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 дисциплины

Аудит информационной безопасности

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

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. **Цели освоения дисциплины**

Целью освоения дисциплины «Аудит информационной безопасности» является освоение теоретических основ и изучение принципов проведения аудита информационной безопасности, ознакомление с методами и средствами проведения аудита информационной безопасности в вычислительных сетях и приобретение практических навыков проведения аудита информационной безопасности.

Данный курс вырабатывает у студентов знания, навыки и умения организовывать процесс сбора событий информационной безопасности в объекте информатизации, выявление инцидентов безопасности и меры противодействия возникающим угрозам информационной безопасности.

2. Место дисциплины в структуре ОП

«Аудит информационной безопасности» относится к числу дисциплин обязательной части образовательной программы.

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Операционные системы» – знание принципов функционирования современных операционных систем и умение их администрировать.

«Вычислительные сети» – знание принципов функционирования вычислительных сетей.

Знания и навыки, полученные в результате изучения дисциплины «Аудит информационной безопасности», используются студентами в дальнейшем при научно-исследовательской работе и в профессиональной деятельности.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

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)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	И-ОПК-1_1 Способен на основе анализа информации о потенциальных рисках и угрозах, видах и возможностей нарушителей, целей и задач защиты,разработать и обосновать требования к системе	**Знать:** - основы системного подхода к обеспечению информационной безопасности; - методы моделирования, применяемые при оценке рисков информационной безопасности. **Уметь** - осуществлять классификацию задач и процессов информационной безопасности; - применять методы моделирования для аудита информационной безопасности. **Владеть** - навыками аудита информационной безопасности и анализа последствий при возникновении угроз в сфере

	обеспечения информационной безопасности	информационной безопасности; - навыками использования программных средств, применяемых при аудите информационной безопасности.
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**И_УК-1_1** Осуществляет системный анализ задачи, выделяя ее базовые составляющие	**Знать:** - методологию системного подхода при решении задач аудита информационной безопасности. **Уметь** - осуществлять классификацию задач и процессов информационной безопасности; - выстраивать процесс обеспечения информационной безопасности. **Владеть** - навыками аудита информационной безопасности и анализа последствий при возникновении угроз в сфере информационной безопасности; - навыками критического анализа возникаемых задач информационной безопасности.
	И_УК-1_2 Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	**Уметь** - выявлять проблемные ситуации, используя методы аудита информационной безопасности; - ранжировать выявленные угрозы информационной безопасности. **Владеть** - навыками устранения выявленных угроз информационной безопасности.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 акад. часов.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**						**Формы текущего контроля успеваемости Форма промежуточной аттестации** ***(по семестрам)***
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	
1	Введение.	2		2				4	Опрос на практических занятиях
2	Развертывание виртуальной сетевой лаборатории.	2		6	8			8	Выполнение лабораторной работы
3	Программные средства проведения аудита информационной безопасности.	2		4	4			8	Выполнение лабораторной работы
4	Журналирование событий	2		2	2			8	Выполнение

	в ОС Microsoft Windows.								лабораторной работы
5	Журналирование событий в ОС Linux.	2		2	2			8	Выполнение лабораторной работы
		2					0.3	3.7	Зачет
	Всего за 2 семестр 72 часа			16	16		0.3	39.7	
6	Журналирование событий в прикладном ПО.	3		6	6			1	Выполнение лабораторной работы
7	Сбор событий информационной безопасности.	3		6	6			1	Выполнение лабораторной работы
8	Реагирование на инциденты информационной безопасности.	3		4	4			2	Выполнение лабораторной работы
		3				2	0.5	33.5	Экзамен
	Всего за 3 семестр 72 часа			16	16	2	0.5	37.5	
	ИТОГО	**144**		**32**	32	2	**0.8**	**77.2**	

Содержание разделов дисциплины:

Тема № 1 Введение.

1.1. Международные и российские стандарты аудита информационной безопасности.

1.2. Угрозы информационной безопасности. Обзор материалов банка данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru).

