

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.34 Безопасные информационные технологии

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.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	14
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	35
6. Учебно-методическое и информационное обеспечение дисциплины.....	37
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	37

## 1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-2 Способен проводить анализ безопасности компьютерных систем

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

- организационно-управленческий
- эксплуатационный

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 12 Обеспечение безопасности (в сфере защиты информации)

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-2 Способен проводить анализ безопасности компьютерных систем	Анализирует безопасность компьютерных систем и информационных технологий

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-2 Способен проводить анализ безопасности компьютерных систем

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		5	6	7	8	10
1	Безопасность систем баз данных			+	+	
2	Программно-аппаратная защита информации	+	+			
3	Эксплуатационная практика					+

## 2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Безопасные информационные технологии» относится к обязательной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Безопасные информационные технологии» изучается в 6, 7 семестрах.

## 3. Объем и содержание дисциплины

3.1. Объем дисциплины: 8 з.е.

Очная: 8 з.е.

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>288</b>

Контактная работа	120
Лекции (Лекции)	60
Лабораторные (Лаб. раб.)	60
Самостоятельная работа (СР)	132
Экзамен	36
Зачет	-

### 3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
6 семестр					
1	Интернет-зависим ость.	3	4	14	Выполнение практических работ.; Защита лабораторной работы в компьютерном классе.
2	Вредоносное программное обеспечение, хакинг.	2	4	12	Выполнение практических работ.; Защита лабораторной работы в компьютерном классе.
3	Вымогательство и фишинг в сети.	2	5	12	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
4	Инсайдерские атаки.	3	3	12	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
5	Нежелательный контент.	6	3	12	Выполнение практических работ.; Защита лабораторной работы в компьютерном классе.

6	Манипулирование сознанием и действиями пользователя. Кибербуллинг.	6	3	12	Выполнение практических работ.; Защита лабораторной работы в компьютерном классе.
7	Уровень знаний об информационно-коммуникационных угрозах в молодежной группе.	6	6	14	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
7 семестр					
8	Способность противостоять информационным угрозам в молодежной группе.	6	4	8	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
9	Методы борьбы с интернет-зависимостью.	6	4	8	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
10	Методы борьбы с вредоносными программами.	4	4	6	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
11	Методы борьбы с фишингом.	4	4	6	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.

12	Методы борьбы с нежелательным контентом.	6	8	8	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.
13	Методы борьбы с манипулированием сознания и действиями пользователей.	6	8	8	Защита лабораторной работы в компьютерном классе.; Выполнение практических работ.

### Тема 1. Интернет-зависимость. (ПК-2)

#### Лекция.

Интернет-зависимость. Навязчивый веб-серфинг. Пристрастие к виртуальному общению. Виртуальные знакомства. Навязчивые потребности. Опасность интернет-зависимости для школьников. Исследование «Дети онлайн». Социальные сети - иллюзия полной занятости. Интернет-зависимость как уязвимость пользователя перед преступниками. Типовые примеры реализации угрозы.

#### Лабораторные работы.

Мониторинг действий пользователя с помощью программного продукта HideTracev.

#### Задания для самостоятельной работы.

1. Подготовьте доклад взаимосвязь интернет-зависимости и психических заболеваний
2. Выделите основные типы интернет-зависимости.
3. Чем грозит долгое пребывание в сети.
4. Назовите примеры реализации информационных угроз, связанных с интернет-зависимостью.
5. Какие программные решения можно предложить для снижения интернет-зависимости у детей, подростков и взрослых людей.

### Тема 2. Вредоносное программное обеспечение, хакинг. (ПК-2)

#### Лекция.

Определение вируса. Проблемы антивирусной защиты информации. Вирусы и их классификация. Среда обитания и алгоритмы вирусов. Деструктивные возможности вирусов (безвредные; неопасные; опасные вирусы; очень опасные). Полиморфик-вирусы. Полиморфные расшифровщики. Изменение выполняемого кода. Стелс-вирусы. Троянские программы. Программы шпионы, программные закладки. Хакерские утилиты "backdoor"; Программы- шпионы. Клавиатурные шпионы. Модели программ-шпионов. Программные закладки. Программный шпионаж. Хакер. Хакерская атака. Хакинг.

#### Лабораторные работы.

Использование плагина защиты McAfeeSiteAdvisor. Комплексная система защиты –Avira Security Suite. Антивирусное программное решение Avast! FreeAntivirus.

#### Задания для самостоятельной работы.

1. Подготовьте доклад по тенденциям развития вредоносного программного обеспечения.
2. Выделите отличительные признаки хакерской атаки. Выделите основные цели хакерских атак.
3. Установите плагин защиты в браузеры Google Chrome и Mozilla Firefox.
4. С помощью плагина защиты просмотрите отчет о безопасности веб-сайта.
5. Поведите полное сканирование системы. Установит высокий приоритет процесса сканирования, для обнаружения вредоносных программ.
6. Осуществите целенаправленный поиск Rootkit.
7. Добавьте межсетевой экран в доверенную зону антивирусного решения.
8. Создайте новый профиль сканирования только исполняемых файлов.
9. Настройте систему антиспама. Создайте правило удаления писем, содержащих вирусы.
10. Проведите анализ исходящего трафика по протоколам HTTP, SMTP и UDP. В случае обнаружения угрозы, заблокируйте подозрительные пакеты.

