

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»  
Институт математики, физики и информационных технологий  
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:  
Директор института



Н. Л. Королева  
«05» июля 2021 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.О.33 Защита программ и данных

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

**Автор программы:**

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «26» ноября 2020 г. № 1461).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	4
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	8
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	22
6. Учебно-методическое и информационное обеспечение дисциплины.....	24
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	24

## 1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-3 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- эксплуатационный

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-3 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	Проводит инструментальный мониторинг защищенности компьютерных систем, сетей через анализ программ и данных

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-3 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		4	6	7	8
1	"Networksecurity"	+			
2	Анализ защищенности компьютерных сетей	+			
3	Безопасность компьютерных сетей	+			
4	Ознакомительная практика		+		
5	Системы и сети передачи информации			+	+

## 2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Защита программ и данных» относится к обязательной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Защита программ и данных» изучается в 9 семестре.

### 3.Объем и содержание дисциплины

3.1.Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>108</b>
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
9 семестр					
1	Классификация компьютерных вирусов.	4	5	7	Внеаудиторная самостоятельная работа. (Лабораторная работа); Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)
2	Среда обитания и алгоритмы вирусов.	8	7	10	Внеаудиторная самостоятельная работа. (Лабораторная работа); Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)

3	Троянские программы.	8	8	10	Внеаудиторная самостоятельная работа. (Лабораторная работа); Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)
4	Вымогательство в сети Интернет	7	7	10	Внеаудиторная самостоятельная работа. (Лабораторная работа); Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)
5	Методы обнаружения и удаления компьютерных вирусов.	5	5	7	Внеаудиторная самостоятельная работа. (Лабораторная работа); Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)

### Тема 1. Классификация компьютерных вирусов. (ПК-3)

#### Лекция.

Определение вируса. Проблемы антивирусной защиты информации. Вирусы и их классификация.

#### Лабораторные работы.

Антивирусное решение Avast! Free Antivirus.

#### Задания для самостоятельной работы.

1. Установите программный продукт.
2. Выберите способ сканирования. Сканируйте компьютер на наличие вредоносных объектов.
3. Просмотрите отчет о сканировании. Настройте уровень сканирования в реальном времени.
4. Настройте функции Avast!, выполняющиеся в «облаке». Включите автоматический режим «AutoSandbox».
5. Сгенерируйте пакет поддержки.

### Тема 2. Среда обитания и алгоритмы вирусов. (ПК-3)

#### Лекция.

Среда обитания вирусов (файловые; загрузочные; макро; сетевые). Особенности алгоритмов работы вирусов (резидентность; использование стелс-алгоритмов; самошифрование и полиморфичность; использование нестандартных приемов).

Деструктивные возможности вирусов (безвредные; неопасные; опасные вирусы; очень опасные). Загрузочные вирусы. Алгоритм работы загрузочного вируса. Файловые вирусы. Способы заражения. Алгоритм работы файлового вируса. Макро-вирусы. Word/Excel/Office-вирусы. Алгоритм работы Word макро-вирусов. Алгоритм работы Excel и Access макро-вирусов. Полиморфизм-вирусы. Полиморфные расшифровщики. Уровни полиморфизма. Изменение выполняемого кода. Стелс-вирусы.

#### **Лабораторные работы.**

Комплексная система защиты - Outpost Security Suite Pro.

#### **Задания для самостоятельной работы.**

1. Установите программный продукт Outpost Security Suite Pro.
2. Настройте программу. Включите функцию «Эвристический анализ». Добавьте программу Dr. Web в список исключений Антивируса.
3. Установите глобальные правила блокировки. Защитите паролем приложение Outpost Security Suite Pro.

### **Тема 3. Троянские программы. (ПК-3)**

#### **Лекция.**

Программы шпионы, программные закладки. «Вредные программы». Хакерские утилиты удаленных компьютеров («backdoor»). Возможности утилит скрытого администрирования. Троянские кони (логические бомбы) и их деструктивные действия. Программы-шпионы. «Intended»-вирусы. Конструкторы вирусов и полиморфизм-генераторы. «Злые шутки» (hoax). Программы-шпионы. Клавиатурные шпионы. Модели программ-шпионов. Программные закладки. Программный шпионаж.

