ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля): **Теоретические основы систем обнаружения, предупреждения компьютерных атак**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Омельченко Т. А., старший преподаватель

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - Целью освоения дисциплины является теоретическая и практическая подготовка выпускника в области эксплуатации и проектирования современных систем обнаружения атак для обеспечения их эффективного применения

Задачи дисциплины:

- изучить основы мониторинга информационных систем
- выработка практических навыков применения основ мониторинга для обеспечения безопасности
- информирование об основных направлениях работы систем обнаружения атак
- информирование о способах реагирования на инциденты безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Теоретические основы систем обнаружения, предупреждения компьютерных атак» относится к части учебного плана, формируемой участниками образовательных отношений.

Дисциплина изучается на 5 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

- ПК-6 Способен проводить анализ безопасности компьютерных систем

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

виды политик безопасности компьютерных систем и сетей

Студент должен уметь:

выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации

Студент должен владеть навыками:

разработки профиля защиты компьютерных систем

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Девятый семестр	Десятый семестр
Контактная работа (всего)	**144**	**80**	**64**
Лабораторные	48	32	16
Лекции	64	32	32
Практические	32	16	16
Самостоятельная работа (всего)	**36**	**28**	**8**
Виды промежуточной аттестации	**72**	**36**	**36**
Экзамен	72	36	36
Общая трудоемкость часы	**252**	**144**	**108**
Общая трудоемкость зачетные единицы	**7**	**4**	**3**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лабораторные (48 ч.)

Девятый семестр. (32 ч.)

Тема 1. Угрозы информационной системе (2 ч.)

Угрозы информационной системе

Тема 2. Уязвимости информационной системы (2 ч.)

Уязвимости информационной системы

Тема 3. Типичный сценарий действий нарушителя (2 ч.)

Типичный сценарий действий нарушителя

Тема 4. Признаки осуществления атаки (2 ч.)

Признаки осуществления атаки

Тема 5. Безопасность сетевого уровня модели OSI (2 ч.)

Безопасность сетевого уровня модели OSI

Тема 6. Сетевые анализаторы и «снифферы» (2 ч.)

Сетевые анализаторы и «снифферы»

Тема 7. Мониторинг безопасности беспроводных сетей (2 ч.)

Мониторинг безопасности беспроводных сетей

Тема 8. Понятие обнаружения атак (2 ч.)

Понятие обнаружения атак

Тема 9. Распределённые атаки и их признаки (2 ч.)

Распределённые атаки и их признаки

Тема 10. Компоненты и утилиты ОС для контроля состояния узла и сети (2 ч.)

Компоненты и утилиты ОС для контроля состояния узла и сети

Тема 11. Анализ защищённости на уровне ОС (2 ч.)

Анализ защищённости на уровне ОС

Тема 12. Этапы и средства реализации атак (2 ч.)

Этапы и средства реализации атак

Тема 13. Технологии обнаружения атак (2 ч.)

Технологии обнаружения атак

Тема 14. Мониторинг в операционной системе Windows (2 ч.)

запуск утилиты и анализирования информации в ней

Тема 15. Мониторинг в операционной системе Windows (2 ч.)

Мониторинг ресурсов в операционной системе Windows

Тема 16. Мониторинг в операционной системе Linux (2 ч.)

знакомство с несколькими утилитами для мониторинга и анализ информации в них

Десятый семестр. (16 ч.)

Тема 17. Мониторинг в операционной системе Linux (2 ч.)

Мониторинг ресурсов в операционной системе семейчива Linux

Тема 18. Сканер уязвимостей (2 ч.)

Типичные уязвимости прикладного уровня

Настройка и конфигурирование сканирования уязвимостей

Тема 19. Сканер уязвимостей (2 ч.)

Как выполнить безопасное и этичное сканирование уязвимостей

Тема 20. Сканер уязвимостей (2 ч.)

Примеры конфигураций сканирования

Чего не делает сканирование уязвимостей

Тема 21. ПК «Сканер-ВС» (2 ч.)

Выявление, анализ и устранение уязвимостей.

Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ.

Инвентаризация информационных ресурсов.

Проведение внутренних аудитов.

Соответствие требованиям нормативных документов, определяющих необходимость проведения контроля эффективности СЗИ.

Тема 22. ПК «Сканер-ВС» (2 ч.)

сбор информации: nmap, zenmap;
поиск уязвимостей: OpenVAS, nikto;
анализ веб-приложений: wpscan, burpsuite, owasp-zap;
атаки на пароли: john, johnny;
эксплуатация уязвимостей: metasploit framework;
сниффинг: wireshark.

Тема 23. ПК «Сканер-ВС» (2 ч.)

