**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,**
**СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**
**(СПбГУТ)**

---

Кафедра Защищенных систем связи
(полное наименование кафедры)

СПбГУТ))) Документ подписан простой электронной подписью
Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

УТВЕРЖДАЮ
И.о.первого проректора
_____ С.И. Ивасишин
«01» 07 2022 г.

Регистрационный №_22.05/72-Д

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Эксплуатация уязвимостей программного обеспечения
(наименование дисциплины)

образовательная программа высшего образования

11.03.02 Инфокоммуникационные технологии и системы связи
(код и наименование направления подготовки / специальности)

бакалавр
(квалификация)

Защищенные системы и сети связи
(направленность / профиль образовательной программы)

очная форма
(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «11.03.02 Инфокоммуникационные технологии и системы связи», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 930, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

## 1. Цели и задачи дисциплины

Целью преподавания дисциплины «Эксплуатация уязвимостей программного обеспечения» является:

изучение студентом основных видов уязвимостей программного обеспечения, а также освоение основных методов и средств анализа и устранения уязвимостей программных реализаций.

Эта цель достигается путем решения следующих(ей) задач(и):

развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций; - формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности; - формирование навыков анализа программных реализаций на предмет наличия уязвимостей;

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Эксплуатация уязвимостей программного обеспечения» Б1.В.28 является дисциплиной части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «11.03.02 Инфокоммуникационные технологии и системы связи». Изучение дисциплины «Эксплуатация уязвимостей программного обеспечения» опирается на знании дисциплин(ы) «Защищенные операционные системы».

## 3. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 1

| № п/п | Код компетенции | Наименование компетенции |
|---|---|---|
| 1 | ПК-13 | Способен к администрированию процесса оценки производительности и контроля использования и производительности сетевых устройств, программного обеспечения информационно-коммуникационной системы |
| 2 | ПК-24 | Способен определять параметры безопасности и защиты программного обеспечения сетевых устройств |

Индикаторы достижения компетенций

Таблица 2

| | |
|---|---|
| ПК-13.1 | Знает архитектуру, общие принципы функционирования сетевых устройств и программного обеспечения администрируемой информационно-коммуникационной системы, протоколы всех модели взаимодействия открытых систем |
| ПК-13.2 | Знает метрики производительности администрируемой сети, модель ISO для управления сетевым трафиком, модели IEEE |
| ПК-13.3 | Умеет пользоваться нормативно-технической документацией в области инфокоммуникационных технологий, использовать современные методы контроля производительности инфокоммуникационных систем |

| | |
|---|---|
| ПК-13.4 | Умеет работать с контрольно-измерительными аппаратными и программными обеспечением; конфигурировать операционные системы сетевых устройств информационно-коммуникационной системы |
| ПК-13.5 | Владеет методами оценки требуемой производительности сетевых устройств и программного обеспечения администрируемой сети |
| ПК-13.6 | Владеет навыками установки кабельных и сетевых анализаторов для контроля изменения номиналов сетевых устройств и программного обеспечения администрируемой сети в целом и отдельных подсистем инфокоммуникационной системы |
| ПК-13.7 | Владеет навыками установки дополнительных программных продуктов для тарификации сетевых ресурсов и параметризации дополнительных программных продуктов для тарификации сетевых ресурсов |
| ПК-24.1 | Умеет выяснять приемлемые для пользователей параметры работы сети в условиях нормальной (обычной) работы (базовые параметры) |
| ПК-24.10 | Знает инструкции по установке администрируемых сетевых устройств |
| ПК-24.11 | Знает инструкции по эксплуатации администрируемых сетевых устройств |
| ПК-24.12 | Знает инструкции по установке администрируемого программного обеспечения |
| ПК-24.13 | Знает инструкции по эксплуатации администрируемого программного обеспечения |
| ПК-24.14 | Знает протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем |
| ПК-24.15 | Знает модель ISO для управления сетевым трафиком |
| ПК-24.16 | Знает модели IEEE |
| ПК-24.17 | Знает защищенные протоколы управления |
| ПК-24.18 | Знает основные средства криптографии |
| ПК-24.19 | Знает регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе |
| ПК-24.2 | Умеет применять аппаратные средства защиты сетевых устройств от несанкционированного доступа |
| ПК-24.20 | Знает требования охраны труда при работе с сетевой аппаратурой администрируемой сети |
| ПК-24.21 | Владеет навыками планирования защиты приложений от несанкционированного доступа |
| ПК-24.22 | Владеет навыками оценки безопасности и защиты приложений от несанкционированного доступа |
| ПК-24.23 | Владеет навыками планирования защиты операционных систем от несанкционированного доступа |
| ПК-24.24 | Владеет навыками оценки защиты операционных систем от несанкционированного доступа |
| ПК-24.3 | Умеет применять программные средства защиты сетевых устройств от несанкционированного доступа |
| ПК-24.4 | Умеет применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа |
| ПК-24.5 | Умеет пользоваться нормативно-технической документацией в области инфокоммуникационных технологий |
| ПК-24.6 | Знает общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети |
| ПК-24.7 | Знает архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети |
| ПК-24.8 | Знает классификацию операционных систем согласно классам безопасности |
| ПК-24.9 | Знает средства защиты от несанкционированного доступа операционных систем и систем управления базами данных |

## 4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

| Вид учебной работы | | Всего часов | Семестры |
|---|---|---|---|
| | | | 7 |
| Общая трудоемкость | 3 ЗЕТ | 108 | 108 |
| **Контактная работа с обучающимися** | | 50.25 | 50.25 |
| в том числе: | | | |
| Лекции | | 20 | 20 |
| Практические занятия (ПЗ) | | 16 | 16 |
| Лабораторные работы (ЛР) | | 14 | 14 |
| Защита контрольной работы | | | - |
| Защита курсовой работы | | | - |
| Защита курсового проекта | | | - |
| Промежуточная аттестация | | 0.25 | 0.25 |
| **Самостоятельная работа обучающихся (СРС)** | | 57.75 | 57.75 |
| в том числе: | | | |
| Курсовая работа | | | - |
| Курсовой проект | | | - |
| И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала | | 49.75 | 49.75 |
| Подготовка к промежуточной аттестации | | 8 | 8 |
| **Вид промежуточной аттестации** | | | Зачет |

## 5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 4

| № п/п | Наименование раздела дисциплины | Содержание раздела | № семестра | | |
|---|---|---|---|---|---|
| | | | очная | очно-заочная | заочная |
| 1 | Раздел 1. Анализ программных реализаций | Задача анализа программных реализаций. Метод экспериментов, статический метод, динамический метод. Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков. Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. Анализ потоков данных. Особенности анализа оверлейного кода, параллельного кода. Особенности анализа машинного кода в среде, управляемой сообщениями. | 7 | | |
| 2 | Раздел 2. Защита программ от исследования | Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение. Методы обфускации (запутывания программного кода). | 7 | | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Раздел 3. Программные закладки | Понятие программной закладки. Классификация программных закладок. Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам. Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя. | 7 | | |
| 4 | Раздел 4. Внедрение программных закладок | Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование. | 7 | | |
| 5 | Раздел 5. Противодействие программным закладкам | Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок. | 7 | | |
| 6 | Раздел 6. Компьютерные вирусы как особый класс программных закладок | Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода. | 7 | | |

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 5

| № п/п | Наименование обеспечиваемых (последующих) дисциплин |
|---|---|
| 1 | Защита операционных систем сетевых устройств |

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 6

| № п/п | Наименование раздела дисциплины | Лекции | Практ. занятия | Лаб. занятия | Семинары | СРС | Всего часов |
|---|---|---|---|---|---|---|---|
| 1 | Раздел 1. Анализ программных реализаций | 2 | 4 | | | 10 | 16 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | Раздел 2.<br>Защита программ от исследования | 2 | 4 | 4 | | 10 | 20 |
| 3 | Раздел 3.<br>Программные закладки | 6 | | 4 | | 10 | 20 |
| 4 | Раздел 4.<br>Внедрение программных закладок | 2 | 4 | 4 | | 5 | 15 |
| 5 | Раздел 5.<br>Противодействие программным закладкам | 4 | 4 | | | 9.75 | 17.75 |
| 6 | Раздел 6.<br>Компьютерные вирусы как особый класс программных закладок | 4 | | 2 | | 5 | 11 |
| | Итого: | 20 | 16 | 14 | - | 49.75 | 99.75 |

