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

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование
дисциплины (модуля): **Расследование компьютерных инцидентов**

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:
Яриков В. Г., кандидат педагогических наук, доцент

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 - Формирование у студентов достаточных теоретических знаний и практических навыков по расследованию компьютерных инцидентов безопасности.

Задачи дисциплины:

- Знать методику и порядок расследования компьютерных инцидентов, инструментарий по расследованию компьютерных инцидентов. Основные признаки, источники данных для расследования компьютерных инцидентов.
- Уметь проводить организационные мероприятия при расследовании компьютерных инцидентов, подготовительные работы по расследованию компьютерных инцидентов, применять соответствующие программно-аппаратные средства, анализировать полученные результаты, оформлять результаты профессиональной деятельности в служебной документации, проводить расследования таргетированных атак.
- Владеть инструментальными средствами анализа инцидентов, навыками работы с документацией, заполнения отчетов, средствами защиты информации, инструментами анализа эффективности систем защиты информации

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Расследование компьютерных инцидентов» 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-5 Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов

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

Студент должен знать:

анализ существующей практики производства судебно-экспертных исследований компьютерных систем; базовые средства получения несанкционированного доступа к конфиденциальной информации; основные группы мер криминалистического предупреждения преступлений в сфере компьютерной информации; методики расследования компьютерных преступлений

Студент должен уметь:

применять специальные методы решения экспертных задач

Студент должен владеть навыками:

приемами типовых методических рекомендаций проведения экспертного исследования следов работы с операционными системами и компьютерными базами данных

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Девятый семестр
Контактная работа (всего)	**64**	**64**
Лабораторные	32	32
Лекции	32	32
Самостоятельная работа (всего)	**80**	**80**
Виды промежуточной аттестации		
Зачет с оценкой		+
Общая трудоемкость часы	**144**	**144**

Общая трудоемкость зачетные единицы	**4**	**4**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (32 ч.)

Девятый семестр. (32 ч.)

Тема 1. Понятие компьютерного инцидента. (2 ч.)

Основные термины и определения в области компьютерной криминалистики (форензики). Обзор федерального законодательства

Тема 2. Документальное оформление инцидентов. (2 ч.)

Принципы разработки документов для документального оформления инцидентов.

Тема 3. Угрозы безопасности информации и основные виды атак. (2 ч.)

Основные предпосылки для возникновения компьютерных инцидентов. Признаки компьютерного инцидента.

Тема 4. Угрозы безопасности информации и основные виды атак. (2 ч.)

Принципы информационной безопасности. Разновидности угроз информационной безопасности. Объективные уязвимости.

Тема 5. Основные меры по минимизации нанесенного ущерба. (2 ч.)

Анализ следов инцидентов с использованием утилит восстановления данных dd, testdisk и R.Saver.

Тема 6. Основные меры по минимизации нанесенного ущерба. (2 ч.)

Идентификация ущерба. Классификация ущерба. Количественная оценка ущерба.

Тема 7. Восстановление информации с использованием утилит dd, testdisk и R.Saver. (2 ч.)

Анализ следов инцидентов с использованием утилит восстановления данных dd, testdisk и R.Saver.

Тема 8. Деятельность организации Interpol по борьбе с международной компьютерной преступностью. (2 ч.)

Интерпол как международная организация. Понятие компьютерной преступности и ее виды. Классификация компьютерных преступлений по Интерполу.

Тема 9. Политики информационной безопасности: первый уровень организационно-распорядительных документов системы информационной безопасности (2 ч.)

Иерархическая структура документации по информационной безопасности. Первый уровень иерархической структуры документации по информационной безопасности.

Тема 10. Политики информационной безопасности: первый уровень организационно-распорядительных документов системы информационной безопасности (2 ч.)

Базовый набор частных политик ИБ. Проверка качества частной политики ИБ. Второй уровень иерархической структуры документации по
информационной безопасности.

Тема 11. Анализ дампов памяти с использованием Volatile и Windbg. (2 ч.)

Типы аварийных дампов памяти Windows. Анализ аварийного дампа памяти в WinDBG.

Тема 12. Управление инцидентами и событиями информационной безопасности. (2 ч.)

Этапы управления инцидентами и событиями ИБ. Обнаружение компьютерных атак. Анализ данных о событиях безопасности.

Тема 13. Управление инцидентами и событиями информационной безопасности. (2 ч.)

Реагирование на инциденты и ликвидация их последствий. Установление причин инцидентов. Анализ результатов устранения последствий инцидентов.

Тема 14. Реагирование на инциденты информационной безопасности в РФ (2 ч.)

Структура системы управления инцидентами. Определение инцидента и события информационной безопасности.

Тема 15. Реагирование на инциденты информационной безопасности в РФ (2 ч.)

Работа с инцидентами информационной безопасности. Стратегия по инцидент-менеджменту,

предлагаемая ГОСТом. Расследование инцидентов информационной безопасности сторонними силами.

Тема 16. Контроль состояния и конфигураций сетевых устройств с использование Efros Config Inspector и средства мониторинга Zabbix. (2 ч.)