1.3. Уязвимости и их классификация. Метрики CVSSv1, CVSSv2, CVSSv3.

1.4. Типовые уязвимости веб-приложений.

1.5. Матрица MITRE ATT&CK.

Тема № 2 Развертывание виртуальной сетевой лаборатории.

2.1. Гипервизор Oracle VirtualBox.

2.2. Конфигурация сетевых интерфейсов и взаимодействие виртуальных машин.

2.3. Платформа эмуляции Eve-NG.

2.4. Взаимодействие компонентов виртуальной сетевой лаборатории.

Тема № 3 Программные средства проведения аудита информационной безопасности.

3.1. Сканеры уязвимостей.

3.2. Инвентаризация ПО и уязвимостей. Язык Open Vulnerability and Assessment Language.

3.3. Поиск и устранение уязвимостей на примере образа виртуальной машины Metasploitable 2.

Тема № 4 Журналирование событий в ОС Microsoft Windows.

4.1. Журналы безопасности ОС Microsoft Windows.

4.2. Конфигурация аудита событий безопасности в ОС Microsoft Windows.

4.3. Дополнительные источники событий ОС Microsoft Windows. Sysmon.

4.4. Журналирование событий в домене Active Directory.

Тема № 5 Журналирование событий в ОС Linux.

5.1. Журналы событий ОС Linux.

5.2. Конфигурация службы auditd. Журналирование специфичных событий.

5.3. Архивирование событий.

Тема № 6 Журналирование событий в прикладном ПО.

6.1. Журналирование событий в СУБД.

6.2. Журналирование событий веб-приложений.
6.3. Журналирование событий в почтовых серверах.
6.4. Журналирование событий в файловых серверах.
Тема № 7 Сбор событий информационной безопасности.
7.1. Агентный и безагентный сбор событий информационной безопасности.
7.2. Системы хранения событий информационной безопасности. ElasticSearch.
7.2. SIEM-системы. OSSIM.
7.3. Корреляция. Разработка правил корреляции по матрице MITRE ATT&CK.
Тема № 8 Реагирование на инциденты информационной безопасности.
8.1. Генерация инцидентов информационной безопасности на основе матрицы MITRE ATT&CK и их выявление.
8.2. Проведение расследования компьютерных инцидентов.
8.3. Исследование носителей компьютерной информации.
8.4. Устранение последствий инцидентов информационной безопасности.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:
программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:
- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Oracle VirtualBox (свободно распространяемое ПО);
- Eve-NG (свободно распростаняемое ПО);

- Ubuntu (свободно распространяемое ПО);
- Kali Linux (свободно распространяемое ПО);
- OSSIM (свободно распростаняемое ПО);
- ElasticSearch (свободно распростаняемое ПО).

7. 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. Электронно-библиотечная система «Юрайт» https://www.biblio-online.ru/

3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).

4. Новости в сфере информационной безопасности и защиты компьютерной информации журнала «Хакер»: https://xakep.ru/tag/news и журнала «Информационная безопасность»: http://itsec.ru/main.php.

5. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»: http://www.kaspersky.ru/internet-security-center.

6. Федеральный банк данных угроз безопасности, ведущийся в разделе «Техническая защита информации» официального сайта ФСТЭК России (https://bdu.fstec.ru).

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. Таненбаум Э. Архитектура компьютера. / Э. Таненбаум; [пер. с англ. Ю. Гороховского, Д. Шинтякова] - 5-е изд. - СПб.: Питер, 2013. - 843 с.

2. Таненбаум Э. Современные операционные системы. / Э. Таненбаум, Х. Бос; [пер. с англ. А. Леонтьевой, М. Малышевой, Н. Вильчинского] - 4-е изд. - СПб.: Питер, 2019. - 1119 с.: ил.

3. Таненбаум Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл; [пер. с англ. А. Гребенькова] - 5-е изд. - СПб.: Питер, 2019. - 955 с.

4. Бирюков А. А. Информационная безопасность: защита и нападение М.: ДМК Пресс, 2017. -434 с.