### **Тема 3. Вымогательство и фишинг в сети. (ПК-2)**

#### **Лекция.**

Вымогательство. Жертвы вымогательства (посетители брачных онлайн-салонов, сайтов знакомств, интернет-салонов, поисковых ресурсов). Вымогательство и вредоносные (тройанские) программы. Trojan-Ransom. Фишинг. Фишинговая атака. Phishing-атака с использованием электронной почты. Phishing веб-сайт. Характеристики электронных писем злоумышленников. Характеристики нелегитимных веб-сайтов. Хищение конфиденциальных данных.

#### **Лабораторные работы.**

Работа с расширением для браузера – фишинг фильтр. Проверка регистрационной информации с помощью службы WHOIS.

#### **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.
4. Поведите анализ содержания фишинговых сообщений. Создайте правила для динамических черных списков.
5. Выделите этапы фишинговых атак.
6. Установите расширение в браузеры для борьбы с фишингом.
7. Проверьте работу фишинг фильтра по блокированию сайтов – игровых, социальных сетей, развлекательных, новостных, тематических, видео-сайтов, образовательных и т. д.
8. Найдите регистрационную информацию для игровых, социальных сетей, развлекательных, новостных, тематических, видео-сайтов, образовательных и т. д. сайтов. Проанализируйте полученную информацию.

### **Тема 4. Инсайдерские атаки. (ПК-2)**

#### **Лекция.**

Определение инсайда. Доступ к конфиденциальной информации. Халатный инсайдер. Манипулируемый инсайдер. Обиженный инсайдер. Нелояльный инсайдер. Подрабатывающий инсайдер. Внедренный инсайдер. Аналитические данные от утечки



информации в компаниях и организациях. Вывод корпоративной информации из внутренней компьютерной сети. Проблема использования социальных сетей и мобильной связи на рабочем месте. Финансовые потери, связанные с затратами на ликвидацию последствий нарушений. Издержки на соблюдение правовых норм.

### **Лабораторные работы.**

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

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

1. Составьте прогностический портрет злоумышленника-инсайдера.
2. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности халатного инсайдера.
3. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности манипулируемого инсайдера.
4. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности обиженного инсайдера.
5. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности нелояльного инсайдера.
6. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности подрабатывающего инсайдера.
7. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности внедренного инсайдера.
8. На основе проведенного анализа сформулируйте основные меры защиты.
9. На примере организации (компании) проанализируйте виды данных, которые наиболее подвержены утечке информации.

## **Тема 5. Нежелательный контент. (ПК-2)**

### **Лекция.**

Нежелательный контент. Контент. Контентные риски. Негативные контентные материалы: незаконные и неэтичные. Неэтичная и вредоносная информация. Контент как средство манипулирования сознанием различных групп людей. Потенциальные угрозы при столкновении детей и подростков с нежелательным контентом.

### **Лабораторные работы.**

Использование фишинг-фильтра WOT (WebofTrust).

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

1. Подготовьте доклад на тему «Контент как средство манипулирования сознанием различных групп пользователей».
2. Выделите, что относится к незаконному контенту. Какие меры необходимо применять к создателям и распространителям незаконного контента в сети Интернет.
3. Выделите основные категории неэтичного контента для различных возрастных групп пользователей. На основе анализа сформулируйте динамические списки нежелательных для посещения сайтов.
4. Установите плагин в браузеры для блокирования нежелательного контента.
5. Проанализируйте репутацию ряда игровых, информационных, новостных, региональных, тематических, видео-сайтов, социальных и образовательных сайтов.
6. Откорректируйте репутацию ряда сайтов с помощью фишинг-фильтра WOT (WebofTrust).
7. Как можно подтасовать репутацию веб-сайтах.

## **Тема 6. Манипулирование сознанием и действиями пользователя. Кибербуллинг. (ПК-2)**

### **Лекция.**

Точки воздействия. Домогательство. Преследование. Бойкот. Манипулирование. Незаконный контакт и сексуальная эксплуатация ребенка. Понятие кибербуллинг. Киберпреследование в социальных сетях. Публикация унижительных материалов. Компрометация взломанных профилей и Интернет-ресурсов жертвы.

### **Лабораторные работы.**

Запрет посещения нежелательных категорий сайтов с помощью белых или динамических черных списков посредством программного продукта KidsControl.

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

1. Подготовьте доклад на тему «Новые приемы манипулирования сознанием и действием человека через Интернет, социальные сети и ВЕБ 2.0».
2. Выделите основные признаки манипулирования сознанием и действиями пользователей. Сформулируйте основные способы противодействия манипулированию.
3. Выделите возрастные группы, которые больше подвержены травле в сети Интернет.
4. Перечислите основные методы нападения по схеме кибербуллинга. Сформулируйте правила по определению такого понятия как «кибербуллинг» в сети Интернет.
5. Установите программный продукт KidsControl. Обеспечьте защиту своего персонального компьютера от кибербуллинга с помощью данного программного решения.

## **Тема 7. Уровень знаний об информационно-коммуникационных угрозах в молодежной группе. (ПК-2)**

### **Лекция.**

Обзор литературных данных и материалов Центра компьютерной безопасности ТГУ имени Г. Р. Державина об актуальном уровне информационно-коммуникационных угроз для пользователя

### **Лабораторные работы.**

Разработка анкеты в области безопасных ИКТ.

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

1. Пройти блок анкетирование «Актуальность вирусной атаки для вашего ПК. Способность противостоять угрозе. Уровень знаний».
2. Пройти анкетирование «Как часто Вы сталкивались с нежелательным контентом в сети. Уровень знаний».
3. Пройти анкетирование «Как часто Вы сталкивались с фишингом? Уровень знаний».
4. Пройти анкетирование «Подвержены ли Вы манипуляциям в информационной сфере? Уровень знаний».
5. Пройти анкетирование «Интернет-зависимость. Уровень знаний».

