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

«Проектно-технологическая 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.

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 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 – проектно-технологическая практика.

Способ проведения практики **-** стационарная.

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

Время проведения практики – 5 курс 10 семестр.

2. Место практики в структуре образовательной программы

Целью проектно-технологической практики являются систематизация, расширение, закрепление и углублению профессиональных знаний, полученных в результате изучения дисциплин направления и специальных дисциплин профильной программы подготовки в области информационной безопасности и математических методов обработки и защиты информации.

Углубленное изучение встроенных механизмов безопасности операционных систем (ОС) Windows и Linux; приобретение навыков администрирования ОС Windows и Linux; углубленное изучение Active Directory (AD), приобретение навыков настройки безопасной работы домена Windows.

Овладение необходимыми профессиональными компетенциями и совершенствование навыков использования программных и программно-аппаратных средств защиты информации, в том числе отечественного производства, с учетом знания реализованных в них математических методов защиты информации и области применения.

Основной задачей технологической практики является приобретение опыта в правильной с точки зрения безопасности настройке современных ОС и их сетевого взаимодействия. Во время проектно-технологической практики студент должен:

изучить:

- права и привилегии пользователей, системные учетные записи, аудит, процессы идентификации, аутентификации и авторизации, User Account Control в ОС Windows;
- права пользователей, процессы идентификации, аутентификации и авторизации в ОС Linux;
- возможности Windows Firewall и iptables;
- протоколы NTLM, Kerberos, SMB;
- управление доменом Windows с помощью групповых политик.

выполнить:

- создать домен Windows из нескольких рабочих станций и контроллера домена, моделирующего сеть некоторой организации;
- создать учетные записи для работы на рабочих станциях, для администрирования рабочих станций, для контроллера домена;

– выполнить анализ защищенности домена: проанализировать возможность получения прав локального администратора на рабочих станциях, проверить возможность повышения привилегий на рабочих станциях и т. д.; проанализировать уязвимость к современным эксплоитам.

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.

Знания и навыки, полученные и закрепленные в результате прохождения производственной технологической практики, используются студентами при разработке курсовых и выпускных работ.

3. Планируемые результаты обучения при прохождении учебной (ознакомительной, стационарной) практики, соотнесенные с планируемыми результатами освоения ОП специалитета.

Процесс прохождение учебной (ознакомительной, стационарной) практики нацелен на формирование следующих элементов компетенций в соответствии с ФГОС ВО № 1459 от 26.11.2020 для специальности 10.05.01 «Компьютерная безопасность», направленных на приобретение следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-2.3 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов	**ИД-ОПК-2.2_1** Знает программные и программно-аппаратные средства защиты информации и математические принципы, лежащие в основе их работы.	**Знает** современные программные и программно-аппаратные средства защиты информации, в том числе отечественного производства, реализованные в них математические методы защиты информации и области их применения.
		Умеет 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. **Владеет навыками** аудита и организации мероприятий по защите информации.

	ИД-ОПК-2.2_2 Способен применять программные и программно-аппаратные средства защиты информации для решения задач профессиональной деятельности	**Знает** основные принципы настройки безопасной корпоративной сети; методы и средства контроля эффективности технической защиты информации; основные методы управления информационной безопасностью в современных ОС. **Умеет** выявлять проблемные места, ограничения конкретных решений в сфере информационной безопасности; грамотно указать на существующие проблемы и ограничения; предложить обоснованные выбор программных и программно-аппаратных средств защиты информации с учетом существующих проблем и ограничений. Способен – настраивать стандартные средства обеспечения информационной безопасности; проводить технико-экономическое обоснование стандартных проектных решений, связанных с обеспечением и управлением ИБ. **Владеет навыками** применения программных и программно-аппаратных средств, в том числе отечественного производства, для решения задач профессиональной деятельности. Владеет навыками настройки политики безопасности основных ОС; осуществления мер противодействия нарушениям сетевой безопасности.

4. Объем практики составляет 6 зачетных единиц, **216** 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 технологической 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.

Перечень типовых контрольных вопросов, задаваемых при защите отчета о прохождении производственной практики:

- Семейство протоколов NTLM и проблемы с их безопасностью.
- Стандартный протокол аутентификации в доменах Windows Kerberos. Аспекты безопасности.
- Семейство протоколов доступа к сетевым ресурсам SMB.
- Модель управления доступом в Linux. Процессы идентификации, аутентификации и авторизации субъектов доступа.
- Модель управления доступом в Windows. Процессы идентификации, аутентификации и авторизации субъектов доступа.

– Групповые политики Windows и их применение для повышения безопасности корпоративной сети.
– Возможности брандмауэра Windows.
– Возможности iptables.
– Принцип работы, применение и защита от сетевого сканера nmap.
– Основные подходы к анализу защищенности корпоративной сети.