#### **Лабораторные работы.**

Проверка сертификата сетевой безопасности.

#### **Задания для самостоятельной работы.**

1. Проверьте безопасность соединения в Google Chrome, Opera, Mozilla Firefox. Определите отсутствия безопасного соединения.
2. Выделите способы проникновения программ-вымогателей в устройство пользователя. Сформируйте основные меры предупреждения заражения программами-вымогателями.

### **Тема 4. Вымогательство в сети Интернет (ПК-3)**

#### **Лекция.**

Вымогательство. Жертвы вымогательства (посетители брачных онлайн-салонов, сайтов знакомств, интернет-салонов, поисковых ресурсов). Вымогательство и вредоносные (тройные) программы.

#### **Лабораторные работы.**

Поиск и блокирование конфиденциальных данных на основе программного решения DLP Lite.

#### **Задания для самостоятельной работы.**

1. Подготовьте доклад по тенденциям развития вымогательства в сети.
2. Выделите способы проникновения программ-вымогателей в устройство пользователя. Сформируйте основные меры предупреждения заражения программами-вымогателями.
3. Выделите, что необходимо делать если вы все же стали жертвой мошенников.

### **Тема 5. Методы обнаружения и удаления компьютерных вирусов. (ПК-3)**

#### **Лекция.**

Способы противодействия компьютерным вирусам. Обезвреживание и удаление известного вируса. Способы обнаружения и удаления неизвестного вируса. Обнаружение резидентного вируса. Windows-вирусы. Обнаружение файлового вируса. Обнаружение макро-вируса.

### Лабораторные работы.

Блокирование нежелательных объектов на основе Adguard.

### Задания для самостоятельной работы.

1. Установите программный продукт Adguard. Включите пользовательский фильтр антибаннера.
2. Включите модуль «Родительский контроль».
3. Сообщите о рекламе.

## 4. Контроль знаний обучающихся и типовые оценочные средства

### 4.1. Распределение баллов:

9 семестр

- посещаемость – 10 баллов
- текущий контроль – 71 балл
- контрольные срезы – 2 среза: 10 баллов, 9 баллов
- премиальные баллы – 20 баллов

### Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Классификация компьютерных вирусов.	Внеаудиторная самостоятельная работа. (Лабораторная работа)	10	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы. 1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.



		<p>Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)</p>	<p>8</p> <p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>8 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>3 балла – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>1 балл - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
--	--	---	---

2.	Среда обитания и алгоритмы вирусов.	Внеаудиторная самостоятельная работа. (Лабораторная работа)	10	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
----	-------------------------------------	---	----	--

		<p>Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)</p>	<p>8</p> <p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>8 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>3 балла – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>1 балл - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
--	--	---	---

3.	Троянские программы.	Внеаудиторная самостоятельная работа. (Лабораторная работа)	10	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
----	----------------------	---	----	---

		<p>Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)</p>	<p>8</p> <p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>8 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>3 балла – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>1 балл - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
--	--	---	---

4.	Вимогательств о в сети Интернет	Внеаудит орная самостоят ельная работа. (Лаборато рная работа)	7	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>7 баллов – лабораторная работа выполнена в полном объёме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
----	---------------------------------------	---	---	---

		<p><b>Выступление с докладом . Внеаудиторная самостоятельная работа. (Доклад) (контрольный срез)</b></p>	<p>10</p> <p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику. Основные качества доклада подлежащего оценке:  10 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.  3 балла – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.  1 балл - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
--	--	--	--

5.	Методы обнаружения и удаления компьютерных вирусов.	<b>Внеаудиторная самостоятельная работа. (Лабораторная работа)(контрольный срез)</b>	9	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>9 баллов – лабораторная работа выполнена в полном объёме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>2 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
----	---	--	---	---