## **Тема 8. Способность противостоять информационным угрозам в молодежной группе. (ПК-2)**

### **Лекция.**

Обзор литературных данных и материалов Центра компьютерной безопасности ТГУ имени Г. Р. Державина о способности различных групп пользователей противостоять информационным угрозам.

### **Лабораторные работы.**

Разработка анкеты в области безопасных ИКТ.

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

1. Пройти блок анкетирование «Актуальность вирусной атаки для вашего ПК. Способность противостоять угрозе».
2. Пройти анкетирование «Как часто Вы сталкивались с нежелательным контентом в сети. Способность противостоять угрозе».
3. Пройти анкетирование «Как часто Вы сталкивались с фишингом? Способность противостоять угрозе».
4. Пройти анкетирование «Подвержены ли Вы манипуляциям в информационной сфере? Способность противостоять угрозе».
5. Пройти анкетирование «Интернет-зависимость. Способность противостоять угрозе».

## **Тема 9. Методы борьбы с интернет-зависимостью. (ПК-2)**

### **Лекция.**

Методы борьбы с интернет-зависимостью. Психологический подход.

Программный подход. Основные правила, позволяющие снизить зависимость пользователей. Борьба с «фейковыми» новостями.

### **Лабораторные работы.**

Блокирование рекламы и нежелательных объектов на веб-страницах с помощью утилиты Adguard.

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

1. Подготовьте доклад на тему «Интернет-зависимость - проблема современного общества».
2. Выделите методы борьбы с интернет-зависимостью, и какой характер они носят.
3. Сформулируйте признаки распознавания интернет-зависимых пользователей сети Интернет. Выделите возрастные группы пользователей, которые больше подвержены данной угрозе.
4. Перечислите психологические методы преодоления интернет-зависимости. Выделите пути решения данной зависимости у разных групп пользователей сети Интернет.
5. Перечислите программное решение, позволяющее снизить интернет-зависимость.
6. Установите утилиту Adguard. С помощью данной утилиты отключите фильтрацию «Полезной рекламы», экспортируйте список сайтов пользовательского фильтра, запретите загрузку исполняемых файлов, ограничьте время работы пользователя в сети Интернет.

## **Тема 10. Методы борьбы с вредоносными программами. (ПК-2)**

### **Лекция.**

Методы обнаружения и удаления компьютерных вирусов. Профилактика вирусного заражения и уменьшение предполагаемого ущерба. Профилактика вирусного заражения и уменьшение предполагаемого ущерба. Использование специализированных программ. Антивирусные программные средства. Антивирусные программы. Комплексные средства. Методика использования антивирусных программ. Профилактика заражения компьютера. Основные правила защиты. Проблема защиты от вирусов. Восстановление пораженных объектов. Прогнозы развития вредоносных программ и антивирусного ПО. Рейтинг антивирусных программных средств. Прогнозы развития средств противодействия.

### **Лабораторные работы.**

Комплексная система защиты—OutpostSecuritySuitePro.

Антишпионское программное обеспечение Ad-Aware Pro. Антивирус Касперского для Win-dows. Антивирус Dr.web для windows. Антивирусное программное обеспечение Kaspersky Internet Security

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

1. Классифицируйте антивирусные программные средства.
2. Сформулируйте прогнозы развития вредоносных программ и антивирусного программного решения.
3. Проанализируйте рейтинг антивирусных программных средств.
4. Предложите правила защиты от вирусного заражения и уменьшения предполагаемого ущерба.
5. Перечислите технические методы борьбы с вредоносными программами.
6. В антивирусном решении настройте журнал событий для анализа переданных пакетов TCP/IP.
7. Запретите приложениям выполнять любые сетевые операции.
8. Создайте профиль проверки только системной памяти и процессов. Поставьте, чтобы он выполнялся каждый раз при запуске компьютера. Что выполнял?
9. Защитите от утечки номер вашей кредитной карты и пароль входа в систему.
10. Заблокируйте доступ к вашему компьютеру любому компьютеру из сети. Создайте низкоуровневое правило блокирующее трафик с удаленного UDP порта.
11. Запретите передачу пароля на все сайты, кроме www.google.ru.
12. Просканируйте локальное сетевое окружение. Заблокируйте все IP-адреса на 30 минут.

## **Тема 11. Методы борьбы с фишингом. (ПК-2)**

### **Лекция.**

Организационные меры противодействия мошенничества в сети Интернет. Работа в сети Интернет. Методы противодействия преступлениям в электронной коммерции. Нелицензионное программное обеспечение. Формы авторизации. Конфиденциальная информация. Идентификационные данные. Предупреждения браузера о проблемах с сертификатом. Методы противодействия преступлениям в электронной коммерции. Надёжные торговые платформы. Регистрационная информация об интернет-домене. Сертификат сетевой безопасности. Антивирусное решение. Интернет-обозреватель. Фишинг-фильтр.

### **Лабораторные работы.**

Проверка сертификата сетевой безопасности.

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

1. Проанализируйте меры, позволяющие успешно противостоять фишинговым атакам. Перечислите программные меры противодействия фишингу.
2. Выделите социальные, организационные меры противодействия фишингу.
3. Перечислите методы противодействия преступлениям в электронной коммерции.
4. Проверьте сертификаты сетевой безопасности у ряда игровых, информационных, новостных, региональных, тематических, видео-сайтов, социальных и образовательных сайтов через браузеры Opera, Google Chrome, Mozilla Firefox. Проанализируйте полученную информацию.
5. Выделите надежные торговые платформы.