б) дополнительная литература

1. Белов Е.Б, Лось В.П. и др., «Основы информационной безопасности», Учебное пособие для вузов..- М.: Горячая линия – Телеком, 2006. – 544 с.

2. Девянин П.Н. Модели безопасности компьютерных систем. / П.Н. Девянин - Москва: Академия, 2005. - 320 с.

3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для вузов. - М.: Академия, 2014. - 331 с.

4. Проскурин В.Г., «Защита программ и данных», 2-е издание, учебное пособие для студ. учреждений высш. проф. образования, М., Издательский центр «Академия», 2012.- 208с

5. Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс] / Крис Касперски. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2010. — 446 с. — 5-93455-175-2. — Режим доступа: http://www.iprbookshop.ru/65405.html

6. Ю. Диогенес, Э. Озкайя Кибербезопасность стратегии атак и обороны. М.: ДМК Пресс, 2020. - 326 с.

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

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа;
-учебные аудитории для проведения практических занятий: лабораторию программно-аппаратных средств обеспечения информационной безопасности;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для проведения лабораторных занятий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор:

Доцент кафедры компьютерной безопасности и математических методов обработки информации		А.А. Горохов
должность, ученая степень	*подпись*	*И.О. Фамилия*

Приложение № 1 к рабочей программе дисциплины
«Аудит информационной безопасности»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Лабораторная работа №1
(проверка сформированности ОПК-1, индикатор И_ОПК-1_1)

Пример задания:

Вариант 1

1. В среде виртуализации VirtualBox создать виртуальную машину, установить эмулятор Eve-NG.
2. Создать виртуальную машину, установить ОС Kali linux.
3. В эмуляторе Eve-NG создать виртуальный компьютер, настроить на нем адресацию.
4. В эмуляторе Eve-NG добавить маршрутизатор Mikrotik, настроить на нем адресацию.
5. Настроить сетевое взаимодействие между виртуальной машиной Kali linux и виртуальным компьютером через используемый маршрутизатор.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное задание – 2 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №2
(проверка сформированности УК-1, индикатор И_УК-1_2)

Пример задания:

Вариант 1

1. В среде виртуализации VirtualBox добавить виртуальную машинуMetasploitable 2.
2. Установить и настроить сканер уязвимостей OpenVAS, настроить сетевое взаимодействие с виртуальной машиной Metasploitable 2.
3. Провести поиск уязвимостей в виртуальной машине Metasploitable с использованием сканера уязвимостей OpenVAS.
4. Провести поиск уязвимостей в виртуальной машине Metasploitable 2 с использованием интерпретатора OVAL.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 2 балла;
- задание № 2 – 2 балла;
- задание № 3 – 3 балла;
- задание № 4 – 3 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №3
(проверка сформированности УК-1, индикатор И_УК-1_1)

Пример задания:

Вариант 1

1. В среде виртуализации VirtualBox создать машину под управлением ОС Microsoft Windows.
2. Настроить аудит определенного события информационной безопасности (аудит успеха/отказа – ввод пароля, доступ к файлу, создание пользователя и т.д.).
3. Сгенерировать событие из задания 2 и продемонстрировать его в журнале событий.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 3 балла;
- задание № 2 – 3 балла;
- задание № 3 – 4 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №4
(проверка сформированности УК-1, индикатор И_УК-1_1)

Пример задания:

Вариант 1

1. В среде виртуализации VirtualBox создать машину под управлением ОС Linux.

2. Настроить аудит определенного события информационной безопасности (аудит успеха/отказа – ввод пароля, доступ к файлу, создание пользователя и т.д.).
3. Сгенерировать событие из задания 2 и продемонстрировать его в журнале событий.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 3 балла;
- задание № 2 – 3 балла;
- задание № 3 – 4 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №5
(проверка сформированности УК-1, индикатор И_УК-1_1)

Пример задания:

Вариант 1

1. В среде виртуализации VirtualBox создать машину и установить на нее операционную систему, совместимую с источником событий – СУБД MySQL.
2. Установить СУБД MySQL.
3. Настроить аудит определенного события информационной безопасности (аудит успеха/отказа – ввод пароля, выполнение SQL-запроса).
4. Сгенерировать событие из задания 3 и продемонстрировать его в журнале событий.

