Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. А. Бабаева

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие по изучению дисциплины для студентов
направления подготовки 09.03.03 Прикладная информатика

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент:
доцент кафедры информационной безопасности ФГБОУ ВО
«Калининградский государственный технический университет
А. Г. Жестовский

Бабаева, А. А.
Информационная безопасность: учебно-методическое пособие по изучению дисциплины для студентов направления подготовки 09.03.03 Прикладная информатика / А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 19 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Информационная безопасность» студентами направления подготовки 09.03.03 Прикладная информатика.

Учебно-методическое пособие предназначено для изучения и эффективного освоения теоретических основ обеспечения информационной безопасности организаций, формирования умения и практических навыков применения методов и средств защиты информации

Учебно-методическое пособие рассмотрено и одобрено кафедрой информационной безопасности 14 июня 2022 г., протокол № 9

Учебно-методическое пособие рассмотрено и одобрено методической комиссией Института цифровых технологий 17 февраля 2023 г., протокол № 1

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов направления подготовки 09.03.03 Прикладная информатика, изучающих дисциплину «Информационная безопасность».

Цель освоения дисциплины: приобретение студентом умения решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

В курсе рассматриваются основные положения информационной безопасности и защиты информации. Рассматриваются основные законодательные акты, касающиеся вопросов информационной безопасности. Вводится понятие информации с точки зрения предмета защиты информации, определяются основные категории, которым должна удовлетворять информация. Вводятся понятие атаки на информацию, рассматриваются основные виды атак, последствия от них. Вводятся понятия информационной системы, информационной сети, рассматриваются основные виды угроз на них и способы защиты от этих угроз. Для распределенных компьютерных сетей возможные виды угроз передачи информации рассматриваются с привязкой их к уровням модели межсетевого взаимодействия OSI. Рассматриваются основные стандарты и спецификации в области информационной безопасности, как международные, так и российские, изучаются основные понятия, определенные в них.

Задачи дисциплины:

- изучить основные положения информационной безопасности;
- изучить основные законодательные акты в вопросах ИБ;
- изучить понятия атака, угроза, уязвимость и последствия от их реализации;
- изучить способы защиты от угроз безопасности для ИС и сетей.

Дисциплина «Информационная безопасность» относится к Блоку 1 общепрофессионального модуля программы ООП направления подготовки 09.03.03 Прикладная информатика.

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины; возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе «Содержание дисциплины» приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы) и контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

2. ТЕМАТИЧЕСКИЙ ПЛАН

2.1. Очная форма обучения

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции		
1	Основные понятия информационной безопасности	Тема 1.1: Информация как объект защиты. Законодательные основы по защите информации	1	3
		Тема 1.2: Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы	1	3
		Тема 1.3: Угрозы информационной системы (случайные, преднамеренные воздействия)	1	4
2	Защита доступа к информационным ресурсам	Тема 2.1: Стандартные и специальные права доступа	1	4
		Тема 2.2: Управление правами доступа пользователей/групп к информационным ресурсам	1	3
		Тема 2.3: Базовая стратегия использования групп. Матрица доступа	1	3
3	Особенности защиты информации в компьютерных сетях	Тема 3.1: Информационные компьютерные сети. Удаленные атаки	1	3
		Тема 3.2: Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI	1	4
4	Основы криптографической защиты данных	Тема 4.1: Блочные и потоковые криптосистемы	1	3
		Тема 4.2: Криптосистемы с открытым ключом	1	3
		Тема 4.3: Методы и средства хранения и распределения ключей. Определения и классификация криптопротоколов	1	4
5	Безопасность удаленного доступа и межсетевого взаимодействия	Тема 5.1: Угрозы сетевым компонентам на уровнях модели OSI	1	3
		Тема 5.2: Способы защиты информации в сетях. Протоколы защиты информации в сетях	2	3
		Тема 5.3: Классификация сетевых атак. Межсетевые экраны	2	3
			16	**46**

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лабораторные занятия		
1	Основные понятия информационной безопасности	Средства обеспечения безопасности ОС Windows	6	7
2	Защита доступа к информационным ресурсам	Формирование матрицы доступа и ее реализация	8	6
3	Особенности защиты информации в компьютерных сетях	Симметричные криптосистемы	8	7
4	Основы криптографической защиты данных	Обмен ключами	8	7
5	Безопасность удаленного доступа и межсетевого взаимодействия	Организация межсетевого экрана	8	7
		Изучение антивирусных программных комплексов	8	6,25
			44	**40,25**
		Рубежный (текущий) и итоговый контроль		
		Итоговый контроль (экзамен)	x	33,75
				33,75
		Всего	**60**	**120**

