

*Приложение 2.27.1к ОПОП по специальности
09.02.11 Разработка и управление программным обеспечением*

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Многопрофильный колледж

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ДЛЯ ЛАБОРАТОРНЫХ ЗАНЯТИЙ
УЧЕБНОЙ ДИСЦИПЛИНЫ**

ОП.05 Основы информационной безопасности

для обучающихся специальности

09.02.11 Разработка и управление программным обеспечением

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ.....	3
2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ.....	4
Лабораторное занятие №1	4
Лабораторное занятие №2	5
Лабораторное занятие №3	6
Лабораторное занятие №4	7
Лабораторное занятие №5	8
Лабораторное занятие №6	9
Лабораторное занятие №7	10

1 ВВЕДЕНИЕ

Важную часть теоретической и профессиональной практической подготовки обучающихся составляют лабораторные занятия.

Состав и содержание лабораторных занятий направлены на реализацию Федерального государственного образовательного стандарта среднего профессионального образования.

Ведущей дидактической целью лабораторных занятий является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей).

В соответствии с рабочей программой учебной дисциплины «Основы информационной безопасности» предусмотрено проведение лабораторных занятий.

В результате их выполнения, обучающийся должен уметь:

Уд 3_ОП.05. Реализовывать защиту от распространенных уязвимостей (SQLi, XSS, CSRF);

Уд 4_ОП.05. Применять безопасные практики аутентификации и управления сессиями;

Уд 5_ОП.05. Использовать средства статического и динамического анализа кода;

Уо 02.02. Использовать современное программное обеспечение и цифровые средства для решения профессиональных задач; проявлять культуру информационной безопасности.

Содержание лабораторных занятий ориентировано на подготовку обучающихся к освоению профессионального модуля программы подготовки специалистов среднего звена по специальности и овладению **профессиональными компетенциями:**

ПК 2.2. Разрабатывать модули программного обеспечения

А также формированию общих компетенций:

ПК 2.2. Разрабатывать модули программного обеспечения;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

Лабораторные занятия проводятся в рамках соответствующей темы, после освоения дидактических единиц, которые обеспечивают наличие знаний, необходимых для ее выполнения.

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Лабораторное занятие №1

Организация защиты от атак

Цель: сформировать умения выявлять актуальные киберугрозы (фишинг, вредоносное ПО, сетевые атаки) и подбирать организационно-технические меры защиты.

Выполнив работу, вы будете уметь:

Уд 3_ОП.05 Реализовывать защиту от распространенных уязвимостей (SQLi, XSS, CSRF).

Материальное обеспечение: как в таблице 2.3

ПК, OWASP Threat Dragon, Draw.io, матрица угроз MITRE ATT&CK, доступ к интернет-ресурсам.

Задание:

1. Проанализировать архитектуру типового веб-приложения;
2. Выявить потенциальные векторы атак с использованием OWASP Threat Dragon;
3. Составить матрицу угроз по методологии MITRE ATT&CK;
4. Предложить организационно-технические меры защиты для каждой категории угроз.

Порядок выполнения работы:

1. Описание компонентов системы и потоков данных (диаграмма DFD)
2. Идентификация активов и точек входа для атак;
3. Моделирование угроз в OWASP Threat Dragon по категориям STRIDE;
4. Сопоставление угроз с тактиками MITRE ATT&CK;
5. Разработка плана контрмер (технических и организационных);
6. Оформление отчета с таблицей угроз и рекомендациями.

Форма представления результата:

Отчет с диаграммой потоков данных, таблицей угроз (STRIDE/ATT&CK), матрицей рисков и планом контрмер.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Лабораторное занятие №2

Организация работы VPN и межсетевого экрана

Цель: сформировать умения настройки VPN-туннелей, правил межсетевого экрана и оценки эффективности фильтрации трафика.

Выполнив работу, вы будете уметь:

Уд 3_ОП.05 Реализовывать защиту от распространенных уязвимостей (SQLi, XSS, CSRF).

Материальное обеспечение:

ПК, виртуальные машины (VMware/VirtualBox), OpenVPN, WireGuard, iptables/nftables, pfSense, Wireshark.