Сканер уязвимостей
Сканер сети
Поиск эксплойтов

Тема 24. ПАК «Рубикон-К» (2 ч.)

Принцип работы с сетевыми нтерфейсами на примере ПАК "Рубикон-К". Настройка сетевых интерфейсов для безопасного взаимодействия с сетью.

5.2. Содержание дисциплины: Практические (32 ч.)

Девятый семестр. (16 ч.)

Тема 1. Угрозы информационной системе (2 ч.)

Угрозы информационной системе

Тема 2. Уязвимости информационной системы (2 ч.)

Уязвимости информационной системы

Тема 3. Типичный сценарий действий нарушителя (2 ч.)

Типичный сценарий действий нарушителя

Тема 4. Признаки осуществления атаки (2 ч.)

Признаки осуществления атаки

Тема 5. Безопасность сетевого уровня модели OSI (2 ч.)

Безопасность сетевого уровня модели OSI

Тема 6. Сетевые анализаторы и «снифферы» (2 ч.)

Сетевые анализаторы и «снифферы»

Тема 7. Мониторинг безопасности беспроводных сетей (2 ч.)

Мониторинг безопасности беспроводных сетей

Тема 8. Понятие обнаружения атак (2 ч.)

Понятие обнаружения атак. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.

Десятый семестр. (16 ч.)

Тема 9. Распределённые атаки и их признаки (2 ч.)

Распределённые атаки и их признаки

Тема 10. Компоненты и утилиты ОС для контроля состояния узла и сети (2 ч.)

Компоненты и утилиты ОС для контроля состояния узла и сети

Тема 11. Анализ защищённости на уровне ОС (2 ч.)

Анализ защищённости на уровне ОС

Тема 12. Этапы и средства реализации атак (2 ч.)

Этапы и средства реализации атак

Тема 13. Технологии обнаружения атак (2 ч.)

Технологии обнаружения атак

Тема 14. Мониторинг в операционной системе Windows (2 ч.)

запуск утилиты и анализирования информации в ней

Тема 15. Мониторинг в операционной системе Windows (2 ч.)

Мониторинг ресурсов в операционной системе Windows

Тема 16. Мониторинг в операционной системе Linux (2 ч.)

знакомство с несколькими утилитами для мониторинга и анализ информации в них

5.3. Содержание дисциплины: Лекции (64 ч.)

Девятый семестр. (32 ч.)

Тема 1. Угрозы информационной системы. (2 ч.)

Угрозы информационной системы. Классификация угроз.

Тема 2. Уязвимости информационной системы. (2 ч.)

Классификации и реестры уязвимостей. База данных известных уязвимостей.

Тема 3. Типичный сценарий действий нарушителя. (2 ч.)

Типичный сценарий действий нарушителя. Математическая модель сценариев действий нарушителя по реализации угроз информационной безопасности.

Тема 4. Типичный сценарий действий нарушителя. (2 ч.)

Классификация сетевых атак. Технологии обнаружения атак и алгоритмы действий по их устранению. Признаки осуществления атаки

Тема 5. Признаки осуществления атаки. (2 ч.)

Показатели угроз безопасности на уровнях модели OSI. Безопасность сетевого уровня модели OSI. Защита компьютерных сетей на четырех уровнях модели ISO/OSI.

Тема 6. Признаки осуществления атаки. (2 ч.)

Принципы работы пакетных снифферов. Ограничения использования снифферов.Методы перехвата сетевого трафика. Ложные запросы ARP. Обзор программных пакетных снифферов.

Тема 7. Безопасность сетевого уровня модели OSI. (2 ч.)

Мониторинг безопасности беспроводных сетей. Защита беспроводных сетей на сетевом уровне. Выделение беспроводной сети в отдельный сегмент.
Использование IPSec для защиты трафика беспроводных клиентов (практика). Защита беспроводного сегмента с помощью L2TP. Применение
технологий VPN для защиты беспроводных сетей.

Тема 8. Безопасность сетевого уровня модели OSI. (2 ч.)

Определение типов систем обнаружения вторжений. Понятие обнаружения атак Узловые IDS.

Тема 9. Сетевые анализаторы и «снифферы». (2 ч.)

Распределённые атаки и их признаки. Классификация удаленных атак на распределенные вычислительные системы

Тема 10. Сетевые анализаторы и «снифферы». (2 ч.)

Компоненты и утилиты ОС для контроля состояния узла и сети

Тема 11. Мониторинг безопасности беспроводных сетей. (2 ч.)

Анализ защищённости на уровне ОС

Тема 12. Мониторинг безопасности беспроводных сетей. (2 ч.)

Этапы и средства реализации атак

Тема 13. Понятие обнаружения атак. (2 ч.)