2.2. Заочная форма обучения

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции		
1	Основные понятия информационной безопасности	Тема 1.1: Информация как объект защиты. Законодательные основы по защите информации	1	4
		Тема 1.2: Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы	1	4
		Тема 1.3: Угрозы информационной системы (случайные, преднамеренные воздействия)	2	4
2	Защита доступа к информационным ресурсам	Тема 2.1: Стандартные и специальные права доступа	x	4
		Тема 2.2: Управление правами доступа пользователей/групп к информационным ресурсам	x	4
		Тема 2.3: Базовая стратегия использования групп. Матрица доступа	x	4
3	Особенности защиты информации в компьютерных сетях	Тема 3.1: Информационные компьютерные сети. Удаленные атаки	x	4
		Тема 3.2: Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI	x	4
4	Основы криптографической защиты данных	Тема 4.1: Блочные и потоковые криптосистемы	x	4
		Тема 4.2: Криптосистемы с открытым ключом	x	4
		Тема 4.3: Методы и средства хранения и распределения ключей. Определения и классификация криптопротоколов	x	4
5	Безопасность удаленного доступа и межсетевого взаимодействия	Тема 5.1: Угрозы сетевым компонентам на уровнях модели OSI	x	4
		Тема 5.2: Способы защиты информации в сетях. Протоколы защиты информации в сетях	x	4
		Тема 5.3: Классификация сетевых атак. Межсетевые экраны	x	4
			4	**56**

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лабораторные занятия		
1	Основные понятия информационной безопасности	Средства обеспечения безопасности ОС Windows	2	9
2	Защита доступа к информационным ресурсам	Формирование матрицы доступа и ее реализация	2	9
3	Особенности защиты информации в компьютерных сетях	Симметричные криптосистемы	2	9
4	Основы криптографической защиты данных	Обмен ключами	2	9
5	Безопасность удаленного доступа и межсетевого взаимодействия	Организация межсетевого экрана	1	9
		Изучение антивирусных программных комплексов	1	9
			10	**54**
		Рубежный (текущий) и итоговый контроль		
		Контрольная работа	x	44,5
		Итоговый контроль (экзамен)	x	6,75
				62
		Всего	**14**	**166**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1. Раздел 1 Основные понятия информационной безопасности

3.1.1. Тема 1.1 Информация как объект защиты. Законодательные основы по защите информации

Перечень изучаемых вопросов:

Требования к защите информации. Концепции многоуровневой информационной защиты системы. Структура систем защиты. Объекты и субъекты защиты, понятие и виды защищаемой информации.

Методические указания к изучению:

Рассматриваются основные требования к защите информации, изучаются концепции многоуровневой системы защиты информации и структура защиты для автоматизированных информационных систем. Изучаются вопросы объектов и субъектов защиты и понятия защищаемой информации и ее виды.

Литература:

1. Куприянов, А. И. Основы защиты информации: учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - Москва: Академия, 2008. - 256 с.

2. Галатенко, В. А. Основы информационной безопасности: учеб. пособие / В. А. Галатенко. - 4-е изд. - Москва: Интернет-Университет Информационных технологий : БИНОМ. Лаборатория знаний, 2008. - 205 с.

Контрольные вопросы:

1. Требования к системе защиты информации.
2. Концепция многоуровневой системы ЗИ.
3. Объекты и субъекты защиты, виды защищаемой информации.

3.1.2. Тема 1.2 Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы

Перечень изучаемых вопросов:

Понятие информации, классы защищаемой информации. Особенности создания информационных систем и их виды. Свойства информации с точки зрения информационной безопасности. Конфиденциальность, целостность и доступность информации.

Методические указания к изучению:

Рассматриваются виды информационных систем и особенности обеспечения защиты в них. Изучается понятие информационной системы с точки зрения обеспечения информационной безопасности.

Литература:

1. Галатенко, В. А. Стандарты информационной безопасности: курс лекций: учеб. пособие / В. А. Галатенко; ред. В. Б. Бетелин. - 2-е изд. - Москва: ИНТУИТ.РУ, 2006. – 264 с.

2. Малюк, А. А. Введение в защиту информации в автоматизированных системах: учеб. пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 3-е изд., стер. - Москва: Горячая линия-Телеком, 2005. - 146 с.

Контрольные вопросы:

1. Виды информационных систем.
2. Виды информации и классы защиты.
3. Свойства безопасности информации.