		<p>Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)</p>	<p>10</p> <p>Доклад студента предполагает организацию совместной дискуссии автора, преподавателя и студентов по вопросам, связанных с определенным разделом, проблеме или способе реализации т.п. После доклада все члены группы активно участвуют в обсуждении, добавляют информацию, задают вопросы и делают замечания докладчику.</p> <p>Основные качества доклада подлежащего оценке:</p> <p>6 баллов – четко сформулированы проблемы, соответствующая теме доклада; полнота раскрытия материала темы доклада; в основной части логично, связно и полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; нет замечаний по презентационному материалу; правильно используются и приведены авторитетные источники информации; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>10 баллов – четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; в основной части полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; заключение содержит выводы, логично вытекающие из содержания основной части; есть замечания по презентационному материалу; выполнена задача заинтересованности слушателей в группе, активная дискуссия среди студентов при обсуждении доклада.</p> <p>6 баллов - четко сформулированы проблемы, соответствующая теме доклада; достаточно раскрыта тема доклада; недостаточно полно рассмотрены решения проблемы; деление презентации на введение, основную часть и заключение; есть замечания по презентационному материалу; слабо выполнена задача заинтересованности слушателей в группе.</p>
--	--	---	--

6.	Посещаемость	10	10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.
7.	Премияльные баллы	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции
8.	Итого за семестр	100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

#### 4.2 Типовые оценочные средства текущего контроля

##### **Внеаудиторная самостоятельная работа. (Лабораторная работа)**

##### Тема 1. Классификация компьютерных вирусов.

##### **Лабораторная работа №1. ZoneAlarmInternetSecurity 2012**

##### **Контрольные задания**

- 1 Включите функцию автоматического отключения интернета
- 2 Настройте антивирус так, чтобы ежемесячно во вторник сканировались все жесткие диски.
- 3 Просканируйте систему и выведите отчет о сканировании в файл
- 4 Включите функцию защиту браузера.
- 5 Настройте антивирус так, чтобы он блокировал интернет-сервисы
- 6 Выполните полную проверку локального диска С, при этом сканировались только системные файлы и объекты в системной памяти. После сканирования зараженные объекты поместите в карантин.
- 7 Проверьте обновление данной программы и базы вредоносных программ

##### Тема 2. Среда обитания и алгоритмы вирусов.

##### **Лабораторная работа №2. Panda Internet Security 2012**

##### **Контрольные задания**

- 1 Установить порты или зоны, которые могут использоваться программами для установки соединений.
- 2 Активировать/настроить параметры антиспамовой защиты.
- 3 Установить и активизировать модуль резервных копий.

- 4 Отключить автоматическую защиту от известных угроз.
- 5 Отправить файл в вирусную лабораторию.
- 6 Активизировать защиту от мошенничества.
- 7 Создать резервные копии файлов с помощью PandaInternetSecurity 2012.
- 8 Настроить защиту конфиденциальной информации(номер счета).
- 9 Настроить брандмауэр, чтобы пользоваться папками совместного доступа, расположенными на других сетевых компьютерах.
- 10 Проверить файлы с расширением \*.zip и вывести отчет.
- 11 Проверить входящие электронные сообщения.
- 12 Добавить WWW.USAFIS.ORG в список ненадежных URL
- 13 Используя родительский контроль примените фильтр для пользователя student, когда он входит в интернет.
- 14 Запретить принимать входящие сообщения и отправлять исходящие сообщения приложению Mail.ru Агент.

### Тема 3. Троянские программы.

#### Лабораторная работа №3.eScanAntiVirusEdition

##### Контрольные задания

- 1 Произвести сканирование локальных дисков.
- 2 Произвести сканирование рабочего стола.
- 3 Запланируйте проверку съемных носителей ежедневно 12:00.
- 4 Определите сканируемые типы файлов DOC, EXE, JPEG, MP3.
- 5 Защитить настройки антивируса паролем.
- 6 Запретить доступ к исполняемым файлам на usb носителях.
- 7 Заблокируйте приложение InternetExplorer.
- 8 Настройте защиту папки «Мои документы» от изменения или удаления файлов.
- 9 С помощью брандмауэра антивируса заблокируйте весь сетевой трафик.
- 10 С помощью почтового антивируса заблокируйте вложения типа \*.rar.
- 11 Удалить программный продукт.