Технологии обнаружения атак Признаки заражения компьютера вредоносными программами. Источники вредоносных программ. Методы обнаружения вредоносных программ. Антивирусные программы.

Тема 14. Понятие обнаружения атак. (2 ч.)

Журналы событий. Категории аудита безопасности. Проверка события входа в аккаунт.Проверка управления аккаунтом.Проверка доступа к службе каталогов.

Тема 15. Распределённые атаки и их признаки. (2 ч.)

Сортировка, группировка и фильтрация журналов событий. Диаграмма средней загрузки процессора. Диаграмма возникновения наиболее важных событий управления учетными записями.

Тема 16. Компоненты и утилиты ОС для контроля состояния узла и сети. (2 ч.)

Использование команды top. Использование команды vmstat. Использование команды w. Использование команды uptime. Использование команды ps
Использование команды free.

Десятый семестр. (32 ч.)

Тема 17. Мониторинг в операционной системе Linux (2 ч.)

Использование команды iostat. Использование команды sar. Использование команды mpstat.

Использование команды pmap. Использование команды iptraf. Использование команды tcpdump.

Тема 18. Сканер уязвимостей (2 ч.)

Типичные уязвимости прикладного уровня. Настройка и конфигурирование сканирования уязвимостей.

Тема 19. Сканер уязвимостей (2 ч.)

Чего не делает сканирование уязвимостей.

Тема 20. Сканер уязвимостей (2 ч.)

Как выполнить безопасное и этичное сканирование уязвимостей. Примеры конфигураций сканирования.

Тема 21. ПК «Сканер-ВС» (2 ч.)

ПК «Сканер-ВС». Назначение. Преимущества.

Тема 22. ПК «Сканер-ВС» (2 ч.)

Инвентаризация ресурсов сети.
Поиск уязвимостей.
Сетевой аудит стойкости паролей.
Подбор эксплойтов.
Перехват и анализ сетевого трафика.
Аудит беспроводных сетей.
Аудит обновлений ОС Windows.
Аудит ОС «Astra Linux Special Edition».

Тема 23. ПК «Сканер-ВС» (2 ч.)

Локальный аудит стойкости паролей.
Поиск остаточной информации.
Гарантированная очистка информации.
Аудит установленного аппаратного и программного обеспечения.
Функция сравнения отчетов позволяет отслеживать изменения конфигурации системы.
Контроль целостности.

Тема 24. ПАК «Рубикон-К» (2 ч.)

Принцип работы с сетевыми нтерфейсами на примере ПАК "Рубикон-К". Настройка сетевых интерфейсов для безопасного взаимодействия с сетью.

Тема 25. Аналитическая работа с СОА при помощи СУБД. (2 ч.)

Оператор SELECT; Проекция; Выбор; Соединения; Выбор столбцов; SQL-операторы; Заголовки столбцов; Использование арифметических операторов; Использование псевдонимов; Структура таблицы.

Тема 26. Аналитическая работа с СОА при помощи СУБД. (2 ч.)

Ограничение строк выборки; Символьные строки и даты в предложении WHERE; Операторы сравнения; Подстановочные символы; Идентификатор ESCAPE; Примеры сортировки. Функции SQL.

Тема 27. Аналитическая работа с СОА при помощи СУБД. (2 ч.)

Однострочные и многострочные функции; Символьные и числовые функции; Виды функций; Таблица DUAL; Работа с датами. Функции преобразования;

Тема 28. Аналитическая работа с СОА при помощи СУБД. (2 ч.)

Неявное и явное преобразование; Инструкции; Вложенные функции; Условное выражение CASE.

Тема 29. Подходы к организации экспертно-аналитической деятельности в центрах мониторинга. (2 ч.)

Центр мониторинга информационной безопасности
(Security Operation Center); Обзор методики CRAMM;
Обзор методологии COBIT for Risk.

Тема 30. Подходы к организации экспертно-аналитической деятельности в центрах мониторинга. (2 ч.)

Нормативное регулирование деятельности центров ГосСОПКА; подключение к ГосСОПКА; реагирование на инцидент
Реестр уязвимостей БДУ ФСТЭК России; MITRE
CVE и база данных NVD; OSVDB; Secunia Advisory and Vulnerability Database; VND от CERT/CC; Exploit Database.

Тема 31. Подходы к организации экспертно-аналитической деятельности в центрах мониторинга. (2 ч.)

Агрегаторы информации об уязвимостях. Автоматическое извлечение и сканирование файлов; Автоматическое назначение имени хоста и подсети;
CIDR подсети для сопоставления имени сегмента сети через конфигурационный файл.