Задание:

1. Развернуть виртуальную лабораторную среду с двумя сетевыми сегментами;
2. Настроить VPN-туннель между сегментами;
3. Реализовать правила межсетевого экрана для фильтрации входящего/исходящего трафика;
4. Протестировать конфигурацию и зафиксировать результаты анализа трафика.

Порядок выполнения работы:

1. Установка и настройка виртуальных машин с ОС Linux;
2. Генерация ключей и конфигурация OpenVPN/WireGuard;
3. Настройка правил iptables: разрешение/запрет портов, протоколов, IP-адресов;
4. Тестирование соединения и проверка применения правил;
5. Захват и анализ трафика в Wireshark;
6. Документирование конфигурации и результатов тестирования.

Форма представления результата:

Отчет с конфигурационными файлами VPN и firewall, скриншотами работы Wireshark, описанием примененных правил и результатов тестов.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Лабораторное занятие №3

Тестирование на проникновение и анализ уязвимостей

Цель: сформировать умения проводить тестирование на проникновение, сканирование уязвимостей и оценку их критичности с использованием CVSS.

Выполнив работу, вы будете уметь:

Уд 5_ОП.05 Использовать средства статического и динамического анализа кода.

Материальное обеспечение:

ПК, Kali Linux, OWASP ZAP, Burp Suite Community, Nmap, Metasploit (опционально), CVSS Calculator (NVD).

Задание:

1. Провести сканирование уязвимого веб-приложения (DVWA/Juice Shop);
2. Выявить уязвимости категорий OWASP Top 10;
3. Оценить критичность найденных уязвимостей по CVSS;
4. Предложить методы устранения выявленных проблем.

Порядок выполнения работы:

1. Настройка целевого уязвимого приложения в виртуальной среде;
2. Пассивное и активное сканирование с помощью OWASP ZAP
3. Ручная проверка подозрительных точек ввода (SQLi, XSS, CSRF);
4. Расчет CVSS-баллов для каждой уязвимости (вектор, базовая оценка);
5. Формирование отчета с приоритизацией исправлений;
6. Демонстрация эксплуатации одной уязвимости (в учебной среде).
- 7.

Форма представления результата:

Отчет со списком уязвимостей, векторами CVSS, скриншотами сканирования, рекомендациями по устранению.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Лабораторное занятие №4

Выполнение резервного копирования и восстановления данных. Управление доступом к данным

Цель: сформировать умения настройки резервного копирования, восстановления данных и управления правами доступа (RBAC, ACL).

Выполнив работу, вы будете уметь:

Уд 4_ОП.05 Применять безопасные практики аутентификации и управления сессиями.

Материальное обеспечение:

ПК, ОС Windows/Linux, системы резервного копирования (Bacula, Duplicati, rsync), облачные хранилища (S3, Nextcloud).

Задание:

1. Реализовать схему резервного копирования с заданной периодичностью;
2. Провести восстановление данных из резервной копии;
3. Настроить разграничение прав доступа к файлам и директориям;
4. Протестировать политику доступа для разных групп пользователей.

Порядок выполнения работы:

1. Создание тестовой структуры данных с разным уровнем конфиденциальности;
2. Настройка расписания и параметров резервного копирования (rsync/cp-утилиты);
3. Имитация потери данных и выполнение процедуры восстановления;
4. Настройка ACL: определение пользователей/групп, назначение прав (rwx);
5. Проверка применения политик доступа (успешный/неуспешный доступ);
6. Документирование процедур и результатов тестирования.

Форма представления результата:

Отчет со скриптами/конфигурациями резервного копирования, логами восстановления, таблицей прав доступа и результатами проверок.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Лабораторное занятие №5

Изучение модели облачных услуг и их безопасности

Цель: сформировать умения анализа моделей облачного обслуживания (IaaS, PaaS, SaaS), оценки угроз для облачных сред и настройки базовых средств защиты.

Выполнив работу, вы будете уметь:

Уо 02.02 Использовать современное программное обеспечение, различные цифровые средства для решения профессиональных задач; проявлять культуру информационной безопасности.