3.1.3. Тема 1.3 Угрозы информационной системы (случайные, преднамеренные воздействия)

Перечень изучаемых вопросов:

Виды угроз информационной безопасности, классификация угроз. Взаимосвязь угроз и уязвимостей. Руководящие документы ФСТЭК.

Методические указания к изучению:

Рассматриваются основные угрозы информационной безопасности и их классификация и особенности. Изучаются основные документы ФСТЭК в области моделирования угроз ИБ и создания списка актуальных угроз.

Литература:

1. Галатенко, В. А. Стандарты информационной безопасности: курс лекций: учеб. пособие / В.А. Галатенко; ред. В. Б. Бетелин. - 2-е изд. - Москва: ИНТУИТ.РУ, 2006. - 264 с.

2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учеб. пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 3-е изд., стер. - Москва: Горячая линия-Телеком, 2005. - 146 с.

Контрольные вопросы:

1. Классификация угроз ИБ.
2. Актуальные угрозы для ИС, способы определения.
3. Руководящие документы ФСТЭК РФ в области моделирования угроз.

3.2. РАЗДЕЛ 2 ЗАЩИТА ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

3.2.1. Тема 2.1 Стандартные и специальные права доступа

Перечень изучаемых вопросов:

Права доступа, виды прав доступа, политики безопасности, понятие администрирования.

Методические указания к изучению:

Рассматриваются основные виды прав доступа, понятие права доступа и способы разграничения, группы пользователей.

Литература:

1. Галатенко, В. А. Стандарты информационной безопасности : курс лекций : учеб. пособие / В.А. Галатенко; ред. В. Б. Бетелин. - 2-е изд. - Москва: ИНТУИТ.РУ, 2006. - 264 с.

2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учеб. пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 3-е изд., стер. - Москва: Горячая линия-Телеком, 2005. - 146 с.

Контрольные вопросы:

1. Право доступа.
2. Виды прав доступа.
3. Способы разграничения прав доступа.

3.2.2. Тема 2.2 Управление правами доступа пользователей/групп к информационным ресурсам

Перечень изучаемых вопросов:

Управление доступом, пользователи и группы, варианты управления доступом и разграничением доступа.

Методические указания к изучению:

Рассматриваются понятия управления доступом и основные способы управления доступом для пользователей отдельных и групп пользователей. Виды информационных ресурсов и правила ограничение доступа к ним.

Литература:

1. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учеб. пособие для студ. высш. учеб. завед.: учеб. пособие / В. И. Завгородний. - Москва: Логос, 2001. – 264 с.

2 Основы информационной безопасности: учеб. пособие / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2006. - 544 с.

Контрольные вопросы:

1. Правила управления доступом.
2. Группы и отдельные пользователи и особенности разграничения доступа для них.
3. Виды информационных ресурсов.

3.2.3. Тема 2.3 Базовая стратегия использования групп. Матрица доступа

Перечень изучаемых вопросов:

Матрица доступа, роли доступа, стратегии использования групп и разграничение доступа на различных уровнях.

Методические указания к изучению:

Рассматриваются понятия матрицы доступа и ролей доступа. Изучаются вопросы применения основных стратегий использования групп и правил разграничения доступа в них.

Литература:

1. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учеб. пособие для студ. высш. учеб. завед.: учеб. пособие / В. И. Завгородний. - Москва: Логос, 2001. – 264 с.
2. Основы информационной безопасности: учеб. пособие / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2006. - 544 с.

Контрольные вопросы:

1. Матрица доступа.
2. Роли доступа и группы пользователей.
3. Стратегии использования групп пользователей для разграничения доступа.

3.3. РАЗДЕЛ 3. ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

3.3.1. Тема 3.1 Информационные компьютерные сети. Удаленные атаки

Перечень изучаемых вопросов:

Способы защиты информации в сетях различного вида, протоколы защиты в сетях и их распределение по уровням модели.

Методические указания к изучению:

Рассматриваются способы защиты информации в сетях и основные протоколы защиты при межсетевом взаимодействии. Подходы к обеспечению безопасности для таких соединений и особенности их использования.

1. Литература:

2. Садердинов, А. А. Информационная безопасность предприятия: учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - 4-е изд. - Москва: Дашков и К°, 2007. - 335 с.
3. Коваленко, Ю. И. Методика защиты информации в организациях [Электронный ресурс]: монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. - Москва: Русайнс, 2018. - 164 с. (ЭБС «Book.ru»).