Вариант 2

1. В среде виртуализации VirtualBox создать машину и установить на нее операционную систему, совместимую с источником событий – веб-сервером Apache Tomcat.
2. Установить Apache Tomcat.
3. Настроить аудит определенного события информационной безопасности (аудит успеха/отказа – доступ к файлам веб-сервера).
4. Сгенерировать событие из задания 3 и продемонстрировать его в журнале событий.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 2 балла;
- задание № 2 – 2 балла;
- задание № 3 – 3 балла;
- задание № 4 – 3 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №6
(проверка сформированности УК-1, индикатор И_УК-1_2)

Пример задания:

Вариант 1

1. В среде виртуализации VirtualBox создать машину и установить на нее ElasticSearch, OSSIM или любую другую систему сбора событий.
2. Настроить сбор событий с источника из лабораторной работы №5.
3. Продемонстрировать в системе сбора событий сгенерированное событие из лабораторной работы №5.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 4 балла;
- задание № 2 – 3 балла;
- задание № 3 – 3 балла;

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №7
(проверка сформированности ОПК-1, индикатор И_ОПК-1_1)

Пример задания:

Вариант 1

1. В виртуальной машине Metasploitable устранить уязвимость, удовлетворяющую следующим критериям:
-значение CVSSv2 у уязвимости выше, чем 7.0
-служба, подверженная уязвимости, функционирует на TCP-порту 21.
2. Продемонстрировать работоспособность службы после устранения указанной уязвимости.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное

- задание № 1 – 6 балла;
- задание № 2 – 4 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список заданий к зачету

На зачете проверяется сформированность компетенции УК-1, (индикаторы И_УК-1_1, И_УК-1_2).

Зачет выставляется по результатам контрольной работы при условии набора по итогам ее выполнения студентом с одной попытки не менее 6 баллов.

Примеры заданий:

Вариант 1.

1. Установить ОС Linux или Windows на виртуальную машину.
2. Настроить аудит успеха и отказа для входа в ОС Linux или Windows. Настроить аудит доступа к файлам в каталоге /home/user или C:\Users\user.
3. Предоставить преподавателю учетную запись и пароль пользователя User.
4. После авторизации преподавателем на виртуальной машине, выяснить, какой пользователь осуществил неудачную попытку входа в ОС.
5. После авторизации преподавателем на виртуальной машине выяснить, к какому файлу был запрошен доступ.

<u>Правила выставления оценки по результатам зачетной работы:</u>

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 2 балла;
- задание № 2 – 2 балла;
- задание № 3 – 2 балла;
- задание № 4 – 2 балла;
- задание № 5 – 2 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам зачетной работы – 10 баллов,

Набранное количество баллов от 6-10 соответствует оценке «зачтено, менее 6 баллов – оценке «не зачтено» (умения на данном этапе освоения дисциплины не сформированы).

Список заданий к экзамену

На зачете проверяется сформированность компетенции ОПК-1 (индикатор И_ОПК-1_1).

Оценка выставляется по результатам экзаменационной работы.

Примеры заданий:

Вариант 1.

1. Развернуть виртуальную машину Metasploitable 2 (ссылка), настроить необходимое для Вашей работы сетевое окружение (например, сканер уязвимостей OpenVAS, Kali linux), настроить сетевое взаимодействие, убедиться, что виртуальные машины видят друг друга. Нарисовать схему сети с IP-адресами используемого оборудования.
2. Сменить пароли по-умолчанию для заданной службы, в качестве ответа перечислить список пользователей, которым были заданы новые пароли, и используемые команды. Варианты служб: VNC, MySQL, Postgres, ОС Linux.
3. Для заданного порта описать запущенную службу, ее версию, назначение, наиболее критичные уязвимости и их описание.
4. Составить инструкцию по устранению выявленной критичной уязвимости: словесное описание (например, обновление до версии а.с, или модификация файла конфигурации) и список команд, которые необходимо применить для устранения.