## **Тема 12. Методы борьбы с нежелательным контентом. (ПК-2)**

### **Лекция.**

Организационные меры борьбы. Плагины и дополнения: WOT (Web of Trust), Adblock Plus, PublicFox, FoxFilter. Поисковые системы. Специализированные ресурсы. Юридические механизмы. Нежелательная информация. Мониторинг действий пользователя. Надежные методы защиты. Технология фильтрации сайтов. Интегрированные решения. Фильтрация негативного контента. Комплексные продукты для защиты домашних компьютеров. Веб-фильтры: CyberPatrol, CyberSitter, ChildWebGuardian, NetNanny. Фильтрация контента на четырех уровнях: онлайн сообщество, провайдер, шлюз в Интернет защищаемой сети, клиентская станция.

### **Лабораторные работы.**

Установка и настройка расширения для браузера Adblock Plus.

Расширения для браузера FoxFilter. Веб-фильтр CyberPatrol. Блокирование загрузки и показа элементов веб-страниц.

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

1. Подготовьте доклад о методах борьбы с нежелательным контентом. Выделите специализированные ресурсы, предоставляющие информацию о методах борьбы с нежелательным контентом.
2. Перечислите юридические механизмы нежелательного контента.
3. Перечислите организационные и технические методы блокирования нежелательного контента.
4. Установите плагин в браузеры для блокирования нежелательного контента.
5. Установите расширения для браузеров Adblock Plus.
6. Создайте список сайтов с допустимой рекламой посредством отправки запроса разработчику Adblock Plus.
7. Предложите способ просмотра сайтов с навязчивой рекламой после установки в браузер Adblock Plus.
8. Составьте список комплексных продуктов для защиты домашних компьютеров.
9. Проверьте фильтрацию контента на четырех уровнях: онлайн сообщество, провайдер, шлюз в Интернет защищаемой сети, клиентская станция.

## **Тема 13. Методы борьбы с манипулированием сознанием и действиями пользователей. (ПК-2)**

### **Лекция.**

Методы борьбы с манипулированием сознанием и действиями пользователей.

Юридический механизм. Сбор доказательной базы. Уголовный и административный кодекс. Набор правил для школьников и подростков. Технические методы борьбы с манипулированием сознанием пользователей. Защита от коммуникационных угроз. Психологические особенности ребенка. Этническое поведение в сети. Агрессивные и негативные ресурсы. Специализированное программное обеспечение: «Родительский контроль» и «Семейная безопасность». Детский браузер.

### **Лабораторные работы.**

Защита от коммуникационных угроз. Этническое поведение в сети. Работа с веб-фильтром «Интернет-Цензор». Родительский контроль. Семейная безопасность. Детский браузер.

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

1. Перечислите сервисы и технологии, которые может использовать злоумышленник для манипулирования действиями пользователя.
2. Выделите эффективные методы в борьбе с манипуляторами.
3. Законспектируйте программные продукты, которые можно использовать для

блокирования «киберхулиганов». Выделите возрастные группы, которые больше подвержены травле в сети Интернет.

4. Проанализируйте работу программного обеспечения «Родительский контроль» и «Семейная безопасность». Перечислите наиболее эффективные браузеры для детей.

5. Сформируйте набор правил пользования интернет ресурсами для школьников и подростков.

#### 4. Контроль знаний обучающихся и типовые оценочные средства

##### 4.1. Распределение баллов:

##### 6 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

##### Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мак. кол-во баллов	Методика проведения занятия и оценки
1.	Интернет-зависимость.	Выполнение практических работ.	7	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.

		Защита лабораторной работы в компьютерном классе.	5	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>3 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>
2.	Вредоносное программное обеспечение, хакинг.	Выполнение практических работ.	7	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>

		Защита лабораторной работы в компьютерном классе.	5	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 3 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.
3.	Вимогательств о и фишинг в сети.	Защита лабораторной работы в компьютерном классе.	5	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 3 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.



		Выполнение практических работ.	7	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.
4.	Инсайдерские атаки.	Защита лабораторной работы в компьютерном классе.	5	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 3 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.
		Выполнение практических работ.	7	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.

5.	Нежелательный контент.	Выполнение практических работ.	7	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.
		Защита лабораторной работы в компьютерном классе.	5	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 3 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.
6.	Манипулирование сознанием и действиями пользователя. Кибербуллинг.	<b>Выполнение практических работ.(контрольный срез)</b>	10	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.

		Защита лабораторной работы в компьютерном классе.	5	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>3 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>
7.	Уровень знаний об информационно-коммуникационных угрозах в молодежной группе.	<b>Защита лабораторной работы в компьютерном классе.(контрольный срез)</b>	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>6 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>3 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>

		Выполнение практических работ.	5	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.
8.	Посещаемость		10	10баллов – стопроцентное посещение занятий студентом 5 балла – посещаемость студента составляет не менее 80 % занятий 3-балла – посещаемость студента составляет не менее 50 % занятий 1 балл – посещаемость студента составляет не менее 25 % занятий
9.	Премияльные баллы		20	Дополнительные премияльные 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 / журнале из перечня ВАК – 10 / 15 / 20
10.	Итого за семестр		100	

#### 7 семестр

- посещаемость – 10 баллов
- текущий контроль – 46 баллов
- контрольные срезы – 2 среза по 7 баллов каждый
- премияльные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

#### Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
--------	------------------------------------	---------------------------------	--------------------	--------------------------------------

1.	Способность противостоять информационным угрозам в молодежной группе.	Защита лабораторной работы в компьютерном классе.	3	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>3 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>2 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>
		Выполнение практических работ.	7	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>