Контрольные вопросы:

1. Сетевые протоколы.
2. Протоколы защиты в сетях общего пользования.
3. Способы межсетевого взаимодействия.

3.3.2. Тема 3.2 Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI

Перечень изучаемых вопросов:

Модель OSI, уровни модели и распределение протоколов взаимодействия по уровням. Безопасность удаленного доступа и межсетевое взаимодействия. Угрозы компонентам ИС по уровням модели.

Методические указания к изучению:

Рассматривается понятие модели взаимодействия OSI и ее уровни. Изучаются основные угрозы сетевым компонентам на различных уровнях модели и актуальные угрозы для всех типом компонентов ИС.

Литература:

1. Садердинов, А. А. Информационная безопасность предприятия: учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - 4-е изд. - Москва: Дашков и К°, 2007. - 335 с.

2. Коваленко, Ю. И. Методика защиты информации в организациях [Электронный ресурс]: монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. - Москва: Русайнс, 2018. - 164 с. (ЭБС «Book.ru»).

Контрольные вопросы:

1. Модель OSI, уровни.
2. Угрозы компонентам ИС.
3. Межсетевое взаимодействие: особенности.

3.4. РАЗДЕЛ 4 ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ

3.4.1. Тема 4.1 Блочные и потоковые криптосистемы

Перечень изучаемых вопросов:

Криптосистемы и их виды. Блочные и потоковые криптосистемы. Основы криптографической защиты.

Методические указания к изучению:

Рассматривается понятие криптографической защиты, основные направления. Изучаются блочные и потоковые криптосистемы и вопросы особенности их использования. Преимущества и недостатки, область применения.

Литература:

1. Информационная безопасность открытых систем: в 2 т.: учеб. / С. В. Запечников [и др.]. - Москва: Горячая линия-Телеком, 2006. - Т. 1: Угрозы, уязвимости, атаки и подходы к защите. - 535 с. 8.

2. Рябко, Б.Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия-Телеком, 2005. - 229 с.

Контрольные вопросы:

1. Основы криптографической защиты.
2. Блочные и потоковые криптосистемы.
3. Виды криптосистем.
4. Преимущества и недостатки различных подходов при криптозащите.

3.4.2. Тема 4.2 Криптосистемы с открытым ключом

Перечень изучаемых вопросов:

Виды криптосистем по типу ключа, криптосистемы с открытым ключом, их особенности и область применения.

Методические указания к изучению:

Рассматривается вопрос применения различных типов ключей в области криптошифрования. Изучаются особенности использования криптосистем с открытым ключом и их преимущества и недостатки.

Литература:

1. Информационная безопасность открытых систем: в 2 т.: учеб. / С. В. Запечников [и др.]. - Москва: Горячая линия-Телеком, 2006. - Т. 1: Угрозы, уязвимости, атаки и подходы к защите. - 535 с. 8.

2. Рябко, Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия-Телеком, 2005. - 229 с.

Контрольные вопросы:

1. Открытые и закрытые ключи шифрования.
2. Криптосистемы с открытым ключом.
3. Преимущества и недоставки систем крипто защиты с открытыми ключами.

3.4.3. Тема 4.3 Методы и средства хранения и распределения ключей. Определения и классификация криптопротоколов

Перечень изучаемых вопросов:

Методы и средства хранения и распределения ключей. Определения и классификация криптопротоколов.

Методические указания к изучению:

Рассматриваются понятия криптопротоколов и их классификация. Изучаются вопросы методов и средств хранения и распределения ключей. Сертификаты ключей.

Литература:

1. Информационная безопасность открытых систем: в 2 т.: учеб. / С. В. Запечников [и др.]. - Москва: Горячая линия-Телеком, 2006. - Т. 1: Угрозы, уязвимости, атаки и подходы к защите. - 535 с. 8.

2. Рябко, Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия-Телеком, 2005. - 229 с.

Контрольные вопросы:

1. Криптопротоколы.
2. Методы и средства хранения ключей.
3. Методы распределения ключей.

3.5. РАЗДЕЛ 5 БЕЗОПАСНОСТЬ УДАЛЕННОГО ДОСТУПА И МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

3.5.1. Тема 5.1 Угрозы сетевым компонентам на уровнях модели OSI

Перечень изучаемых вопросов:

Уровни модели и распределение протоколов взаимодействия по уровням. Безопасность удаленного доступа и межсетевое взаимодействие. Угрозы компонентам ИС по уровням модели.

Методические указания к изучению:

Рассматривается понятие модели взаимодействия OSI и ее уровни. Изучаются основные угрозы сетевым компонентам на различных уровнях модели и актуальные угрозы для всех типов компонентов ИС.

Литература:

1. Садердинов, А. А. Информационная безопасность предприятия: учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - 4-е изд. - Москва: Дашков и К°, 2007. - 335 с.

2. Коваленко, Ю. И. Методика защиты информации в организациях [Электронный ресурс]: монография / Ю. И. Коваленко, Г.И. Москвитин, М. М. Тараскин. - Москва: Русайнс, 2018. - 164 с. (ЭБС «Book.ru»).

Контрольные вопросы:

1. Уровни модели.
2. Угрозы сетевым компонентам.
3. Безопасность межсетевого взаимодействия.

3.5.2. Тема 5.2 Способы защиты информации в сетях. Протоколы защиты информации в сетях

Перечень изучаемых вопросов:

Способы защиты информации в сетях различного вида, протоколы защиты в сетях и их распределение по уровням модели.

Методические указания к изучению:

Рассматриваются способы защиты информации в сетях и основные протоколы защиты при межсетевом взаимодействии. Подходы к обеспечению безопасности для таких соединений и особенности их использования.

Литература:

1. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учеб. пособие для студ. высш. учеб. завед.: учеб. пособие / В. И. Завгородний. - Москва: Логос, 2001. – 264 с.

2. Основы информационной безопасности: учеб. пособие / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2006. - 544 с.

Контрольные вопросы:

1. Сетевые протоколы.
2. Протоколы защиты в сетях общего пользования.
3. Способы межсетевого взаимодействия.

3.5.3. Тема 5.3 Классификация сетевых атак. Межсетевые экраны

Перечень изучаемых вопросов:

Сетевые атаки, виды сетевых атак. Атаки на отказ в обслуживании, атаки типа «человек посередине». Межсетевые экраны, их разновидности, способы настройки и особенности применения в области ИБ.

Методические указания к изучению:

Рассматривается необходимость применения межсетевых экранов в процессе передачи информации по сетям общего пользования. Изучаются основные группы и виды межсетевых экранов, их особенности и область применения.

Литература:

1. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учеб. пособие для студ. высш. учеб. завед.: учеб. пособие / В. И. Завгородний. - Москва: Логос, 2001. – 264 с.

2. Основы информационной безопасности: учеб. пособие / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2006. - 544 с.

Контрольные вопросы:

1. Межсетевые экраны, их виды.
2. Сетевые атаки, классификация.
3. Особенности применения межсетевых экранов в области защиты ИС.

4. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1. ТЕКУЩАЯ АТТЕСТАЦИЯ

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: контроль самостоятельной работы по темам дисциплины, контроль выполнения лабораторных работ, контрольные работы в виде ответов на вопросы.

4.2. УСЛОВИЯ ПОЛУЧЕНИЯ ПОЛОЖИТЕЛЬНОЙ ОЦЕНКИ:

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой экзамен

Критерии оценок на **дифференцированном экзамене** по дисциплине (отлично, хорошо, удовлетворительно, неудовлетворительно):

- «ОТЛИЧНО» выставляется в случае правильных, полных и четких ответов на теоретические вопросы, с их проецированием и интерпретацией на сегодняшнюю ситуацию. Допускаются непринципиальные погрешности или небольшая незавершенность ответов, диктуемых лимитом времени.

- «ХОРОШО» - в случаях: правильных и четких ответов при незначительных замечаниях, неточностях.

- «УДОВЛЕТВОРИТЕЛЬНО» - в случаях ответа на большую часть (не менее 50 % основных положений); при правильном ответе на один вопрос или неполных ответах на два вопроса.

- «НЕУДОВЛЕТВОРИТЕЛЬНО» - при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

К экзамену допускаются студенты, имеющие по всем текущим контролям положительные оценки.