## 6. Лекции

Очная форма обучения

Таблица 7

| № п/п | Номер раздела | Тема лекции | Всего часов |
|---|---|---|---|
| 1 | 1 | Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. Анализ потоков данных. | 2 |
| 2 | 2 | Защита программ от исследования | 2 |
| 3 | 3 | Понятие программной закладки. Модель «наблюдатель» | 2 |
| 4 | 3 | Модель «перехват» | 2 |
| 5 | 3 | Модель «искажение» | 2 |
| 6 | 4 | Методы внедрения программных закладок | 2 |
| 7 | 5 | Методы выявления программных закладок | 2 |
| 8 | 5 | Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок | 2 |
| 9 | 6 | Бинарные вирусы Windows и Linux. . Сетевые вирусы. Скриптовые вирусы | 2 |
| 10 | 6 | Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению | 2 |
| | | Итого: | 20 |

## 7. Лабораторный практикум

Очная форма обучения

Таблица 8

| № п/п | Номер раздела | Наименование лабораторной работы | Всего часов |
|---|---|---|---|
| 1 | 2 | Знакомство с дизассемблером IDA | 4 |
| 2 | 3 | Знакомство с методами преодоления защиты программного кода от анализа. | 4 |
| 3 | 4 | Разработка и реализация программы, защищённой политикой безопасности, на объектно-ориентированном языке программирования Java. | 4 |
| 4 | 6 | Настройка и использование специализированного антивирусного программного обеспечения. | 2 |
| | | Итого: | 14 |

## 8. Практические занятия (семинары)

Очная форма обучения

Таблица 9

| № п/п | Номер раздела | Тема занятия | Всего часов |
|---|---|---|---|
| 1 | 1 | Анализ ядра Windows средствами Microsoft Debugging Tools. | 4 |
| 2 | 2 | Знакомство с отладчиками режима пользователя. | 4 |
| 3 | 4 | Программирование алгоритмов обфускации | 4 |
| 4 | 5 | Изолированная программная среда и программные ловушки. | 4 |
| | | Итого: | 16 |

## 9. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

## 10. Самостоятельная работа

Очная форма обучения

Таблица 10

| № п/п | Номер раздела | Содержание самостоятельной работы | Форма контроля | Всего часов |
|---|---|---|---|---|
| 1 | 1 | Изучение материалов лекции. Локализация и пресечение вирусных атак. | Отчет | 10 |
| 2 | 2 | Изучение материалов лекции. Программирование и внедрение закладок. | Отчет | 10 |
| 3 | 3 | Изучение материалов лекции. Знакомство с методами преодоления защиты программного кода от анализа. | Отчет | 10 |
| 4 | 4 | Изучение материалов лекции. Описание точек выполнения программы, в которых производится обращение к подсистеме безопасности на языке программирования AspectJ | Отчет | 5 |
| 5 | 5 | Изучение материалов лекции. Разработка и реализация на языке AspectJ соединительного модуля между программой и подсистемой безопасности в виде аспекта, унаследованного от абстрактного. | Отчет | 9.75 |
| 6 | 6 | Изучение материалов лекции. Компьютерные вирусы как особый класс программных закладок | Отчет | 5 |
| | | | Итого: | 49.75 |

## 11. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для самостоятельной работы по дисциплине рекомендовано следующее учебно-методическое обеспечение:

- Положение о самостоятельной работе студентов в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича;

- рекомендованная основная и дополнительная литература;
- конспект занятий по дисциплине;
- слайды-презентации и другой методический материал, используемый на занятиях;
- методические рекомендации по подготовке письменных работ, требования к их содержанию и оформлению (реферат, эссе, контрольная работа) ;
- фонды оценочных средств;
- методические указания к выполнению лабораторных работ для студентов;

## 12. Фонд оценочных средств для проведения промежуточной аттестации обучающихся

Фонд оценочных средств разрабатывается в соответствии с локальным актом университета "Положение о фонде оценочных средств" и является приложением к рабочей программе дисциплины.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Для каждого результата обучения по дисциплине определяются показатели и критерии оценки сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

- Вопросы для экзамена в количестве 20 шт
- КИМ в количестве 100шт

## 13. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

13.1. Основная литература:


1. Антивирусная защита компьютерных систем : [Электронный ресурс] : учебное пособие. - 2-е изд. - М. : ИНТУИТ, 2016. - 323 с. - URL: https://e.lanbook.com/book/100728. - Б. ц. Книга из коллекции ИНТУИТ - Информатика
2. Буйневич, Михаил Викторович. Защита программ и данных : учебное пособие / М. В. Буйневич, К. Е. Израилов, А. В. Красов ; рец.: И. В. Котенко, Е. В. Стельмашонок ; Федер. агентство связи, С.-Петерб. гос. ун-т телекоммуникаций

им. проф. М. А. Бонч-Бруевича. - СПб. : СПбГУТ. Ч. 2 : Способы защиты анализа. - 2020. - 52 с. : ил. - 279.41 р.

13.2. Дополнительная литература:

1. Штеренберг, Станислав Игоревич. Компьютерные вирусы : учебное пособие / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков ; рец.: Е. А. Вельмисов, Н. Н. Бабин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ. Ч. 1. - 2015. - 62 с. : ил. - 343.89 р.
2. Штеренберг, Станислав Игоревич.
Компьютерные вирусы : [Электронный ресурс] : лабораторный практикум / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков ; рец. Н. Н. Бабин ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2015. - 20 с. : ил. - 207.93 р.

## 14. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

- www.sut.ru
- lib.spbgut.ru/jirbis2_spbgut

## 15. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем.

15.1. Программное обеспечение дисциплины:

- GNU Assembler
- Linux
- Visual Studio Community
- Windows ИКСС

15.2. Информационно-справочные системы:

- ЭБС iBooks (https://ibooks.ru)
- ЭБС Лань (https://e.lanbook.com/)
- ЭБС СПбГУТ (http://lib.spbgut.ru)

## 16. Методические указания для обучающихся по освоению дисциплины

15.1. Планирование и организация времени, необходимого для изучения дисциплины

Важным условием успешного освоения дисциплины «Эксплуатация уязвимостей программного обеспечения» является создание системы правильной организации труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Все задания, включая вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующего аудиторного занятия (лекции, практического занятия), что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками.

Система университетского обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь, лекций и практических занятий), работа на которых обладает определенной спецификой.

15.2. Подготовка к лекциям

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета, как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная,

кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

15.3. Подготовка к практическим занятиям

Тщательное продумывание и изучение вопросов плана основывается на проработке пройденного материала (материала лекций, практических занятий), а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Необходимо понимать, что невозможно во время аудиторных занятий изложить весь материал из-за лимита аудиторных часов, и при изучении дисциплины недостаточно конспектов занятий. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

15.4. Рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание ученика на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это

сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информации может быть использована при написании текста реферата или другого задания.

Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам;
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, слова-описания общих понятий, разъяснения, примеры, толкования, «словотворчество»
- повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;
- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);
- использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не

хватает для выражения тех или иных коммуникативных намерений).

15.5. Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).

## 17. Материально-техническое обеспечение дисциплины

Таблица 11

| № п/п | Наименование специализированных аудиторий и лабораторий | Наименование оборудования |
|---|---|---|
| 1 | Лекционная аудитория | Аудио-видео комплекс |
| 2 | Аудитории для проведения групповых и практических занятий | Аудио-видео комплекс |
| 3 | Компьютерный класс | Персональные компьютеры |
| 4 | Аудитория для курсового и дипломного проектирования | Персональные компьютеры |
| 5 | Аудитория для самостоятельной работы | Компьютерная техника |
| 6 | Читальный зал | Персональные компьютеры |
| 7 | Лаборатория программно-аппаратных средств обеспечения информационной безопасности | Лабораторные стенды (установки)<br>Контрольно-измерительные приборы |

Лист изменений № 1 от 9 января 2020 г

Рабочая программа дисциплины
**«Эксплуатация уязвимостей программного обеспечения»**

Код и наименование направления подготовки/специальности:
**11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность/профиль образовательной программы:
**Защищенные системы и сети связи**

---

Из п. 14.2 Информационно-справочные системы исключить с 08.01.2020 г. строку: ЭБС IPRbooks (http://www.iprbookshop.ru)

Основание: прекращение контракта № 4784/19 от 25.01.2019 г. на предоставление доступа к электронно-библиотечной системе IPRbooks.

Внесенные изменения утверждаю:

Начальник УМУ _____ Л.А. Васильева