Материальное обеспечение:

ПК, интернет-браузер, консоли облачных провайдеров (Yandex Cloud, AWS Free Tier, Microsoft Azure), документация CSA, OWASP Cloud Security.

Задание:

1. Проанализировать модели IaaS/PaaS/SaaS и распределение ответственности;
2. Выявить угрозы для выбранной облачной модели с использованием CSA CCM;
3. Настроить базовые политики безопасности в облачной консоли (IAM, сетевые правила);
4. Задokumentировать конфигурацию и рекомендации по усилению защиты.

Порядок выполнения работы:

1. Изучение документации провайдера и модели ответственности (Shared Responsibility);
2. Регистрация в тестовом аккаунте облачного провайдера;
3. Создание ресурсов (ВМ, хранилище) с применением минимальных привилегий;
4. Настройка IAM-политик: роли, пользователи, разрешения;
5. Конфигурация сетевых правил (Security Groups, NSG);
6. Анализ конфигурации на соответствие лучшим практикам (CIS Benchmarks);
7. Оформление отчета с матрицей угроз и скриншотами настроек.

Форма представления результата:

Отчет с анализом модели ответственности, таблицей угроз облачной среды, конфигурациями IAM и сетевых правил, рекомендациями по защите.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Лабораторное занятие №6

Работа с инцидентами информационной безопасности

Цель: сформировать умения обнаружения, классификации, расследования и реагирования на инциденты ИБ с использованием SIEM-систем.

Выполнив работу, вы будете уметь:

Уд 5_ОП.05 Использовать средства статического и динамического анализа кода.

Материальное обеспечение:

ПК, TheHive, MISP, ELK Stack (Elasticsearch, Logstash, Kibana), Syslog-ng, демонстрационные наборы логов.

Задание:

1. Настроить сбор и нормализацию логов в SIEM-системе;
2. Создать правила корреляции для детектирования типовых атак;
3. Проанализировать демонстрационный инцидент и восстановить цепочку событий;
4. Сформировать отчет о расследовании с рекомендациями по предотвращению.

Порядок выполнения работы:

1. Развертывание ELK Stack или использование готовой среды;
2. Настройка парсеров для различных источников логов (веб-сервер, ОС, приложение);
3. Создание дашбордов и алертов на подозрительную активность;
4. Анализ предоставленного набора логов: идентификация IOC, временная шкала;
5. Классификация инцидента по типу (malware, unauthorized access, data leak);
6. Формирование отчета: описание, влияние, принятые меры, рекомендации.

Форма представления результата:

Отчет с конфигурацией правил корреляции, скриншотами дашбордов, временной шкалой инцидента, выводами и рекомендациями.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Лабораторное занятие №7

Разработка политики информационной безопасности

Цель: сформировать умения разработки и документирования корпоративной политики ИБ, парольной политики, правил доступа и планов реагирования на инциденты.

Выполнив работу, вы будете уметь:

Уо 02.02 Использовать современное программное обеспечение, различные цифровые средства для решения профессиональных задач; проявлять культуру информационной безопасности.

Материальное обеспечение:

ПК, текстовые процессоры (MS Word, LibreOffice Writer), шаблоны политик (ISO 27001, NIST, ФСТЭК), системы контроля версий (Git).

Задание:

1. Разработать проект политики информационной безопасности для условной организации;
2. Включить разделы: парольная политика, управление доступом, реагирование на инциденты;
3. Согласовать требования с нормативными документами РФ;
4. Оформить документ в соответствии с корпоративными стандартами.

Порядок выполнения работы:

1. Анализ целевой аудитории и области действия политики;
2. Изучение шаблонов и требований (152-ФЗ, ФСТЭК, ГОСТ Р 57580);
3. Разработка структуры документа: цели, область, термины, положения, ответственность;
4. Формулировка конкретных требований (длина пароля, срок действия, блокировка);
5. Описание процедур реагирования на инциденты (этапы, роли, сроки)
6. Рецензирование и финальное оформление документа.

Форма представления результата:

Документ «Политика информационной безопасности» с разделами: общие положения, требования к аутентификации, управление доступом, реагирование на инциденты, ответственность, приложения.

Критерии оценки:

«5» (отлично): выставляется студенту, если лабораторная работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.