньшую сторону.

#### **2. Грамотное изложение отчета о проделанной работе в письменной и устной форме.**

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур, документы должны быть оформлены в соответствии с правилами, идентичными «Правилам оформления выпускной квалификационной работы в ФГБОУ ВО «Ярославский государственный университет им. П.Г. Демидова».

**3. Ответы студента на вопросы.**

**4. Наличие правильно оформленных документов в соответствии с «ЯрГУ-СК-П-217-2021 Положение о практике обучающихся».**

Отсутствие или грубые нарушения в оформлении документов (отсутствие печатей, подписей или содержательной части) могут быть основанием для выставления оценки «неудовлетворительно».

## **7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» для прохождения практики**

### **а) основная литература**

1. Торокин А. А. Инженерно-техническая защита информации: учеб. пособие для вузов. / А. А. Торокин; Учеб.-метод. совет по образованию в области информационной безопасности - М.: Гелиос АРВ, 2005. - 959 с.
2. О. В. Казарин, И. Б. Шубинский Надежность и безопасность программного обеспечения: учебное пособие для вузов — Москва: Издательство Юрайт, 2022. <https://urait.ru/viewer/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-493262>
3. Указ президента России от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности российской Федерации»  
<http://www.kremlin.ru/acts/bank/41460>
4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ.  
<http://www.kremlin.ru/acts/bank/42128>

### **б) дополнительная литература**

1. А. А. Молдовян, Д. Н. Молдовян, А. Б. Левина Протоколы аутентификации с нулевым разглашением секрета: учебное пособие — Санкт-Петербург: НИУ ИТМО, 2016. <https://books.ifmo.ru/file/pdf/1887.pdf>
2. Косолапов Ю. В. Протоколы защищенных вычислений на основе линейных схем разделения секрета: учебное пособие - Ростов н/Д: ЮФУ, 2020.  
<https://www.studentlibrary.ru/book/ISBN9785927533176.html>
3. ГОСТ Р ИСО/МЭК 56045-2014г., «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью». Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2015.  
<https://docs.cntd.ru/document/1200112882?ysclid=loecyk6d0x919888757>
4. ГОСТ Р ИСО/МЭК ТО 19791-2008г., «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. <https://docs.cntd.ru/document/1200076806>
5. ГОСТ Р ИСО/МЭК 27007-2014г., «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2015  
<https://docs.cntd.ru/document/1200112881>

6. ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. <https://docs.cntd.ru/document/1200068822>
7. ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2014. <https://docs.cntd.ru/document/1200105309>
8. ГОСТ Р ИСО/МЭК 53131-2008 «Защита информации. Рекомендации по услугам восстановления информации после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2011. <https://docs.cntd.ru/document/1200085087>
9. ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности», «Часть. 3. Компоненты доверия к безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», Часть 1.-2014.- <https://docs.cntd.ru/document/1200101777>  
Часть 2.-2014.- <https://docs.cntd.ru/document/1200105710>  
Часть 3.-2014.- <https://docs.cntd.ru/document/1200105711>
10. Информационный документ ФСТЭК России № 240/24/3095 от 20.03.2012г. «об утверждении Требований к средствам антивирусной защиты». ФСТЭК России, 2012. <https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-30-iyulya-2012-g-n-240-24-3095?ysclid=loed6c6lus546905797>
11. Руководящий документ ФСТЭК России (бывш. Гостехкомиссия) «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей». (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г., № 114).

**в) ресурсы сети «Интернет» (при необходимости)**

1. Сайт Федеральной службы технического и экспортного контроля Российской Федерации (<https://fstec.ru>) для знакомства с нормативными документами ФСТЭК России.
2. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. <https://www.securitylab.ru/>
3. База данных общеизвестных уязвимостей информационной безопасности <https://cve.mitre.org/>

**8. Образовательные технологии, в том числе электронное обучение и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса**

Обучающиеся перед прохождением преддипломной практики обеспечиваются программой прохождения практики и индивидуальным заданием руководителя практик.

Самостоятельная работа обучающихся подразумевает работу под руководством специалиста от организации – базы практики. Проводя собеседование, руководители обсуждают с обучающимися план будущей практики, формируют вопросы, которые



необходимо раскрыть при составлении отчета о практике, объясняют порядок заполнения дневника прохождения практики и подписывают его, дают рекомендации по изучению необходимого нормативного материала и соответствующей литературы. В дневнике прохождения производственной практики отражается краткое содержание работ, выполняемых обучающимся. Записи должны вноситься обучающимися ежедневно, отражая данные о проделанной работе, и заверяться подписью руководителя по месту прохождения практики.

В ходе прохождения практики обучающийся получает необходимые материалы от руководителя практики и из профессиональных баз данных и информационных справочных систем. В соответствии с описанными задачами обучающийся собирает и обрабатывает информацию для написания отчета.

По окончании практики обучающийся в установленные сроки сдает руководителю практики от факультета дневник и отчет о практике.

## **9. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса по дисциплине используются: для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- электронный университет Moodle ЯрГУ;
- Adobe Acrobat Reader.
- Nmap — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети. <https://nmap.org/>
- Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. <https://www.wireshark.org/>
- Metasploit Project — проект, посвященный информационной безопасности. <https://www.metasploit.com/>

## **10. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT» [http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента» <https://www.studentlibrary.ru>
- ГАРАНТ. Информационно-правовой портал

## **11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- все доступные ресурсы предприятия используются студентами во время проектно-технологической практики.

## **12. Иные сведения (материалы)**

### **Методические указания для студентов по освоению дисциплины**

Для успешного прохождения практики важно уметь эффективно организовать работу, сразу приступать к решению поставленных задач, постоянно знакомится с новыми источниками информации по теме.

Большое внимание следует уделить правилам техники безопасности, правилам внутреннего распорядка организации и ведению дневника.

Следует постоянно контролировать сроки выполнения поставленных задач.

В некоторых случаях возможна корректировка или изменение плана работ по согласованию с руководителем практики от организации.

При оформлении отчета и дневника не следует забывать о приложениях, куда прикладываются исходные коды разработанных, большие отчеты, полученные с помощью программных и программно-аппаратных средств защиты информации.

Чтобы успешно справиться с объемной работой по оформлению отчета о прохождении практики, следует оформлять отчет по частям, в процессе работы добавляя в него новые разделы и пункты с некоторыми логически завершенными частями исследования.

### **Автор(ы):**

Доцент кафедры КБ и ММОИ, к.ф.-м.н.

Федотова Н.П