Выявление атак злоумышленников. Проверка соответствия настроек оборудования требованиям безопасности.

5.2. Содержание дисциплины: Лабораторные (32 ч.)

Девятый семестр. (32 ч.)

Тема 1. Организация взаимодействия с персоналом, внешними организациями, правоохранительными органами. (2 ч.)

Цель работы: разработка документации при взаимодействии с персоналом, внешними организациями, правоохранительными органами.

Тема 2. Документальное оформление инцидентов. (2 ч.)

Цель работы: изучить основные принципы разработки документов для документального оформления инцидентов.

Тема 3. Документальное оформление инцидентов. (2 ч.)

Цель работы: разработка документов для документального оформления инцидентов.

Тема 4. Восстановление информации с использованием утилит dd, testdisk и R.Saver. (2 ч.)

Цель работы: анализ следов инцидентов с использованием утилит восстановления данных dd, testdisk и R.Saver.

Тема 5. Восстановление информации с использованием утилит dd, testdisk и R.Saver. (2 ч.)

Цель работы: ознакомиться с утилитой для восстановления поврежденных разделов или восстановления с них файлов.

Тема 6. Анализ журналов ОС и СрЗИ (2 ч.)

Цель работы: анализ следов инцидентов в журналах ОС и СрЗИ

Тема 7. Функциональные возможностей программы-анализатора сетевого трафика Wireshark при расследовании компьютерных преступлений (2 ч.)

Цель работы: научиться пользоваться основными функциональными возможностями программы Wireshark.

Тема 8. Анализ дампов памяти с использованием Volatile и Windbg. (2 ч.)

Цель работы: поиск и анализ следов инцидентов в дампах памяти ОС и приложений.

Тема 9. Анализ дампов памяти с использованием Volatile и Windbg. (2 ч.)

Цель работы: изучить типы аварийных дампов памяти Windows. Анализ аварийного дампа памяти в WinDBG.

Тема 10. Предотвращение компьютерных преступлений с помощью межсетевого экрана (2 ч.)

Цель работы: научиться пользоваться основными функциональными возможностями программы Netfilter.

Тема 11. Исследование дампов сетевого трафика с использованием Wireshark и TShark. (2 ч.)

Цель работы: изучить инструментарий и методику исследования. "Прослушивание" сетевого трафика.

Тема 12. Исследование дампов сетевого трафика с использованием Wireshark и TShark. (2 ч.)

Цель работы: выявление и анализ следов инцидентов с использованием снифера трафика WireShark

Тема 13. Программная реализация обнаружение заданной сетевой атаки для расследования компьютерных преступлений. (2 ч.)

Цель работы: требуется написать программу, которая в режиме непрерывного мониторинга

осуществляет обнаружение заданной сетевой атаки, автоматически реагирует на нее и сохраняет данные о подозрительной активности.

Тема 14. Контроль состояния и конфигураций сетевых устройств с использование Efros Config Inspector и средства мониторинга Zabbix. (2 ч.)

Цель работы: выявление и анализ изменений конфигурации и прошивок сетевых устройств.

Тема 15. Контроль состояния и конфигураций сетевых устройств с использование Efros Config Inspector и средства мониторинга Zabbix. (2 ч.)

Цель работы: выявление атак злоумышленников. Проверка соответствия настроек оборудования требованиям безопасности.

Тема 16. Обнаружение ARP-spoofing атаки для расследования компьютерных преступлений (2 ч.)

Цель работы: изучить методы обнаружения атаки ARP-spoofing.

6. Виды самостоятельной работы студентов по дисциплине

Девятый семестр (80 ч.)

Вид СРС: Работа с литературой (40 ч.)

Тематика заданий СРС:

Самостоятельная работа с учебниками и книгами, самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях – важнейшее условие формирования студентом у себя научного способа познания.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, хрестоматии и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления, в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание студент должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения, и приводить аналогичные примеры самостоятельно.

Полезно составлять опорные конспекты. При изучении материала по учебной книге полезно либо в тетради на специально отведенных полях, либо в документе, созданном на ноутбуке, планшете и др. информационном устройстве, дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем. Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

Список литературы:

1.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное - Москва:Форум : ИНФРА-М, 2016. - 416 с. - Режим доступа: http://znanium.com/go.php?id=549989

2.Руденков Н.А. Технологии защиты информации в компьютерных сетях [Электронный ресурс]: - Интуит НОУ, 2016. - 369 с. - Режим доступа: http://www.book.ru/book/918258

3.Мэйволд, Э. Безопасность сетей [Электронный ресурс]: учебное - Интуит НОУ, 2016. - 572 с. - Режим доступа: http://www.book.ru/book/917577

Вид СРС: Ознакомление с нормативными документами (40 ч.)

