МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Основы информационной безопасности

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины «Основы информационной безопасности» является теоретическая и практическая подготовка к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления.

Данный курс, на основе использования международных российских стандартов и нормативных требований ФСБ России, ФСТЭК России и Роскомнадзора в сфере обеспечения информационной безопасности, вырабатывает у студентов знания, навыки и умения организовывать системы защиты информации, адекватные возникающим угрозам.

2. Место дисциплины в структуре ОП

«Основы информационной безопасности» относится к базовой части Блока 1.

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Теория информации» – знание основ и содержания современных методов получения, обработки, хранения, использования и уничтожения информации.

Знания и навыки, полученные в результате изучении дисциплины «Основы информационной безопасности», используются студентами в дальнейшем при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**И_УК-1_3** При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения	**Знать** основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. **Уметь** применять основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.
Общепрофессиональные компетенции		
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной	**И-ОПК-1_3** Знает понятия информации, информационной безопасности, место и роль информационной	**Знать** требования российского законодательства в сфере защиты персональных данных, охраны результатов интеллектуальной деятельности.

безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики	**Уметь** формулировать основные требования к защите информации и разрабатывать проекты локальных нормативных и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации. формировать политику информационной безопасности
ОПК- 2.3 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов	**И-ОПК-2.3_3** Способен для конкретной системы осуществлять обоснованный выбор программных и программно-аппаратных средств, обеспечивающих высокую защищенность от вредоносного ПО.	**Уметь** подготовить необходимые документы для подрядчика по проведению работ в сфере лицензирования в области обеспечения защиты информации, аттестации объектов информатизации

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 акад. часа.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	
1	Информационная безопасность Российской Федерации	4	2	2				4	Опрос на практических занятиях
2	Безопасность (защищенность) компьютерных систем.	4	2	2				4	Опрос на практических занятиях
3	Модели нарушителя и типичные атаки.	4	2	2		2		4	Опрос на практических занятиях
4	Вредоносное программное обеспечение.	4	2	2				5	Опрос на практических занятиях
5	Средства защиты и нападения.	4	2	2		2		4	Опрос на практических занятиях
6	Уничтожение информации.	4	2	2				4	Опрос на практических занятиях
7	Защита информации от утечки по техническим каналам	4	2	2				4	Опрос на практических занятиях

8	Компьютерно-техническая экспертиза.	4	2	2				4	Опрос на практических занятиях
							0,3	2,7	Зачет
	Всего	**72**	16	16		4	0,3	35,7	

Содержание разделов дисциплины:

Тема № 1 Информационная безопасность Российской Федерации.

1.1. Угрозы информационной безопасности Российской Федерации.

1.2. Доктрина информационной безопасности.

1.3. Общие принципы защиты информации.

1.4. Классификация угроз.

1.5. Обзор материалов федерального банка данных угроз безопасности, ведущегося в разделе «Техническая защита информации» (https://bdu.fstec.ru) на официальном сайте ФСТЭК России и семейства национальных стандартов защиты от угроз, реализуемых через скрытые каналы (ГОСТ Р ИСО/МЭК 53113-1-2008, 53113-2-2009).

Тема № 2 Безопасность (защищенность) компьютерных систем.

2.1. Обзор средств и методов информационной/компьютерной безопасности.

2.2. Интегрированная программно-аппаратная защита информации Trusted Platform Module (TPM).

2.3. Методы нарушения конфиденциальности, целостности и доступности информации.

2.4. Модели управления доступом.

2.5. Контроль прав доступа.

2.6. Обзор семейства национальных стандартов России в сфере критериев оценки безопасности информационных систем (ГОСТ Р ИСО/МЭК 15408-1-2012 «Часть 1. Введение в общую модель», ГОСТ Р ИСО/МЭК 15408-2-2013 «Часть 2. Функциональные компоненты безопасности», ГОСТ Р ИСО/МЭК 15408-3-2013 «Часть 3. Компоненты доверия к безопасности»).

Тема № 3 Модели нарушителя и типичные атаки.

3.1. Модель действий вероятного нарушителя и модель построения защиты.

3.2. Классификация основных видов атак.

3.3. Сетевая разведка.

3.4. Средства и методы нейтрализации атак.

Тема № 4 Вредоносное программное обеспечение.

4.1. Классификация вредоносных программ.

4.2. Признаки присутствия вредоносного ПО.

4.3. Методы обнаружения вредоносного ПО.

4.4. Способы внедрения вредоносного ПО.

4.5. Примеры сетевых атак.

4.6. Троянские программы, люки, эксплойты.