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

1. Приведите номера и названия нескольких основных правовых нормативных документов в сфере информационной безопасности, регламентирующих разработку политики управления доступом.
2. Кратко расскажите о методах разработки политик управления доступом и информационными потоками, предусмотренных действующими правовыми нормативными документами в сфере информационной безопасности.
3. Кратко расскажите о методы разработки политик управления информационными потоками в компьютерных системах, предусмотренных действующими правовыми нормативными документами в сфере информационной безопасности.
4. 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.
5. 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.
6. Семейство протоколов NTLM и проблемы с их безопасностью.
7. Стандартный протокол аутентификации в доменах Windows Kerberos. Аспекты безопасности.
8. Семейство протоколов доступа к сетевым ресурсам SMB.
9. Расскажите кратко о модели управления доступом в Linux. Процессы идентификации, аутентификации и авторизации субъектов доступа.
10. Расскажите кратко о модели управления доступом в Windows. Процессы идентификации, аутентификации и авторизации субъектов доступа.
11. Групповые политики Windows и их применение для повышения безопасности корпоративной сети.
12. Возможности брандмауэра Windows.
13. Возможности iptables.
14. Принцип работы, применение и защита от сетевого сканера nmap.
15. Основные подходы к анализу защищенности корпоративной сети.

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы на конференции по итогам практики. Проводится собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы.

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.

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

а) основная литература

1. Таненбаум, Э., Современные операционные системы / Э. Таненбаум; [пер. с англ. Н. Вильчинского, А. Лашкевича]. - 3-е изд., СПб., Питер, 2013, 1115с
2. Дейтел Х. Операционные системы. Основы и принципы. 3-е изд. - М.: Бином-Пресс, 2009. - 1024 с.
3. Олифер В. Сетевые операционные системы. - СПб.: Издательство: Питер, 2009. - 668 с.
4. 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.
5. 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.
6. 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).

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. Внутреннее устройство Windows. / М. Русинович, Д. Соломон, А. Ионеску, П. Йосифович; [пер. с англ. Е. Матвеева] - 7-е изд. - СПб.: Питер, 2018. - 942 с.
4. Бражук, А. И. Сетевые средства Linux / Бражук А. И. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/intuit_360.html (дата обращения: 26.01.2022). - Режим доступа : по подписке. Бовет Д. Ядро Linux. Серия: Внесерийная. - СПб.: Издательство: БХВ-Петербург, 2007.-1108 с.
5. Гунько, А. В. Системное программирование в среде Linux : учебное пособие / А. В. Гунько. - Новосибирск : НГТУ, 2020. - 235 с. - ISBN 978-5-7782-4160-2. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785778241602.html (дата обращения: 26.01.2022). - Режим доступа : по подписке

6. Дюгуров, Д. В. Сетевая безопасность на основе серверных продуктов Microsoft / Дюгуров Д. В. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/intuit_359.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.
7. Линн С. Администрирование Microsoft Windows Server 2012. СПб.: Питер, 2014. 304 с.
8. Фленов М. Е. Linux глазами хакера: 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2010. — 480 с.

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/
4. Журнал «Хакер».(https://xakep.ru/).
5. Архив эксплоитов. (https://www.exploit-db.com/)

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

Обучающиеся перед прохождением производственной практики обеспечиваются программой прохождения практики и индивидуальным заданием руководителя практики. Самостоятельная работа обучающихся подразумевает работу под руководством преподавателей, осуществляющих руководство учебной практикой. Проводя собеседование, преподаватели 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. В соответствии с описанными задачами обучающийся собирает и обрабатывает информацию для написания отчета. По окончании практики обучающийся в установленные сроки сдает руководителю практики от института отчет о практике. Отчет по практике содержит титульный лист, содержание (план), текстовую часть, список литературы, приложения, дневник, характеристику.

Необходимым компонентом производственной практики является выполнение индивидуального задания. Индивидуальное задание на практику направлено на углубление и расширение полученных студентами знаний в области информационной безопасности, которое является одним из необходимых условий дальнейшего освоения дисциплин профессионального цикла. Результаты выполнения индивидуального задания оформляются в виде реферата, входящего в состав отчета по практике в качестве его основного раздела.

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

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 (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).
6. Электронно-библиотечная система «Лань» http://e.lanbook.com/
7. ГАРАНТ. Информационно-правовой портал (доступ с компьютеров университета. Собинова, 36а-Библиотека).

11. Материально-техническая база, необходимая для проведения практики

Все доступные ресурсы предприятия используются студентами во время проектно-технологической практики.

12. 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