Правила выставления оценки по результатам экзаменационной работы:

Оценка по результатам экзаменационной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 2 балла;
- задание № 2 – 2 балла;
-задание № 3 – 3 балла;
-задание № 4 – 3 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом, или в случае, когда команды или описание службы неверно или не полностью задокументированы.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам экзаменационной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень – предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является

обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень – предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень – предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями¸ умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

– владение основным объемом знаний по программе дисциплины;

– знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;

– владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;

– способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;

– усвоение основной литературы, рекомендованной рабочей программой дисциплины;

– знание базовых теорий, концепций и направлений по изучаемой дисциплине;

– самостоятельная работа на практических занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

– достаточно полные и систематизированные знания в объёме программы дисциплины;

– использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

– владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;

– способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

– усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

– умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;

– самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

– систематизированные, глубокие и полные знания по всем разделам дисциплины;

– точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

– безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

– способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

– полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

– умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;

– активная самостоятельная работа на практических занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачтено», «не зачтено») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «не зачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение № 2 к рабочей программе дисциплины
«Аудит информационной безопасности»

Методические указания для студентов по освоению дисциплины

Основной учебного материала по дисциплине «Аудит информационной безопасности» являются практические занятия, источники основной и дополнительной литературы, вместе с Web-материалами, указанными в Рабочей программе и доведенными до студентов (преподавателем и через возможности библиотечного фонда ЯрГУ). По всем темам предусмотрены лабораторные занятия, на которых происходит закрепление изученного материала путем применения его к конкретным информационным объектам и отработка навыков работы со специализированным программным обеспечением. Для успешного освоения дисциплины важно углубленное самостоятельное изучение всех тем дисциплины в упомянутых рекомендуемых источниках. Также, в процессе изучения дисциплины, рекомендуется регулярное повторение пройденного практического материала. Материал, представленный в предлагаемой учебной литературе, необходимо еще раз после занятий прорабатывать и, при необходимости, дополнять актуальной информацией, полученной из рекомендованных ресурсов сети «Интернет» и на консультациях и лабораторных занятиях.

Для проверки и контроля усвоения приобретенных практических навыков проводятся мероприятия текущей аттестации в виде лабораторных работ. Также проводятся консультации (при необходимости) по разбору наиболее острых и сложных для усвоения тем, которые вызвали затруднения у студентов.

В конце первого семестра изучения дисциплины студенты сдают зачет. Зачет принимается по экзаменационным билетам, каждый из которых включает в себя два практических вопроса. На зачете проверяются умения и навыки студентов в работе с основными инструментами, применяемыми при аудите информационной безопасности.

В конце второго семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два три практических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к зачету предусмотрена групповая консультация.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать следующую учебную литературу:

1. Таненбаум Э. Архитектура компьютера. / Э. Таненбаум; [пер. с англ. Ю. Гороховского, Д. Шинтякова] - 5-е изд. - СПб.: Питер, 2013. - 843 с.

2. Таненбаум Э. Современные операционные системы. / Э. Таненбаум, Х. Бос; [пер. с англ. А. Леонтьевой, М. Малышевой, Н. Вильчинского] - 4-е изд. - СПб.: Питер, 2019. - 1119 с.: ил.

3. Таненбаум Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл; [пер. с англ. А. Гребенькова] - 5-е изд. - СПб.: Питер, 2019. - 955 с.

4. Бирюков А. А. Информационная безопасность: защита и нападение М.: ДМК Пресс, 2017. -434 с.

Для самостоятельного подбора литературы в библиотеке ЯрГУ рекомендуется использовать:

1. Электронная картотека «Книгообеспеченность» (http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии

книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет