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

«Эксплуатационная практика»

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем (в сфере информационных технологий)»

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.

Ярославль

1. Способ и формы проведения практики

Организация, способ и форма проведение 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 технологическая практика строится на основании ФГОС ВО № 1427 от 17.11.2020 г. на направление подготовки 10.03.01 «Информационная безопасность», по профилю «Безопасность компьютерных систем».

Вид практики - производственная практика.

Тип практики – эксплуатационная практика.

Способ проведения практики - стационарная.

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

Время проведения практики – 4 курс 8 семестр.

2. Место практики в структуре образовательной программы

Эксплуатационная практика относится к обязательной части образовательной программы. В течение эксплуатационной практики студенты применяют знания и умения, полученные при изучении профессиональных дисциплин ООП. Практика должна закрепить и развить полученные навыки администрирования ОС и сетей, а также познакомить студента с методами анализа защищенности как отдельных рабочих станций, так и компьютерных сетей. Подтвердить, что выпускник 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.

Задачи практики: систематизация, расширение, закрепление и углубление теоретических профессиональных знаний, полученных в результате изучения дисциплин направления и специальных дисциплин профильной программы подготовки.

Изучение современных программных и программно-аппаратных средств защиты информации (СЗИ), применяемых на объектах информатизации Российской Федерации.

Изучение и приобретение навыков установки, настройки и сопровождения аппаратно-программных модулей доверенной загрузки (АПМДЗ) Соболь и Dallas Lock.

Изучение и приобретение навыков установки, настройки и сопровождения виртуальной сети ViPNet: программное обеспечение (ПО) ViPNet Administrator, ViPNet Client. программно-аппаратный комплекс ViPNet Coordinator HW.

Изучение и приобретение навыков использования электронного идентификатора (токена) Рутокен. Изучение и приобретение навыков настройки сетевых экранов (МЭ) iptables, Windows Firewall, аппаратных межсетевых экранов.

Изучение и приобретение навыков установки, настройки и сопровождения средств защиты информации от несанкционированного доступа (СЗИ от НСД) Dallas Lock и Secret Net.

3. Планируемые результаты обучения при прохождении эксплуатационной практики, соотнесенные с планируемыми результатами освоения ОП по

направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата).

Процесс прохождение практики нацелен на формирование следующих элементов компетенций в соответствии с ФГОС ВО № 1427 от 17.11.2020 г. на направление подготовки 10.03.01 «Информационная безопасность, направленных на приобретение следующих знаний, умений, навыков и (или) опыта по профилю деятельности «Безопасность компьютерных систем»:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	**ИД-ОПК-10_6** Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	**Знает** основные проблемы обеспечения информационной безопасности на типовых объектах защиты, принципы обеспечения информационной безопасности объекта защиты в рамках комплексного подхода. **Умеет** выявлять проблемные места, ограничения конкретных решений в сфере информационной безопасности; грамотно указать на существующие проблемы и ограничения; предложить правильные решения существующих проблем и ограничений. Способен проводить анализ исходных данных для проектирования защищенной сети. **Владеет навыками** анализа исходных данных для проектирования корпоративной сети, подсистем и средств обеспечения информационной безопасности.

	ИД-ОПК-10_7 Способен разрабатывать политики безопасности, политики управления доступом информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.	**Знает** меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты. **Умеет** формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. **Владеет навыками**. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.	**ИД-ОПК-12_4** Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации.	**Знает** основные методы управления информационной безопасностью в современных ОС; особенности администрирования основных СЗИ. **Умеет** проводить анализ исходных данных для проектирования защищенной сети. Способен настраивать стандартные средства обеспечения информационной безопасности. **Владеет навыками** анализа исходных данных для проектирования корпоративной сети, подсистем и средств обеспечения информационной безопасности.

	ИД-ОПК-12_3 Умеет оценивать информационные риски в автоматизированных системах; умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;	**Знает** методы и средства контроля эффективности технической защиты информации. **Умеет** оценивать информационные риски в информационных системах. – проводить технико-экономическое обоснование стандартных проектных решений, связанных с обеспечением и управлением ИБ. **Владеет навыками** участия в разработке проектной и технической документации по информационной безопасности и проведении технико-экономического обоснования соответствующих проектных решений в области обеспечения и управления ИБ.

4. Объем практики составляет **3** зачетные единицы, **108** акад. часов.

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 простановкой 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

1. Семейство протоколов NTLM и проблемы с их безопасностью.
2. Стандартный протокол аутентификации в доменах Windows Kerberos. Аспекты безопасности.
3. Семейство протоколов доступа к сетевым ресурсам SMB.
4. Модель управления доступом в Linux. Процессы идентификации, аутентификации и авторизации субъектов доступа.
5. Модель управления доступом в Windows. Процессы идентификации, аутентификации и авторизации субъектов доступа.
6. Групповые политики Windows и их применение для повышения безопасности корпоративной сети.
7. Возможности брандмауэра Windows.
8. Возможности iptables.
9. Принцип работы, применение и защита от сетевого сканера nmap.
10. Основные подходы к анализу защищенности корпоративной сети
11. Семейство протоколов NTLM и проблемы с их безопасностью.
12. Стандартный протокол аутентификации в доменах Windows Kerberos. Аспекты безопасности.
13. Семейство протоколов доступа к сетевым ресурсам SMB.
14. Модель управления доступом в Linux. Процессы идентификации, аутентификации и авторизации субъектов доступа.
15. Модель управления доступом в Windows. Процессы идентификации, аутентификации и авторизации субъектов доступа.
16. Групповые политики Windows и их применение для повышения безопасности корпоративной сети.
17. Возможности брандмауэра Windows.
18. Возможности iptables.
19. Принцип работы, применение и защита от сетевого сканера nmap.
20. Основные подходы к анализу защищенности корпоративной сети

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. Рагозин, Ю. Н. Организация и управление подразделением защиты информации на предприятии : учебное пособие / Рагозин Ю. Н. , Мельник В. А. - Санкт-петербург : ИЦ Интермедия, 2019. - 240 с. - ISBN 978-5-4383-0180-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785438301806.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.
2. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных систем предприятий : учебное пособие / В. А. Сердюк. — Москва : Высшая школа экономики, 2011. — 572 с. — ISBN 978-5-7598-0698-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/66085 (дата обращения: 26.01.2022). — Режим доступа: для авториз. пользователей.
3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 26.01.2022).
4. Указ президента России от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности российской Федерации».
5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ.

б) дополнительная литература

1. Молдовян, А. А. Протоколы аутентификации с нулевым разглашением секрета : учебное пособие / А. А. Молдовян, Д. Н. Молдовян, А. Б. Левина. — Санкт-Петербург : НИУ ИТМО, 2016. — 55 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91498 (дата обращения: 26.01.2022). — Режим доступа: для авториз. пользователей.
2. Косолапов, Ю. В. Протоколы защищенных вычислений на основе линейных схем разделения секрета : учебное пособие / Ю. В. Косолапов. - Ростов н/Д : ЮФУ, 2020. - 112 с. - ISBN 978-5-9275-3317-6. - Текст : электронный // ЭБС "Консультант студента"

: [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785927533176.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.
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. - 44с.
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. - 126с.
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. - 27с.
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. - 46с.
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. - 250с.
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. - 48с.
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.-56с., Часть 2.-2014.-164с., Часть 3.-2014.-152с.
10. Информационной документ ФСТЭК России № 240/24/3095 от 20.03.2012г. «об утверждении Требований к средствам антивирусной защиты». ФСТЭК России, 2012.-3с.
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 эксплуатационной 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 вносится 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

1. Nmap — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети.
   https://nmap.org/
2. Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.
   https://www.wireshark.org/
3. Metasploit Project — проект, посвящённый 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)

1. Электронная библиотека учебных материалов ЯрГУ
   http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.
2. НЭБ Национальная электронная библиотека
   https://rusneb.ru/
3. Электронно-библиотечная система «Юрайт»
   https://www.urait.ru/
4. Электронно-библиотечная система «Лань»
   http://e.lanbook.com/
5. ГАРАНТ. Информационно-правовой портал (доступ с компьютеров университета. Собинова, 36а-Библиотека).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Все доступные ресурсы предприятия используются студентами во время преддипломной практики.

10. **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 КБиММОИ, к.ф.-м.н. Федотова Н.П