4.7. Методы защиты от вредоносного ПО. Технологии самозащиты. Место и роль межсетевых экранов в обеспечении безопасности ресурсов АС. Возможности и ограничения антивирусных программ. (обзор

4.8. Специализированные средства и методы выявления вредоносных программ.

Тема № 5 Средства защиты и нападения.

5.1. Информационная война и информационное оружие.

5.2. Особенности технических средств информационной войны.

5.3. Классификация средств защиты и нападения.

5.4. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники.

5.5. Средства силового деструктивного воздействия (СДВ).

Тема № 6 Уничтожение информации.

6.1. Необходимость уничтожения документов. Особенности удаления информации с электронных носителей.

6.2. Политика уничтожения данных.

6.3. Уничтожение конфиденциальной информации (плановое и экстренное).

6.4. Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки".

6.5. Конфиденциальность в социальных сетях.

Тема № 7 Защита информации от утечки по техническим каналам.

7.1. Утечки: понятие, виды.

7.2. Типовые каналы утечки информации.

7.3. Технические каналы утечки.

7.4. Средства и методы обнаружения технических каналов утечки информации.

7.5. Системы защиты конфиденциальных данных от внутренних угроз.

7.6. Технология цифровых отпечатков.

Тема № 8 Компьютерно-техническая экспертиза.

8.1. Компьютерно-техническая экспертиза. Методы экспертизы.

8.2. Проведение расследования компьютерных инцидентов.

8.3. Исследование носителей компьютерной информации.

8.4. Аппаратно-программные средства расследования компьютерных инцидентов.

8.5. Обзор положений ГОСТ Р ИСО/МЭК 18044-2007 «Менеджмент инцидентов информационной безопасности» для решения задач расследования инцидентов безопасности.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках курса, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Основы информационной безопасности» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты лекций по отдельным темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;

посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- Adobe Acrobat Reader;
- Интернет-версия справочной системы Гарант.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:
Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016г. № 646).
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002 (дата обращения: 29.01.2022).
3. Нестеров С.А., Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров, М., Юрайт, 2016, 321с
4. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114688 (дата обращения: 29.01.2022). — Режим доступа: для авториз. пользователей.

5. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / Шаньгин В. Ф. - Москва : ДМК Пресс, 2012. - 592 с. - ISBN 978-5-94074-637-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785940746379.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.

6. Шаньгин, В. Ф. Информационная безопасность и защита информации / Шаньгин В. Ф. - Москва : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785940747680.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.

7. Галатенко, В. А. Стандарты информационной безопасности / Галатенко В. А. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. (Основы информационных технологий) - ISBN 5-9556-0053-1. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN5955600531.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.

8. ГОСТ Р ИСО/МЭК ТО 19791-2008г., «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. - 126с.
9. ГОСТ Р ИСО/МЭК 18045-2013г., «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2014. - 250с.
10. ГОСТ Р ИСО/МЭК 15408-1-2012г., 15408-2-2013г., 15408-3-2013г., «Информационная технология. Методы и средства обеспечения информационной безопасности. Критерии оценки безопасности информационных технологий», «Часть 1. Введение и общая модель», «Часть 2. Функциональные компоненты безопасности», «Часть. 3. Компоненты доверия к безопасности», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», Часть 1.-2014.-56с., Часть 2.-2014.-164с., Часть 3.-2014.-152с.
11. ГОСТ Р ИСО/МЭК 53113-1-2008 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 1. Общие положения», Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2009. - 12с.
12. ГОСТ Р ИСО/МЭК 53113-2-2009 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 2. Рекомендации по защите информации, информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов» Федеральное агентство по техническому регулированию и метрологии России, М.: «Стандартинформ», 2010. - 12с.
13. Руководящие документы ФСТЭК России «Требования к системам обнаружения вторжений», введенных приказом ФСТЭК России от 6 декабря 2011 г. № 638 (зарегистрирован Минюстом России 1 февраля 2012 г., рег. №23088) для 4, 5 и 6 классов ИС.
14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год. http://fstec.ru/component/attachments/download/289 .

15. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).
13. Банк данных угроз безопасности информации ФСТЭК России. https://bdu.fstec.ru/threat

б) дополнительная литература

1. Белов, Е. В. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва : Горячая линия - Телеком, 2011. - 544 с. - ISBN 5-93517-292-5. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN5935172925.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.
2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов / Девянин П. Н. - 2-е изд. , испр. и доп. - Москва : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991203289.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249 (дата обращения: 29.01.2022).
4. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие для вузов / Под ред. профессора О. И. Шелухина. - Москва : Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991203234.html (дата обращения: 29.01.2022). - Режим доступа : по подписке.
5. Проскурин В.Г., «Защита программ и данных», 2-е издание, учебное пособие для студ. учреждений высш. проф. образования, М., Издательский центр «Академия», 2012.- 208с

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

старший преподаватель кафедры КБ и ММОИ		А.В. Саханда
должность, ученая степень	*подпись*	*И.О. Фамилия*

Приложение № 1 к рабочей программе дисциплины
«Основы информационной безопасности»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Перечень вопросов для опросов на практических занятиях:

1. В чем суть отличий российской классификации угроз безопасности от принятой в западных стандартах?
2. В чем состоит суть защиты от нарушения конфиденциальности, целостности и доступности информации?
3. В чем состоит суть различных общеупотребимых моделей управления доступом к компьютерной информации?
4. Как определить вероятные цели компьютерной атаки по признакам формы ее реализации?
5. Каковы составляющие российской системы обеспечения безопасности критических информационных систем от компьютерных атак?
6. Каковы функции участников реализации системы обеспечения безопасности критических информационных систем от компьютерных атак?
7. Какие вы знаете модели взаимодействия программной закладки с атакуемой компьютерной системой?
8. Назовите предпосылки к внедрению и методы внедрения программных закладок.
9. В чем особенности компьютерных вирусов, выделяемых в отдельный класс вредоносных программ?
10. Охарактеризуйте жизненный цикл, особенности функционирования, особенности противодействия компьютерным вирусам того или иного класса.
11. В чем состоит отличие утечки информации по техническим каналам от других видов?
12. В чем состоит суть уникальных идентификаторов интернет-пользователей и электронных "отпечатков" работы в социальных сетях?
13. В чем состоит зависимость методик проведения расследования компьютерных инцидентов от поставленных задач, условий их протекания и результатов?
14. В чем состоит суть и цели «Информационной войны»?
15. Какие вы знаете виды «Информационного оружия»?
16. В чем состоят особенности требований ГОСТ Р ИСО/МЭК 18044-2007 «Менеджмент инцидентов информационной безопасности» для решения задач расследования инцидентов безопасности?
17. Какие вы знаете программные средства, применяемые для расследования компьютерных инцидентов?
18. Какие вы знаете методики исследования носителей компьютерной информации?
19. Какие вы знаете цели и задачи проведения Компьютерно-технических экспертиз?

20. Как и на основе каких нормативных правовых документов оформляются результаты проведения компьютерно-технических экспертиз?

21. В чем состоят особенности положений ГОСТ Р ИСО/МЭК 18045-2012 «Методология оценки безопасности информационных технологий» для аттестации объектов с учетом требований к уровню защищенности компьютерных систем?

22. Какие вы знаете методики проведения Компьютерно-технических экспертиз?

23. В чем состоят особенности работ по аттестации объектов с учетом требований к уровню защищенности компьютерных систем, изложенной в ГОСТ Р ИСО/МЭК ТО 19791-2008 «Оценка безопасности автоматизированных систем»?

24. В чем состоят особенности положений ГОСТ Р ИСО/МЭК 27007-2014 «Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью» для аттестации объектов по защищенности компьютерных систем?

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету

1. Перечислите и охарактеризуйте угрозы информационной безопасности Российской Федерации, указанные в «Доктрины информационной безопасности» Российской Федерации.

2. Назовите и опишите цели, задачи и направленность «Доктрины информационной безопасности» Российской Федерации.

3. Сформулируйте и обоснуйте общие принципы построения защиты информации в России.

4. В чем суть российской классификация угроз и ее отличие от принятой в западных стандартах.

5. Дайте обзор средств и методов информационной/компьютерной безопасности, принятых в России.

6. Дайте описание основных методов нарушения конфиденциальности, целостности и доступности информации.

7. Назовите и охарактеризуйте основные модели управления доступом к компьютерной информации.

8. Назовите и охарактеризуйте общепользовательские системы контроля прав доступа к компьютерной информации.

9. На любом произвольном примере опишите Модель вероятного нарушителя, Модель действий вероятного нарушителя, соотнесите их с Моделью построения защиты на основе двух предыдущих.

10. Приведите и охарактеризуйте известные из учебной литературы классификации основных видов компьютерных атак.

11. Опишите и кратко охарактеризуйте методы и тактику проведения сетевой разведки.

12. Опишите элементы системы обеспечения безопасности критических информационных систем от компьютерных атак.

13. Опишите и кратко охарактеризуйте средства и методы нейтрализации компьютерных атак.

14. Приведите известные их учебной литературы классификации вредоносных программ.

15. Опишите и кратко охарактеризуйте признаки присутствия вредоносного ПО.

16. Назовите и охарактеризуйте способы внедрения вредоносного ПО.

17. Назовите и охарактеризуйте методы обнаружения вредоносного ПО.