4.3. ПРИМЕРНЫЕ ВОПРОСЫ К ЗАЧЕТУ/ЭКЗАМЕНУ ПО ДИСЦИПЛИНЕ

1. Предмет дисциплины «Информационная безопасность и защита информации».
2. Теория и методология информационной безопасности, ее основные понятия.
3. Угрозы национальной безопасности в информационной сфере и их источники.
4. Система обеспечения информационной безопасности.
5. Государственные органы, выполняющие функции обеспечения информационной безопасности и защиты информации.
6. Понятие информации, ее виды и критерии оценки.
7. Задачи, методы и средства защиты информации.
8. Понятие уязвимости и угрозы информации.
9. Источники утраты конфиденциальности и искажения информации.
10. Понятие и виды информационных ресурсов. Информационные ресурсы государственного значения.
11. Понятие конфиденциальности. Критерии выделения информации ограниченного распространения.
12. Классификация противоправных способов получения конфиденциальной информации. Понятие шпионажа и его виды.
13. Правовые способы обеспечения защиты информации.
14. Лицензионная и сертификационная деятельность в области защиты информации.
15. Юридическая ответственность в области информационных отношений и ее виды.
16. Понятие преступления в информационной сфере. Характеристика основных составов преступлений, связанных с информационными отношениями.
17. Правовой режим государственной тайны.
18. Правовой режим служебной тайны.
19. Правовой режим коммерческой тайны.
20. Профессиональные тайны как вид информации ограниченного распространения, особенности их правового режима.

21. Особенности правового режима личной тайны, обеспечение тайны переписки, телефонных переговоров и иных сообщений.

22. Понятие и правовой режим персональных данных.

23. Понятие и виды организационных мер обеспечения информационной безопасности и защиты информации.

24. Анализ и оценка угроз информационной безопасности объекта.

25. Регламентация допуска и доступа персонала к конфиденциальной информации.

26. Служба безопасности, её структура и задачи по обеспечению информационной безопасности.

27. Задачи и способы подбора персонала на работу, связанную с использованием конфиденциальной информации.

28. Предупредительные и профилактические меры, направленные на предотвращение разглашения персоналом конфиденциальной информации.

29. Организация защиты информации при подготовке и проведении совещаний и переговоров.

30. Понятие и виды технических мер обеспечения информационной безопасности и защиты информации.

31. Виды угроз информационной безопасности, исходящих по техническим каналам.

32. Средства и методы технической защиты объектов и информации.

33. Правовое регулирование защиты информации с использованием технических средств. Регламентация использования технических средств защиты информации (вопросы лицензирования и сертификации).

34. Угрозы безопасности информации в процессе использования компьютеров, локальных сетей и средств связи.

35. Виды охраняемых объектов, категории защищаемых помещений. Задачи и направления охраны объектов.

5. ЗАКЛЮЧЕНИЕ

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их как непосредственно в ходе занятий, так и в ходе самостоятельной работы. Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, не подкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста);
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы.

Работа студентов в основном складывается из следующих элементов:

- изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам;
- подготовка и сдача итогового экзамена.

6. ЛИТЕРАТУРА

1. Куприянов, А. И. Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - Москва : Академия, 2008. - 256 с.

2. Бабаш, А. В. Криптографические методы защиты информации [Электронный ресурс]: учебник / А.В. Бабаш, Е.К. Баранова. - Москва: КноРус, 2018. - 190 с. (ЭБС «Book.ru»).

3. Галатенко, В. А. Основы информационной безопасности : учеб. пособие / В. А. Галатенко. - 4-е изд. - Москва : Интернет-Университет Информационных технологий : БИНОМ. Лаборатория знаний, 2008. - 205 с.

4. Сердюк, В.А. Организация и технологии защиты информации [Электронный ресурс] : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. (ЭБС «Университетская библиотека онлайн»).

Дополнительная литература:

1. Баранова, Е.К. Криптографические методы защиты информации. Лабораторный практикум [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш. - Москва: КноРус, 2017. - 200 с. (ЭБС «Book.ru»).

2. Садердинов, А. А. Информационная безопасность предприятия : учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - 4-е изд. - Москва : Дашков и К°, 2007. - 335 с.

3. Коваленко, Ю. И. Методика защиты информации в организациях [Электронный ресурс]: монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. - Москва: Русайнс, 2018. - 164 с. (ЭБС «Book.ru»).

4. Малюк, А. А. Информационная безопасность : концептуальные и методологические основы защиты информации : учеб. пособие / А. А. Малюк. - Москва : Горячая линия-Телеком, 2004. - 280 с.

5. Галатенко, В. А. Стандарты информационной безопасности : курс лекций : учеб. пособие / В. А. Галатенко; ред. В. Б. Бетелин. - 2-е изд. - Москва: ИНТУИТ.РУ, 2006. – 264 с.

6. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учеб. пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 3-е изд., стер. - Москва : Горячая линия-Телеком, 2005. - 146 с.

Локальный электронный методический материал

Алина Андреевна Бабаева

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Редактор М. А. Дмитриева

Уч.-изд. л. 0,9. Печ. л. 1,2.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1