2.	Методы борьбы с интернет-зависимостью.	Защита лабораторной работы в компьютерном классе.	3	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>3 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>2 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>
		Выполнение практических работ.	7	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>

3.	Методы борьбы с вредоносными программами.	Защита лабораторной работы в компьютерном классе.	3	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>3 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>2 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>
		Выполнение практических работ.	7	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>

4.	Методы борьбы с фишингом.	Защита лабораторной работы в компьютерном классе.	3	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>3 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>2 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>
		Выполнение практических работ.(контрольный срез)	7	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>



5.	Методы борьбы с нежелательным контентом.	Защита лабораторной работы в компьютерном классе.	3	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>3 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>2 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>
		Выполнение практических работ.	7	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>

6.	Методы борьбы с манипулированием сознанием и действиями пользователей.	Защита лабораторной работы в компьютерном классе.	3	Лабораторные работы выполняются по текущему разделу или темы дисциплины. 3 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 2 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.
		Выполнение практических работ.(контрольный срез)	7	Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины. Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.
7.	Посещаемость		10	10баллов – стопроцентное посещение занятий студентом 5 балла – посещаемость студента составляет не менее 80 % занятий 3-балла– посещаемость студента составляет не менее 50 % занятий 1 балл – посещаемость студента составляет не менее 25 % занятий
8.	Премияльные баллы		20	Дополнительные премияльные 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 / журнале из перечня ВАК – 10 / 15 / 20

9.	Ответ на экзамене	30	25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно»
10.	Итого за семестр	100	

Итоговая оценка по экзамену 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
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

#### 4.2 Типовые оценочные средства текущего контроля

### Выполнение практических работ.

#### Тема 1. Интернет-зависимость.

1. Подготовьте доклад взаимосвязь интернет-зависимости и психических заболеваний
2. Выделите основные типы интернет-зависимости.
3. Чем грозит долгое пребывание в сети.
4. Назовите примеры реализации информационных угроз, связанных с интернет-зависимостью.
5. Какие программные решения можно предложить для снижения интернет-зависимости у детей, подростков и взрослых людей.

#### Тема 2. Вредоносное программное обеспечение, хакинг.

1. Подготовьте доклад по тенденциям развития вредоносного программного обеспечения.
2. Выделите отличительные признаки хакерской атаки. Выделите основные цели хакерских атак.
3. Установите плагин защиты в браузеры Google Chrome и Mozilla Firefox.
4. С помощью плагина защиты просмотрите отчет о безопасности веб-сайта.
5. Поведите полное сканирование системы. Установит высокий приоритет процесса сканирования, для обнаружения вредоносных программ.
6. Осуществите целенаправленный поиск Rootkit.
7. Добавьте межсетевой экран в доверенную зону антивирусного решения.
8. Создайте новый профиль сканирования только исполняемых файлов.
9. Настройте систему антиспама. Создайте правило удаления писем, содержащих вирусы.
10. Проведите анализ исходящего трафика по протоколам HTTP, SMTP и UDP. В случае обнаружения угрозы, заблокируйте подозрительные пакеты.

#### Тема 3. Вымогательство и фишинг в сети.

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.
4. Поведите анализ содержания фишинговых сообщений. Создайте правила для динамических черных списков.
5. Выделите этапы фишинговых атак.
6. Установите расширение в браузеры для борьбы с фишингом.
7. Проверьте работу фишинг-фильтра по блокированию сайтов – игровых, социальных сетей, развлекательных, новостных, тематических, видео-сайтов, образовательных и т. д.
8. Найдите регистрационную информацию для игровых, социальных сетей, развлекательных, новостных, тематических, видео-сайтов, образовательных и т. д. сайтов. Проанализируйте полученную информацию.

#### Тема 4. Инсайдерские атаки.

1. Составьте прогностический портрет злоумышленника-инсайдера.
2. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности халатного инсайдера.
3. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности манипулируемого инсайдера.
4. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности обиженного инсайдера.
5. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности нелояльного инсайдера.
6. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности подрабатывающего инсайдера.
7. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности внедренного инсайдера.
8. На основе проведенного анализа сформулируйте основные меры защиты.
9. На примере организации (компании) проанализируйте виды данных, которые наиболее подвержены утечке информации.

#### Тема 5. Нежелательный контент.

1. Подготовьте доклад на тему «Контент как средство манипулирования сознанием различных групп пользователей».
2. Выделите, что относится к незаконному контенту. Какие меры необходимо применять к создателям и распространителям незаконного контента в сети Интернет.
3. Выделите основные категории неэтичного контента для различных возрастных групп пользователей. На основе анализа сформулируйте динамические списки нежелательных для посещения сайтов.
4. Установите плагин в браузеры для блокирования нежелательного контента.
5. Проанализируйте репутацию ряда игровых, информационных, новостных, региональных, тематических, видео-сайтов, социальных и образовательных сайтов.
6. Откорректируйте репутацию ряда сайтов с помощью фишинг-фильтра WOT (WebofTrust).
7. Как можно подтасовать репутацию веб-сайтах.

### Тема 6. Манипулирование сознанием и действиями пользователя. Кибербуллинг.

1. Подготовьте доклад на тему «Новые приемы манипулирования сознанием и действием человека через Интернет, социальные сети и ВЕБ 2.0».
2. Выделите основные признаки манипулирования сознанием и действиями пользователей. Сформулируйте основные способы противодействия манипулированию.
3. Выделите возрастные группы, которые больше подвержены травле в сети Интернет.
4. Перечислите основные методы нападения по схеме кибербуллинга. Сформулируйте правила по определению такого понятия как «кибербуллинг» в сети Интернет.
5. Установите программный продукт KidsControl. Обеспечьте защиту своего персонального компьютера от кибербуллинга с помощью данного программного решения.