18. Приведите и охарактеризуйте известные примеры сетевых атак.

19. Дайте определение и охарактеризуйте троянские программы, люки, эксплойты.

20. Назовите и охарактеризуйте методы защиты от вредоносного ПО, технологии самозащиты.

21. Опишите и кратко охарактеризуйте место и роль межсетевых экранов в обеспечении безопасности ресурсов автоматизированных систем.

22. Опишите и кратко охарактеризуйте возможности и ограничения антивирусных программ.

23. Назовите и охарактеризуйте специализированные средства и методы выявления вредоносных программ.

24. Дайте определение и охарактеризуйте термины «Информационная война» и «Информационное оружие».

25. Назовите и охарактеризуйте особенности технических средств ведения информационной войны.

26. Приведите и охарактеризуйте известные из учебной литературы классификации средств защиты информации и нападения на элементы защиты.

27. Приведите и охарактеризуйте известные из учебной литературы классификации электронных устройств перехвата информации, внедряемых в средства вычислительной техники.

28. Опишите и кратко охарактеризуйте средства силового деструктивного воздействия (СДВ).

29. Чем обусловлена необходимость уничтожения документов. Охарактеризуйте особенности удаления информации с современных электронных носителей.

30. Опишите и кратко охарактеризуйте Политику уничтожения данных.

31. Опишите и кратко охарактеризуйте особенности уничтожения конфиденциальной информации (планового и экстренного) на различных носителях.

32. Следы в сети. Опишите и кратко охарактеризуйте уникальные идентификаторы интернет-пользователей и электронные «отпечатки», и относительность «конфиденциальности» в социальных сетях.

33. Назовите и охарактеризуйте средства и методы обнаружения технических каналов утечки информации.

34. Назовите и кратко охарактеризуйте системы защиты конфиденциальных данных от внутренних угроз.

35. Опишите и кратко охарактеризуйте суть и назначение технологии использования цифровых отпечатков.

36. Компьютерно-техническая экспертиза, назовите и охарактеризуйте методы КТ-экспертиз.

37. Методики проведения расследования компьютерных инцидентов в зависимости от поставленных задач, условий их протекания и результатов.

38. Назовите и охарактеризуйте виды и основные методики исследования носителей компьютерной информации.

39. Назовите и охарактеризуйте известные из учебной литературы аппаратно-программные средства, применяемые для расследования компьютерных инцидентов.

40. Приведите пример и поясните суть отдельных элементов методики расследования компьютерных инцидентов.

41. Особенности требований ГОСТ Р ИСО/МЭК 18044-2007 «Менеджмент инцидентов информационной безопасности» для решения задач расследования инцидентов безопасности.

42. Особенности положений ГОСТ Р ИСО/МЭК 18045-2012 «Методология оценки безопасности информационных технологий» для аттестации объектов с учетом требований к уровню защищенности компьютерных систем.

43. Особенности работ по аттестации объектов с учетом требований к уровню защищенности компьютерных систем, изложенной в ГОСТ Р ИСО/МЭК ТО 19791-2008 «Оценка безопасности автоматизированных систем».

44. Особенности положений ГОСТ Р ИСО/МЭК 27007-2014 «Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью» для аттестации объектов по защищенности компьютерных систем.

2. Правила приема зачета.

Оценка знаний по итогу прохождения курса проводится в форме принятия зачета.

На зачете проверяется сформированность всех указанных в учебной программе компетенций.

В билет для зачета включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

Также есть возможность ответить на контрольные вопросы в электронном курсе «Основы информационной безопасности» в LMS Электронный университет Moodle ЯрГУ.

По итогам ответов студенту выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «зачтено» выставляется студенту, если: он знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины, владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется студенту, если: он не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине, не в полной мере владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение №2 к рабочей программе дисциплины
«Основы информационной безопасности»

Методические указания для студентов по освоению дисциплины

Изучение дисциплины предполагает уверенное владение компьютером, умение осуществлять поиск и оценку достоверности необходимой информации в сети Интернет, но студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Основы информационной безопасности». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым в силу обучения на них учащихся сравнительным оценкам знаний из различных источников, критической их оценки. Также без упорных и регулярных самостоятельных занятий в течение семестра, желательно с «упреждающим знакомством» с содержанием предстоящего занятия, крайне сложно усвоить логику и аргументацию упомянутых сравнительных оценок и критического анализа знаний из различных источников, что не позволит студентам развить продвинутого и высокого уровня компетенций.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу, интернет-источники, указанные в разделе 8 настоящей Рабочей программы и электронный курс «Основы информационной безопасности» в LMS Электронный университет Moodle ЯрГУ.