

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

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа производственной практики
«Технологическая 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 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 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 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 – 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.

2. Место практики в структуре образовательной программы

Технологическая практика относится к обязательной части образовательной программы.

Целью 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 закреплённые в результате прохождения производственной технологической практики, используются студентами при разработке курсовых и выпускных работ.

3. Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс прохождения практики направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения 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- 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 | И-ОПК-10.3 Знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности, и принципы формирования политики информационной безопасности организации. И-ОПК-10.4 Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях И-ОПК-10.5 Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с | Знать: - правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности - принципы формирования политики информационной безопасности организации - программно-аппаратные средства защиты информации Уметь: - конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности |

| | | |
|---|---|---|
| | заданными политиками безопасности И-ОПК-10.6 Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты. | |
| Профессиональные компетенции | | |
| ПК-3 Способен обеспечивать контроль над соблюдением требований по защите информации | И-ПК-3.3 Владеет навыками осуществления контроля над соблюдением требований по защите информации | Владеть: навыками применения методов реализации политики информационной безопасности и комплексного подхода к обеспечению информационной безопасности объекта защиты. |

4. Объем практики составляет 5 зачетных единиц, 2 2/3 недели.

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 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.

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.

Список вопросов и (или) заданий для проведения промежуточной аттестации

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. Проводятся 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, 2014. - 1115 с.
2. Дейтел Гарви М. Введение в операционные системы: В 2 т.. Т.1. / Гарви М. Дейтел; Пер. с англ. - М.: Мир, 1987. - 359 с.
3. Проскурин, В. Г. Защита в операционных системах : учебное пособие для вузов / Проскурин В. Г. - Москва : Горячая линия - Телеком, 2014. - 192 с. - ISBN 978-5-9912-0379-1. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785991203791.html>
4. Олифер В. Г. Сетевые операционные системы: [учеб. пособие для вузов]. / В. Г. Олифер, Н. А. Олифер; М-во образования и науки РФ - 2-е изд. - СПб.: Питер, 2009. - 668 с.

б) дополнительная литература

1. Котельников, Е. В. Введение во внутреннее устройство Windows / Котельников Е. В. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/intuit_062.html
2. Внутреннее устройство Windows. / М. Русинович, Д. Соломон, А. Ионеску, П. Йосифович; [пер. с англ. Е. Матвеева] - 7-е изд. - СПб.: Питер, 2018. - 942 с.
3. Мошков, М. Е. Введение в системное администрирование Unix / Мошков М. Е. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/intuit_084.html

4. 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>
5. 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
6. Фленов М. Е. Linux глазами хакер — СПб.: БХВ-Петербург, 2010 https://books.4nmv.ru/books/linux_glazami_khakera_3-e_izd_3643238.pdf

в) ресурсы сети «Интернет»

1. Журнал хакер <https://xakep.ru/>
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. Nmap — свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети. <https://nmap.org/>
5. Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. <https://www.wireshark.org/>
6. Metasploit Project — проект, посвященный информационной безопасности. <https://www.metasploit.com/>
7. Архив эксплоитов. <https://www.exploit-db.com/>

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

В процессе обучения используются следующие образовательные технологии:

Инструктивная лекция – проводится с целью организации последующей самостоятельной работы студентов.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

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 обучающимися. 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. 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

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 ЯпГУ;
- 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, посвящённый информационной безопасности. <https://www.metasploit.com/>

10. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса (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
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента» <https://www.studentlibrary.ru>

11. Материально-техническая база, необходимая для проведения практики

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 знакомиться 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:

старший преподаватель кафедры КБ и ММОИ

А.В. Саханда