### Тема 7. Уровень знаний об информационно-коммуникационных угрозах в молодежной группе.

1. Пройти блок анкетирование «Актуальность вирусной атаки для вашего ПК. Способность противостоять угрозе. Уровень знаний».
2. Пройти анкетирование «Как часто Вы сталкивались с нежелательным контентом в сети. Уровень знаний».
3. Пройти анкетирование «Как часто Вы сталкивались с фишингом? Уровень знаний».
4. Пройти анкетирование «Подвержены ли Вы манипуляциям в информационной сфере? Уровень знаний».
5. Пройти анкетирование «Интернет-зависимость. Уровень знаний».

### Тема 8. Способность противостоять информационным угрозам в молодежной группе.

1. Пройти блок анкетирование «Актуальность вирусной атаки для вашего ПК. Способность противостоять угрозе».
2. Пройти анкетирование «Как часто Вы сталкивались с нежелательным контентом в сети. Способность противостоять угрозе».
3. Пройти анкетирование «Как часто Вы сталкивались с фишингом? Способность противостоять угрозе».
4. Пройти анкетирование «Подвержены ли Вы манипуляциям в информационной сфере? Способность противостоять угрозе».
5. Пройти анкетирование «Интернет-зависимость. Способность противостоять угрозе».

### Тема 9. Методы борьбы с интернет-зависимостью.

- 1 Подготовьте доклад на тему «Интернет-зависимость - проблема современного общества».
- 2 Выделите методы борьбы с интернет-зависимостью, и какой характер они носят.
- 3 Сформулируйте признаки распознавания интернет-зависимых пользователей сети Интернет. Выделите возрастные группы пользователей, которые больше подвержены данной угрозе.
- 4 Перечислите психологические методы преодоления интернет-зависимости. Выделите пути решенияданной зависимости у разных групп пользователей сети Интернет.
- 5 Перечислите программное решение, позволяющее снизить интернет-зависимость.
- 6 Установите утилиту Adguard. С помощью данной утилиты отключите фильтрацию «Полезной рекламы», экспортируйте список сайтов пользовательского фильтра, запретите загрузку исполняемых файлов, ограничьте время работы пользователя в сети Интернет.

### Тема 10. Методы борьбы с вредоносными программами.

- 1 Классифицируйте антивирусные программные средства.
- 2 Сформулируйте прогнозы развития вредоносных программ и антивирусного программного решения.
- 3 Проанализируйте рейтинг антивирусных программных средств.
- 4 Предложите правила защиты от вирусного заражения и уменьшения предполагаемого ущерба.
- 5 Перечислите технические методы борьбы с вредоносными программами.
- 6 В антивирусном решении настройте журнал событий для анализа переданных пакетов TCP/IP.
- 7 Запретите приложениям выполнять любые сетевые операции.
- 8 Создайте профиль проверки только системной памяти и процессов. Поставьте, чтобы он выполнялся каждый раз при запуске компьютера. Что выполнял?
- 9 Защитите от утечки номер вашей кредитной карты и пароль входа в систему.
- 10 Заблокируйте доступ к вашему компьютеру любому компьютеру из сети. Создайте низкоуровневое правило блокирующее трафик с удаленного UDP порта.
- 11 Запретите передачу пароля на все сайты, кроме [www.google.ru](http://www.google.ru).
- 12 Просканируйте локальное сетевое окружение. Заблокируйте все IP-адреса на 30 минут.

### Тема 11. Методы борьбы с фишингом.

- 1 Проанализируйте меры, позволяющие успешно противостоять фишинговым атакам. Перечислите программные меры противодействия фишингу.
- 2 Выделите социальные, организационные меры противодействия фишингу.
- 3 Перечислите методы противодействия преступлениям в электронной коммерции.
- 4 Проверьте сертификаты сетевой безопасности у ряда игровых, информационных, новостных, региональных, тематических, видео-сайтов, социальных и образовательных сайтов через браузеры Opera, Google Chrome, Mozilla Firefox. Проанализируйте полученную информацию.
- 5 Выделите надежные торговые платформы.

### Тема 12. Методы борьбы с нежелательным контентом.

- 1 Подготовьте доклад о методах борьбы с нежелательным контентом. Выделите специализированные ресурсы, предоставляющие информацию о методах борьбы с нежелательным контентом.
- 2 Перечислите юридические механизмы нежелательного контента.
- 3 Перечислите организационные и технические методы блокирования нежелательного контента.
- 4 Установите плагин в браузеры для блокирования нежелательного контента.
- 5 Установите расширения для браузеров AdblockPlus.
- 6 Создайте список сайтов с допустимой рекламой посредством отправки запроса разработчику AdblockPlus.
- 7 Предложите способ просмотра сайтов с навязчивой рекламой после установки в браузер AdblockPlus.
- 8 Составьте список комплексных продуктов для защиты домашних компьютеров.
- 9 Проверьте фильтрацию контента на четырех уровнях: онлайн сообщество, провайдер, шлюз в Интернет защищаемой сети, клиентская станция.

### Тема 13. Методы борьбы с манипулированием сознанием и действиями пользователей.

1. Перечислите сервисы и технологии, которые может использовать злоумышленник для манипулирования действиями пользователя.
2. Выделите эффективные методы в борьбе с манипуляторами.
3. Законспектируйте программные продукты, которые можно использовать для

блокирования «киберхулиганов». Выделите возрастные группы, которые больше подвержены травле в сети Интернет.