Тема 32. Подходы к организации экспертно-аналитической деятельности в центрах мониторинга. (2 ч.)

Определение интерфейса имени хоста и имен подсетей CIDR; Elasticsearch; Способы установки Malcolm; Анализ конфигурации узлов сети; Исключения стандартов CIS

6. Виды самостоятельной работы студентов по дисциплине

Девятый семестр (28 ч.)

Вид СРС: Подготовка рефератов (28 ч.)

Тематика заданий СРС:

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.
Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.
Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.
Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата.
1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;

- культура письменного изложения материала;
- культура оформления материалов работы.

Тематика рефератов:
1. Нейронные сети как метод обнаружения атак
2. Имунные сети как метод обнаружения атак
3. Экспертные системы как метод обнаружения атак

Десятый семестр (8 ч.)

Вид СРС: Конспектирование текстов (8 ч.)

Тематика заданий СРС:

Представляет собой вид внеаудиторной самостоятельной работы студента по созданию обзора информации, содержащейся в объекте конспектирования, в более краткой форме. В конспекте должны быть отражены основные принципиальные положения источника, то новое, что внес его автор, основные методологические положения работы, аргументы, этапы доказательства и выводы. Ценность конспекта значительно повышается, если студент излагает мысли своими словами, в лаконичной форме. Конспект должен начинаться с указания реквизитов источника (фамилии автора, полного наименования работы, места и года издания).
Критерии оценки:
содержательность конспекта, соответствие плану;
отражение основных положений, результатов работы автора, выводов;
ясность, лаконичность изложения мыслей студента;
наличие схем, графическое выделение особо значимой информации;
соответствие оформления требованиям;
грамотность изложения;
конспект сдан в срок.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.
Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ПК-6 Способен проводить анализ безопасности компьютерных систем

Студент должен знать:

виды политик безопасности компьютерных систем и сетей

Вопросы, задания:

1. Разработать новые политики безопасности на основе различных применяемых для этого теоретических моделе
2. Основные виды политик управления доступом и информационными потоками.
3. Компьютерная реализация информационныз объектов.

Студент должен уметь:

выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации

Задания:

1. Сетевые анализаторы и «снифферы»
2. Анализ защищённости на уровне ОС
3. Мониторинг в операционных системах.

Студент должен владеть навыками:

разработки профиля защиты компьютерных систем

Задания:

1. Провести анализ защищённости на уровне ОС.
2. Компоненты и утилиты ОС для контроля состояния узла и сети.
3. Типичный сценарий действий нарушителя.

8.3. Вопросы промежуточной аттестации

Девятый семестр (Экзамен)

1. Угрозы информационной системе
2. Анализ защищённости на уровне ОС
3. Технологии обнаружения атак

Десятый семестр (Экзамен)

1. Компоненты и утилиты ОС для контроля состояния узла и сети
2. Распределённые атаки и их признаки
3. Мониторинг безопасности беспроводных сетей

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Девятый семестр

1. Контрольная работа - от 0 до 30 баллов
2. Устный опрос, собеседование - от 0 до 10 баллов
3. Письменные задания или лабораторные работы - от 0 до 60 баллов
4. Экзамен - от 0 до 40 баллов

Десятый семестр

1. Контрольная работа - от 0 до 30 баллов
2. Устный опрос, собеседование - от 0 до 10 баллов
3. Письменные задания или лабораторные работы - от 0 до 60 баллов

4. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Клименко Ирина Сергеевна Информационная безопасность и защита информации: модели и методы управления [Электронный ресурс]: научное - ИНФРА-М, 2020. - 180 с. - Режим доступа: http://new.znanium.com/go.php?id=1018665

9.2 Дополнительная литература

1. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум [Электронный ресурс]: учебное - Лань, 2020. - 44 с. - Режим доступа: https://e.lanbook.com/book/130179

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.edu.ru. - Федеральный портал «Российское образование»
2. http://elibrary.ru - Научная электронная библиотека

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:
- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Аудитория 2-24б К
Программное обеспечение:
1. Microsoft Windows 7 Professional, 11 лицензий, номер 60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
5. Microsoft Office 2016, 1 лицензия, Сублицензионный договор No 31604241628 от 21.11.16
6. LibreOffice 12 лицензий (свободно-распространяемое

программное обеспечение)
7. FreeBSD, 1 лицензия FreeBSD license свободное программное обеспечение
8. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное программное обеспечение
9. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL) свободное программное обеспечение
10. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение
11. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы (обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/
Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Аудитория 1-27 К
Специализированная мебель:
1. парта со скамьей – 40 шт.

2. учебные места – 80 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, меловая)
2. Мультимедийное оборудование
Аудитория 2-24б К
Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
3. парта со скамьей – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1