### Тема 4. Вымогательство в сети Интернет

#### Лабораторные работа 4. Avira Premium Security Suite

##### Контрольные задания

- 1 Заблокируйте все сетевые подключения.
- 2 Установить высокий приоритет процесса сканирования.
- 3 Осуществить целенаправленный поиск Rootkit.
- 4 Заблокируйте подключение к удаленному рабочему столу.
- 5 Защитите настройки паролем.
- 6 Отмените сканирование исходящей электронной почты
- 7 Запустить программу и проверить любую папку на вирусы из командной строки
- 8 Задать приоритет сканирования
- 9 Исключить проверку папки – «Help»,при сканировании папки – «Windows».
- 10 Установить пароль от изменения другими пользователями настроек данного антивируса

### Тема 5. Методы обнаружения и удаления компьютерных вирусов.

#### Лабораторная работа 5. TheBat! PrivateDisk

##### Контрольные задания

- 1 Установите PrivateDisk на съемный диск.
- 2 Включите автоматическую загрузку программы.
- 3 Установите режим проверки наличия открытых файлов перед отключением диска.
- 4 Создайте виртуальный зашифрованный диск: R объёмом 5 Гб.
- 5 Создайте резервную копию ключа шифрования.
- 6 Восстановите ключ шифрования виртуального зашифрованного диска с резервной копии.

### **Выступление с докладом. Внеаудиторная самостоятельная работа. (Доклад)**

#### Тема 1. Классификация компьютерных вирусов.

Определение вируса. Проблемы антивирусной защиты информации. Вирусы и их классификация.

#### Тема 2. Среда обитания и алгоритмы вирусов.

Среда обитания вирусов (файловые; загрузочные; макро; сетевые). Особенности алгоритмов работы вирусов (резидентность; использование стелс-алгоритмов; самошифрование и полиморфичность; использование нестандартных приемов). Деструктивные возможности вирусов (безвредные; неопасные; опасные вирусы; очень опасные). Загрузочные вирусы. Алгоритм работы загрузочного вируса. Файловые вирусы. Способы заражения. Алгоритм работы файлового вируса. Макро-вирусы. Word/Excel/Office-вирусы. Алгоритм работы Word макро-вирусов. Алгоритм работы Excel и Access макро-вирусов. Полиморфик-вирусы. Полиморфные расшифровщики. Уровни полиморфизма. Изменение выполняемого кода. Стелс-вирусы.

#### Тема 3. Троянские программы.

Программы шпионы, программные закладки. “Вредные программы”. Хакерские утилиты удаленных компьютеров (“backdoor”). Возможности утилит скрытого администрирования. Троянские кони (логические бомбы) и их деструктивные действия. Программы- шпионы. “Intended” – вирусы. Конструкторы вирусов и полиморфик-генераторы. “Злые шутки” (hoax). Программы- шпионы. Клавиатурные шпионы. Модели программ-шпионов. Программные закладки. Программный шпионаж.

#### Тема 4. Вымогательство в сети Интернет

Вымогательство. Жертвы вымогательства (посетители брачных онлайн-салонов, сайтов знакомств, интернет-салонов, поисковых ресурсов). Вымогательство и вредоносные (троянские) программы.

#### Тема 5. Методы обнаружения и удаления компьютерных вирусов.

Способы противодействия компьютерным вирусам. Обезвреживание и удаление известного вируса. Способы обнаружения и удаления неизвестного вируса. Обнаружение резидентного вируса. Windows-вирусы. Обнаружение файлового вируса. Обнаружение макро-вируса.

#### 4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

### **Типовые вопросы зачета (ПК-3)**

1. Определение компьютерного вируса.