Тематика заданий СРС:

Ознакомление с нормативными документами по расследованию компьютерных инцидентов:

1.ГОСТ Р ИСО/МЭК 27001-2006

2. ГОСТ Р ИСО/МЭК ТО 18044-2007

3. ГОСТ Р ИСО/МЭК 17799-2005

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-5 Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов

Студент должен знать:

анализ существующей практики производства судебно-экспертных исследований компьютерных систем; базовые средства получения несанкционированного доступа к конфиденциальной информации; основные группы мер криминалистического предупреждения преступлений в сфере компьютерной информации; методики расследования компьютерных преступлений

Вопросы, задания:

1. Предупреждение инцидентов. Методы.

2. Оформление экспертизы. Виды документов. Порядок оформления.

3. Факторы, влияющие на успешную возможность расследования инцидента. Порядок снятия образов с жестких дисков.

Студент должен уметь:

применять специальные методы решения экспертных задач

Задания:

1. Провести анализ дампов сетевого трафика.

2. Провести анализ журналов сетевых устройств.

3. Порядок исследования сетевых признаков компьютерных инцидентов.

Студент должен владеть навыками:

приемами типовых методических рекомендаций проведения экспертного исследования следов работы с операционными системами и компьютерными базами данных

Задания:

1. Провести проверку файлов-образов виртуальных систем на предмет изменения системных данных.

2. Провести проверку файлов состояний виртуальных систем на предмет изменения системных данных.

3. Восстановить удаленные используя данные с файлов виртуальной памяти ОС.

8.3. Вопросы промежуточной аттестации

Девятый семестр (Зачет с оценкой)

1. Понятие компьютерного инцидента. Основные термины и определения в области компьютерной криминалистики.

2. Законодательство РФ в области компьютерных инцидентов.

3. Угрозы безопасности информации и основные виды атак. Факторы воздействия на информацию и последствия.

4. Основные предпосылки для возникновения компьютерных инцидентов. Признаки компьютерного инцидента.

5. Юридические предпосылки и меры для минимизации нанесенного ущерба.

6. Программно-технические меры для минимизации нанесенного ущерба.

7. Организационные мероприятия. Организация работы с персоналом.

8. Действия в случае возникновения компьютерного инцидента. Расследование компьютерных инцидентов в РФ.

9. Порядок взаимодействия с правоохранительными органами и сторонними организациями.

10. Технические мероприятия. Изъятие и исследование компьютерной техники и носителей информации. Виды документов.

11. Оформление экспертизы. Виды документов. Порядок оформления.

12. Предупреждение инцидентов. Методы.

13. Факторы, влияющие на успешную возможность расследования инцидента. Порядок снятия образов с жестких дисков.

14. Методы анализа образов жестких дисков. Выявление удаленных данных и шифрованных областей. Инструменты. Методы восстановления.

15. Методы анализа журналов ОС и безопасности. Инструменты.

16. Анализ памяти. Инструменты.

17. Анализ файлов виртуальной памяти ОС. Инструменты.

18. Анализ файлов-образов виртуальных систем, файлов состояний виртуальных систем. Инструменты.

19. Порядок исследования сетевых признаков компьютерных инцидентов.

20. Анализ конфигураций сетевых устройств. Инструменты.

21. Анализ журналов сетевых устройств. Инструменты.

22. Анализ дампов сетевого трафика. Основные протоколы. Инструменты.

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.

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное - Москва:Форум : ИНФРА-М, 2016. - 416 с. - Режим доступа: http://znanium.com/go.php?id=549989

2. Руденков Н.А. Технологии защиты информации в компьютерных сетях [Электронный ресурс]: - Интуит НОУ, 2016. - 369 с. - Режим доступа: http://www.book.ru/book/918258

9.2 Дополнительная литература

1. Мэйволд, Э. Безопасность сетей [Электронный ресурс]: учебное - Интуит НОУ, 2016. - 572 с. - Режим доступа: http://www.book.ru/book/917577

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. https://habr.com - Интернет- ресурс "Хабр"
2. http://elibrary.ru/ - Научная электронная библиотека
3. http://www.garant.ru/ - Гарант

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)

Программное обеспечение:
1. Windows 10 Профессиональная, 13 лицензий, номер 65946188.
2. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
3. Microsoft Office 2016, 14 лицензий, сублицензионный договор No31604241628 от 21.11.2016.
4. Oracle VM VirtualBox 15 лицензий GNU GPL свободное программное обеспечение
5. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
6. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745

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

Учебные аудитории для проведения занятий лекционного типа представляют собой специальные помещения, в состав которых входят специализированная мебель и технические средства обучения.

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

Учебные аудитории для проведения лабораторных работ представляют собой компьютерные классы или лаборатории, оснащенные лабораторным оборудованием, в зависимости от степени сложности.

Специализированная мебель:

1. компьютерные столы – 13 шт.
2. стулья – 29 шт.
3. парта – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.

Средства вычислительной техники (15 шт):

1. Компьютерный комплекс Option в составе: Системный блок
клавиатура, мышь, монитор (13 шт);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.

Сетевое оборудование:

1. Маршрутизатор ASUS WL-520GU.
2. Концентратор.

Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор projector DLP ColorBoost II
3. Экран для проектора Digis

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.