4. Проанализируйте работу программного обеспечения «Родительский контроль» и «Семейная безопасность». Перечислите наиболее эффективные браузеры для детей.

5. Сформируйте набор правил пользования интернет ресурсами для школьников и подростков.

### **Защита лабораторной работы в компьютерном классе.**

#### **Тема 1. Интернет-зависимость.**

Мониторинг действий пользователя с помощью программного продукта HideTracev.

#### **Тема 2. Вредоносное программное обеспечение, хакинг.**

Использование плагина защиты McAfeeSiteAdvisor. Комплексная система защиты –Avira Security Suite. Антивирусное программное решение Avast! FreeAntivirus.

#### **Тема 3. Вымогательство и фишинг в сети.**

Работа с расширением для браузера – фишинг фильтр. Проверка регистрационной информации с помощью службы WHOIS.

#### **Тема 4. Инсайдерские атаки.**

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

#### **Тема 5. Нежелательный контент.**

Использование фишинг-фильтра WOT (WebofTrust).

#### **Тема 6. Манипулирование сознанием и действиями пользователя. Кибербуллинг.**

Запрет посещения нежелательных категорий сайтов с помощью белых или динамических черных списков посредством программного продукта KidsControl.

#### **Тема 7. Уровень знаний об информационно-коммуникационных угрозах в молодежной группе.**

Разработка анкеты в области безопасных ИКТ.

#### **Тема 8. Способность противостоять информационным угрозам в молодежной группе.**

Блокирование рекламы и нежелательных объектов на веб-страницах с помощью утилиты Adguard.

#### **Тема 9. Методы борьбы с интернет-зависимостью.**

Комплексная система защиты–OutpostSecuritySuitePro.

Антишпионское программное обеспечение Ad-Aware Pro. Антивирус Касперского для Win-dows. Антивирус Dr.web для windows. Антивирусное программное обеспечение Kaspersky Internet Security

#### **Тема 10. Методы борьбы с вредоносными программами.**

Проверка сертификата сетевой безопасности.

#### Тема 11. Методы борьбы с фишингом.

Установка и настройка расширения для браузера AdblockPlus.

Расширения для браузера FoXFilter. Веб –фильтр CyberPatrol. Блокирование загрузки и показа элементов веб-страниц.

#### Тема 12. Методы борьбы с нежелательным контентом.

Защита от коммуникационных угроз. Этническое поведение в сети. Работа с веб-фильтром «Интернет-Цензор». Родительский контроль. Семейная безопасность. Детский браузер.

#### Тема 13. Методы борьбы с манипулированием сознания и действиями пользователей.

Защита от коммуникационных угроз. Этническое поведение в сети. Работа с веб-фильтром «Интернет-Цензор». Родительский контроль. Семейная безопасность. Детский браузер.

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

#### Типовые вопросы зачета (ПК-2)

1. Классификация компьютерных вирусов.
2. Отличительные черты файловых вирусов.
3. Выделите отличительные признаки хакерской атаки.
4. Выделите основные цели хакерских атак.
5. Перечислите способы проникновения программ-вымогателей в устройство пользователя.
6. Выделите этапы фишинговых атак.
7. Классифицируйте виды инсайдеров.
8. Проанализируйте мировую и российскую практику по обнаружению и привлечению к ответственности халатного, манипулируемого, обиженного, нелояльного, подрабатывающего, внедренного инсайдера.
9. Выделите основные категории неэтичного контента для различных возрастных групп пользователей.
10. Выделите основные признаки манипулирования сознанием и действиями пользователей.
11. Классифицируйте антивирусные программные средства.
12. Выделите социальные, организационные меры противодействия фишингу. Перечислите программные меры противодействия фишингу.
13. Перечислите организационные и технические методы блокирования нежелательного контента.

#### Типовые задания для зачета (ПК-2)

1. Проверить наличие безопасного соединения с сайтом с помощью браузера MozillaFirefox
2. Проверить наличие безопасного соединения с сайтом с помощью браузера GoogleChrome
3. Проверить наличие безопасного соединения с сайтом с помощью браузера Opera
4. Найти 5 сайтов с отсутствующим безопасным соединением
5. Основы работы в визуальной среде программирования Delphi. Создание интерфейса программы.

#### Типовые вопросы экзамена (ПК-2)

1. Перечислите особенности информационно-коммуникационных угроз для молодежных групп пользователей?



