МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Компьютерная вирусология»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В.Ильин
старший преподаватель С.О. Иванов

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информационных систем
«30» августа 2017г., протокол №1

заведующий кафедрой Д.В. Ильин

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета А.В. Щипцова

Директор научной библиотеки Н.Д. Никитина

Начальник управления информатизации И.П. Пивоваров

Начальник учебно-методического управления В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Целью дисциплины является изучение вредоносного кода и средств борьбы с ним.

Основными задачами дисциплины являются изучение:

- принципов работы вредоносного кода и защиты от него;
- изучение имеющихся средств антивирусной защиты;
- правильное реагирование на заражение вредоносным кодом и ликвидация последствий.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина относится к числу обязательных дисциплин вариативной части.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Технологии и методы программирования», «Системное программное обеспечение», «Основы информационной безопасности».

Дисциплина является предшествующей для производственных и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
- способность проводить анализ защищенности автоматизированных систем (ПК-3);
- способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
- способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- структуру вредоносного кода (З1);
- уязвимости и пути распространения вредоносного кода (З2);
- принцип работы средств борьбы с вредоносным кодом (З3);
- возможности существующих антивирусных средств (З4);

уметь:

- классифицировать вредоносный код и последствий его работы (У1);
- выявлять и анализировать вредоносный код (У2);
- защищать и восстанавливать компьютерную систему от действий вредоносного кода (У3);
- применять различные антивирусные средства в зависимости от задач (У4);

владеть навыками:

- методами обнаружения и устранения вредоносного кода (Н1);
- применять инструментальные средства и утилиты для проверки компьютерной системы (Н2);
- написания программ устойчивых к вредоносному воздействию (Н3);
- настройки и применения антивирусных средств для обнаружения и устранения вирусов (Н4).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Вредоносный код	ОПК-3	З1, У1, Н1
Тема 1.1 Основные понятия.		
Тема 1.2 Функции вредоносного кода		
Раздел 2. Противодействие вредоносному коду	ПК-3, ПК-10	З2,У2,Н2, З3,У3,Н3
Тема 2.1 Исследование вредоносного кода		
Тема 2.2 Способы борьбы с вредоносным кодом		
Раздел 3. Средства защиты от вредоносного кода	ПК-25	З4,У4,Н4
Тема 3.1. Антивирусные сканеры.		
Тема 3.2. Средства изоляции приложений		
Зачет	ПК-3, ПК-10, ПК-25	З2,У2,Н2, З3,У3,Н3,З4,У4,Н4

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час
		Л	л/р	п/р	КСР		
Раздел 1. Вредоносный код							
Тема 1.1 Основные понятия.	8	2	2	2		2	
Тема 1.2 Функции вредоносного кода	16	4	4	4		4	4
Раздел 2. Противодействие вредоносному коду							
Тема 2.1 Исследование вредоносного кода	16	4	4	4		4	4
Тема 2.2 Способы борьбы с вредоносным кодом	12	2	2	2		6	
Раздел 3. Средства защиты от вредоносного кода							
Тема 3.1. Антивирусные сканнеры.	8	2	2	2		2	
Тема 3.2. Средства изоляции приложений	8	2	2	2		2	
Зачет	4				2	2	
Итого	72 2 з.е.	16	16	16	2	22	8

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Вредоносный код

Тема 1.1 Основные понятия.

Лекция 1. Вирусы и зловреды.

1. Определение зловредного кода.
2. Классификация зловредов.
3. История вирусов.

Практическое занятие 1. Энциклопедия вирусов.

Тема 1.2 Функции вредоносного кода

Лекция 2. Вредоносное воздействие на компьютерную систему

1. Порча данных.
2. Взлом и перехват информации.
3. Блокирование работы компьютера.
4. Шуточные действия.

Практическое занятие 2. Анатомия компьютерного вируса.

Лекция 3. Способы распространения вредоносного.

1. Автозапуск вредоносного кода.
2. Внедрение в чужой код.
3. Захват привилегий.
4. Способы маскирования.

Практическое занятие 3. Правила безопасной работы пользователя.

Раздел 2. Противодействие вредоносному коду.

Тема 2.1 Исследование вредоносного кода.

Лекция 4. Анализ компьютера на вредоносный код.

1. Признаки появления вирусов.
2. Контроль процессов и служб.
3. Отслеживание потоков данных.

Практическое занятие 4. Изучение следов работы вируса.

Лекция 5. Анализ программ.

1. Статический анализ кода.
2. Динамический анализ программ.

Практическое занятие 5. Дизассемблирование и изучение исполняемого кода.

Тема 2.2 Способы борьбы с вредоносным кодом.

Лекция 6. Устранение вирусов.

1. Устранение источников вредоносного кода.
2. «Лечение» программ и удаление «остатков» вредоносного кода.
3. Исправление конфигурации компьютерной системы.