2. Классификация компьютерных вирусов.
3. Отличительные черты файловых вирусов.
4. Сравнительные характеристики различных файловых вирусов.
5. Способы заражения файловыми вирусами.
6. Принцип размножения файловых червей.
7. Link- вирусы. OBJ и LVB вирусы.
8. Алгоритм работы файловых вирусов.
9. Отличительные черты загрузочных вирусов.
10. Алгоритм работы загрузочных вирусов.
11. Актуальность загрузочных вирусов.
12. Опасность загрузочного вируса.
13. Макро-вирус как особая разновидность вируса.
14. Алгоритм работы макро- вирусов.
15. Отличительные черты полиморфных вирусов.
16. Уровни полиморфизма.
17. Полиморфизм макро- вирусов.
18. Отличительные особенности стелс вирусов.
19. Способы маскировки стелс-вирусов.
20. Стелс - алгоритм в макро- вирусах.
21. Отличительные черты сетевых вирусов- “червей”.
22. Способы проникновения сетевого вируса в компьютерную систему
23. Алгоритм работы сетевых вирусов.
24. Отличительные черты различных типов троянских коней.
25. Классифицируйте троянские кони.
26. Почтовые троянские программы.
27. Утилиты удаленного управления компьютером (backdoor).
28. Алгоритм работы захватчиков.
29. Основные причины распространенности троянских программ.
30. Программные закладки.
31. Модели воздействия программных закладок на компьютер.
32. Деструктивные действия программных закладок.
33. Способы противодействия компьютерным вирусам.
34. Обезвреживание и удаление известного вируса.
35. Способы обнаружения и удаления неизвестного вируса.
36. Обнаружение резидентного вируса.
37. Обнаружение Windows-вирусов.
38. Обнаружение файлового вируса.
39. Обнаружение макро-вируса.
40. Профилактика вирусного заражения и уменьшение предполагаемого ущерба.
41. Методы защиты от клавиатурных шпионов.
42. Меры противодействия программам шпионам.
43. Антивирусные программы. Типы антивирусов.
44. Методика использования антивирусных программ.
45. Профилактика заражения компьютера. Основные правила защиты.
46. Проблема защиты от макро-вирусов.
47. Восстановление пораженных объектов.
48. Защита от программных закладок.
49. Рейтинг антивирусных программных средств. Прогнозы.
50. Требования к антивирусным программам.

### Типовые задания для зачета (ПК-3)

1. Определение компьютерного вируса.
2. Перечислите виды инсайдеров.
3. Алгоритм работы макро- вирусов.
4. Почтовые троянские программы
5. Профилактика заражения компьютера. Основные правила защиты.
6. Отличительные особенности детских браузеров.
7. Методы блокирования нежелательного контента.
8. Юридические механизмы нежелательного контента.
9. Надежные торговые платформы.
10. Понятие кибербуллинга.
11. Методы противодействия фишингу.
12. Классификация антивирусных программных решений.
13. Типы интернет-зависимости для различных групп пользователей.
14. Методы борьбы с манипуляторами.

#### 4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-3	На высоком уровне владеет методами защиты программ и данных от постороннего воздействия. Способен администрировать средства защиты программ данных прикладного и системного программного обеспечения.
«не зачтено» (0 - 49 баллов)	ПК-3	Не владеет методами защиты программ и данных от постороннего воздействия. Не способен администрировать средства защиты программ данных прикладного и системного программного обеспечения.

### 5. Методические указания для обучающихся по освоению дисциплины (модуля)

#### 5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

#### 5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;

- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

### 5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

### 5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;

- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности. соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы:
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Основная литература:**

1. Тамб. гос. ун-т им. Г.Р. Державина Оценка границ и степени изолированности защищенных сред антивирусов. - [Тамбов]: [Б.и.], 2012. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д. В. Защита от вредоносных программ : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

### **6.2 Дополнительная литература:**

1. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В. Защита компьютерных систем от деструктивных программ : Учеб.-метод. пособие. - Тамбов: Изд-во ТГУ, 2005. - 158 с.
3. Защита компьютерных систем от деструктивных программ : учеб.-метод. комплекс, Блок 1: Антивирусное программное обеспечение. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM).

### **6.3 Иные источники:**

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>
2. Федеральная служба по надзору в сфере образования и науки - <http://obrnadzor.gov.ru>
3. Портал «Гуманитарное образование» - <http://www.humanities.edu.ru/>
4. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.edu.ru/>
5. Журнал «Вопросы образования» - <http://www.ecsocman.edu.ru/vo>

## **7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы**

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).



Лицензионное и свободно распространяемое программное обеспечение:

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal Licence

Операционная система Microsoft Windows 10

Adobe Reader XI (11.0.08) - Russian Adobe Systems Incorporated 10.11.2014 187,00 MB 11.0.08

7-Zip 9.20

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
2. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
3. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
4. Российская государственная библиотека. – URL: <https://www.rsl.ru>
5. Российская национальная библиотека. – URL: <http://nlr.ru>
6. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
7. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
8. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

### **Электронная информационно-образовательная среда**

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz)

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.