- 2 Что такое интернет-зависимость?
- 3 Назовите основные типы интернет-зависимости?
- 4 Для кого интернет-зависимость представляет особую опасность?
- 5 Остаетесь on-line дольше, чем намеревались?
- 6 Вы игнорируете домашние обязанности, чтобы подольше побыть в сети?
- 7 Завязываете Вы новые отношения с пользователями интернета?
- 8 Вы проверяете социальные сети и почту, прежде чем заняться необходимыми делами?
- 9 Вы стремитесь заместить тревожные мысли о своей жизни успокаивающими мыслями об интернете?
- 10 Вы ощущаете жизнь без интернета скучной, пустой и безрадостной?
- 11 Вас захватывают мысли об интернете или фантазии о виртуальных друзьях?
- 12 Вы скрываете от других продолжительность вашего пребывания в сети?
- 13 Как часто Вы предпочитаете интернет общению с людьми?
- 14 Чувствуете Вы пустоту, депрессию, раздражение, находясь не за компьютером?
- 15 Что такое вымогательство?
- 16 Кто может стать жертвами вымогательства?
- 17 Что такое фишинг?
- 18 Что является целью фишинг-атаки?
- 19 Что содержат в себе фишинговые сообщения?
- 20 На какие этапы делится фишинговая атака?
- 21 Что такое Phishing веб-сайт?
- 22 Какие характеристики содержат электронные письма злоумышленников?
- 23 Какие характеристики имеют нелегитимные веб-сайты?
- 24 Сколько в среднем живут сайты злоумышленников?
- 25 Что является характерной особенностью нелегитимных писем?
- 26 Какие существуют методы хищения информации?
- 27 Что такое хищение конфиденциальных данных?
- 28 Что способствует успеху фишинг-афер?
- 29 На каких ресурсах сети интернет можно указывать свои персональные данные (паспортные данные, pin коды, номера банковских карт)?
- 30 Какая информация будет «полезна» для злоумышленника?
- 31 Какие сведения о Вас могут потребоваться интернет мошенникам?
- 32 Какие способы интернет мошенничества Вам известны?
- 33 Как часто Вы переходите по всплывающим рекламным баннерам?
- 34 Вы всегда проверяете адрес сайта в адресной строке?
- 35 Как Вы отреагируете на сообщение, в котором Вас просят указать какую либо конфиденциальную информацию?
- 36 Какое антивирусное ПО, способно блокировать переход на фишинговые сайты?
- 37 Перечислите социальные меры противодействия мошенничества в сети Интернет?
- 38 На Ваш взгляд, какие организационные меры борьбы с утечкой документов полезны в борьбе с фишингом?
- 39 Дайте определение понятию «Инсайдер»?
- 40 Что содержит в себе нежелательный контент?
- 41 Что такое контент?
- 42 Что такое контентные риски?
- 43 Что относится к незаконному контенту?
- 44 Что относится к неэтичному контенту?
- 45 Как распознать незаконный контент в сети Интернет?
- 46 Как распознать материалы неэтичного характера в сети Интернет?

- 47 На что может быть направлена неэтичная и вредоносная информация?
- 48 Что входит в список потенциальных угроз среди детей и подростков при столкновении с нежелательным контентом?
- 49 Какие электронные ресурсы могут содержать нежелательный контент?
- 50 К каким информационным угрозам может привести участие в он-лайн играх на деньги?
- 51 Какое наказание предусмотрено за публикацию материалов, разжигающих расовую или национальную дискриминацию?
- 52 Перечислите точки воздействия на пользователя, который подвергается манипулированию сознанием и действиями пользователя?
- 53 Что такое киберпреследование?
- 54 Что такое домогательство?
- 55 Что такое груминг?
- 56 Какая ИТ-угроза вышла на первое место для детей?
- 57 Перечислите методы кибербуллинга.
- 58 Что представляют собой анонимные угрозы?
- 59 Что представляет собой преследование в сети?
- 60 Дайте определение ИТ-угрозе флейминг.
- 61 Что представляет собой хеппислепинг?
- 62 Почему виртуальные знакомства могут подвергнуть реальному риску физическое, эмоциональное и духовное здоровье человека?
- 63 Какие действия пользователя и внешние факторы содействуют реализации угроз коммуникационного характера?
- 64 К каким рискам может приводить манипулирование сознанием и действиями пользователя в сети?

#### **Типовые задания для экзамена (ПК-2)**

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

##### Зачет

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«зачтено» (50 - 100 баллов)	ПК-2	Демонстрирует достаточный уровень теоретических знаний об угрозах информационно-коммуникационного характера. Эффективно использует программные средства общего и специального назначения для безопасности пользователя ИКТ. Способен проводить работы по анализу безопасности компьютерных систем.
«не зачтено» (0 - 49 баллов)	ПК-2	Не показывает теоретических знаний об угрозах информационно-коммуникационного характера. Не может использовать программные средства общего и специального назначения для безопасности пользователя ИКТ. Не способен проводить работы по анализу безопасности компьютерных систем.

#### Экзамен

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-2	Демонстрирует высокий уровень теоретических знаний об угрозах информационно-коммуникационного характера. Эффективно использует программные средства общего и специального назначения для безопасности пользователя ИКТ. Способен проводить работы по анализу безопасности компьютерных систем.
«хорошо» (70 - 84 баллов)	ПК-2	Демонстрирует достаточный уровень теоретических знаний об угрозах информационно-коммуникационного характера. Эффективно использует программные средства общего и специального назначения для безопасности пользователя ИКТ. Способен проводить работы по анализу безопасности компьютерных систем.
«удовлетворительно» (50 - 69 баллов)	ПК-2	Демонстрирует низкий уровень теоретических знаний об угрозах информационно-коммуникационного характера. Частично использует программные средства общего и специального назначения для безопасности пользователя ИКТ. Не способен проводить работы по анализу безопасности компьютерных систем.
«неудовлетворительно» (менее 50 баллов)	ПК-2	Не показывает теоретических знаний об угрозах информационно-коммуникационного характера. Не может использовать программные средства общего и специального назначения для безопасности пользователя ИКТ. Не способен проводить работы по анализу безопасности компьютерных систем.

## 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. 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 от вредоносных программ : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

### **6.2 Дополнительная литература:**

1. Фефилов А. Д. Методы и средства защиты информации в сетях : практическое пособие. - Москва: Лаборатория книги, 2011. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=140796>
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. Портал «Гуманитарное образование» - <http://www.humanities.edu.ru/>
3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.edu.ru/>
4. Федеральная служба по надзору в сфере образования и науки - <http://obrnadzor.gov.ru>
5. 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.