Практическое занятие 6. Устранение Trojan-Ransom.

Раздел 3. Средства защиты от вредоносного кода.

Тема 3.1. Антивирусные сканнеры.

Лекция 7. Антивирусы.

1. Принципы обнаружения и устранения вирусов.
2. Режимы функционирования антивируса.
3. Обеспечение правильной работы антивируса.

Практическое занятие 7. Рейтинги антивирусного ПО.

Тема 3.2. Средства изоляции приложений.

Лекция 8. Песочницы и контейнеры.

1. Основные понятия и определения.
2. Принцип работы.
3. Анализ поведения изолированного приложения.

Практическое занятие 8. Изучение вирусов в песочнице.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторная работа 1. Открытый антивирус ClamAV.	2
Лабораторная работа 2. Бесплатные антивирусы: Avast! Free Antivirus, Avira Free Security Suite, 360 Total Security.	4
Лабораторная работа 3. Корпоративный антивирус Kaspersky Endpoint security.	2
Лабораторная работа 4. Проверочные антивирусы: Dr.Web CureIt.	2

Лабораторная работа 5. «Спасательные» антивирусы: Kaspersky Rescue Disk.	2
Лабораторная работа 6. Специальные антивирусы: AVZ.	2
Лабораторная работа 7. Онлайн антивирусы: Virustotal.com.	2
Итого	16

5.3. Вопросы для самостоятельной работы студента.

1. Загрузочные вирусы.
2. Руткиты и бекдоры.
3. Сетевые черви.
4. Троянские программы.
5. Шифровальщики.
6. Макро-вирусы.
7. Полиморфные вирусы.
8. Рекламное, подозрительное и назойливое поведение программ.
9. Псевдо-антивирусы.
10. Антивирусные комплексы.
11. Угрозы нулевого дня
12. Вирусные эпидемии.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской).

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;

– практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

– лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного

выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Компьютерные вирусы. Основные определения.
2. Классификация компьютерные вирусы.
3. Симптомы заражения.
4. Обзор способов заражения компьютерных систем.
5. Открытые антивирусные программы, примеры.
6. Бесплатные антивирусные программы, примеры.
7. Корпоративные антивирусные программы, примеры.
8. Особенности антивирусных программы
9. История зарождения вируса.
10. Вредоносное воздействие на компьютерную систему.
11. Блокировка компьютера вирусом. Как снять блокировку с компьютера.
12. Способы распространения вирусов.
13. Правила безопасной работы пользователя на компьютере.
14. Способы устранения вирусов.
15. Исправление конфигурации компьютерной системы.
16. Устранение вирусов-вымогателей.
17. Режимы функционирования вирусов.
18. Обеспечение правильной работы антивируса.
19. Песочница. Основные понятия и определения.
20. Песочница. Принципы работы.
21. Проверочные антивирусные программы. Определение и пример.
22. «Спасательные» антивирусные программы. Определение и пример.
23. Специальные антивирусные программы. Определение и пример.
24. Онлайн антивирусы.
25. Способы скрытия признаков вируса.
26. Перечислите основные методы профилактики заражения.

7.2. Оценивание результатов зачета

Оценивание результатов зачета

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания в течение семестра, имеются твердые и полные знания программного материала, правильные действия по применению знаний на практике, четкое изложение материала

Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания в течение семестра, либо наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература.

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Ермаков Д.Г. Применение антивирусных программ для обеспечения информационной безопасности [Электронный ресурс] / Д.Г. Ермаков, А.В. Присяжный. — Электрон. текстовые данные. — Екатеринбург: Уральский федеральный университет, 2013. — 64 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66577.html
2.	Гошко С.В. Технологии борьбы с компьютерными вирусами [Электронный ресурс] / С.В. Гошко. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2009. — 351 c. — 978-5-91359-059-6. — Режим доступа: http://www.iprbookshop.ru/8721.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс] / Крис Касперски. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2010. — 446 c. — 5-93455-175-2. — Режим доступа: http://www.iprbookshop.ru/65405.html
2.	Ташков П. А. Защита компьютера на 100%: сбои, ошибки и вирусы / Ташков П. А. - СПб.: Питер, 2011. - 282с.: ил. - (На 100%). - ISBN 978-5-49807-697-3. 6+2+1

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Windows/ Gentoo linux	лицензия университета/ свободное лицензионное соглашение (https://www.gentoo.org/downloads/)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Антивирус	лицензия университета/ свободное лицензионное соглашение (https://www.clamav.net/downloads)

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru

2.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
3.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
4.	Xgu.ru.	http://xgu.ru/wiki/
5.	Российская Государственная Библиотека	http://www.rsl.ru
6.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
7.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
8.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
9.	Научная электронная библиотека	http://elibrary.ru
10.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
11.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.