АНО ВО «Межрегиональный открытый социальный институт»

УТВЕРЖДЕНО
на заседании Совета факультета
экономики и информационной безопасности
Протокол заседания Совета факультета
№ 12 « 18 » апреля 2018 г.
Декан факультета экономики и
информационной безопасности
_____Т.А. Сафина

ОДОБРЕНО
на заседании кафедры информационной
безопасности
Протокол заседания кафедры
№ 10 « 30 » мая 2018 г.
Зав. кафедрой информационной
безопасности _____Т.М. Гусакова

РАБОЧАЯ ПРОГРАММА

по дисциплине Основы информационной безопасности
(наименование)

образовательная программа 38.03.05 Бизнес-информатика, «Электронный бизнес»

форма обучения очная, заочная

ПРОГРАММА РАЗРАБОТАНА

доцент, канд. техн. наук, доцент
Кречетов А.А.
(должность, Ф. И. О., ученая степень, звание автора(ов) программы)

Йошкар-Ола, 2018

Содержание

1. Пояснительная записка

Цель изучения дисциплины: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Место дисциплины в учебном плане:

Предлагаемый курс относится к обязательным дисциплинам вариативной части образовательной программы 38.03.05 Бизнес-информатика. Электронный бизнес.

Дисциплина «Основы информационной безопасности» обеспечивает овладение следующими компетенциями:

продолжает формирование общепрофессиональной компетенции:

способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1) – 5/6 этап;

начинает формирование профессиональной компетенции:

организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия (ПК-9) – 1/1 этап.

Этапы формирования компетенции
(очная форма обучения)

Код компетенции	Формулировка компетенции	Учебная дисциплина	Семестр	Этап
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Теоретические основы информатики	1	1
		Введение в профессию		
		Общая теория систем	3	2
		Анализ данных		
		Информационные технологии	4	3
		Вычислительные системы, сети, телекоммуникации	5	4
		Рынки ИКТ и организация продаж		
		Учебная практика (практика по получению первичных профессиональных умений и навыков)		
		Моделирование бизнес-процессов	6	5
		Основы информационной безопасности		
		Распределенные	7	6

		системы		
		Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)		
		Производственная практика (преддипломная практика)	8	7
		Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	Основы информационной безопасности	6	1
		Управление информационной безопасностью IT-инфраструктуры	7	2
		Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)		
		Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3

Этапы формирования компетенции
(заочная форма обучения)

Код компетенции	Формулировка компетенции	Учебная дисциплина	Семестр	Этап
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической	Теоретические основы информатики	1	1
		Введение в профессию		
		Информационные технологии	2	2
		Общая теория систем	3	3
		Анализ данных	4	4

	культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Вычислительные системы, сети, телекоммуникации	5	5
		Рынки ИКТ и организация продаж		
		Основы информационной безопасности	6	6
		Учебная практика (практика по получению первичных профессиональных умений и навыков)		
		Распределенные системы	7	7
		Моделирование бизнес-процессов	8	8
		Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)		
		Производственная практика (преддипломная практика)	10	9
		Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	Основы информационной безопасности	6	1
		Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)	8	2
		Управление информационной безопасностью IT-инфраструктуры	10	3

		Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		

В результате освоения дисциплины обучающийся должен:

ОПК-1	**Знать:** -об использовании основных положений теории информационной безопасности на различных уровнях (законодательном, административном, организационном, программно-техническом); -технические и программные средства обеспечения безопасности информационных систем используемых для обеспечения защиты в сфере электронного бизнеса; -методику выбора оптимального решения по уровню информационной безопасности как компромисса между различными требованиями, связанными с безопасностью, качеством разработки, стоимостью и сроками выполнения работ; -основные понятия и задачи криптографии; -способы разграничения доступа и средства их реализации; **Уметь:** -правильно выбирать и применять меры законодательного, административного, организационного и программно-техническом уровня для обеспечения информационной безопасности; -использовать в практической деятельности существующие методы и средства контроля и защиты информации; -применять программные пакеты для шифрования; **Владеть:** -средствами борьбы с компьютерными вирусами; -навыками подбора и использования программно-технических средств ограничения доступа к нежелательному контенту; -навыками обнаружения примеров всех изучаемых явлений в СМИ, Интернет и во время виртуального общения; -внедрения и эксплуатации сервисов информационной безопасности программно-технического уровня, меры законодательного, административного и организационного уровней информационной безопасности.
ПК-9	**Знать:** о современных направлениях и перспективах развития защиты информации. **Уметь:** -правильно проводить анализ угроз информационной безопасности; -выполнять основные этапы решения задач информационной безопасности; -применять на практике основные общеметодологические принципы теории информационной безопасности в сфере электронного бизнеса. **Владеть:** методами обеспечения информационной безопасности в электронном бизнесе.

Формы текущего контроля успеваемости студентов: устный опрос, реферат, практические задачи

Форма промежуточной аттестации: зачет.

Структура и содержания дисциплины

Трудоемкость 3 зачетные единицы, 108 часов, из них:

очная форма обучения: 16 лекционных, 34 практических, 58 часов самостоятельной работы;

заочная форма обучения: 4 лекционных, 8 практических, 92 часа самостоятельной работы, 4 часа контроль.

2.1. Тематический план учебной дисциплины (очная форма обучения)

№ п/п раздела	Наименование разделов и тем	Количество часов по учебному плану				
		Всего	Виды учебной работы			
			Аудиторная работа			Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные занятия	
1	2	3	4	5	6	7
1	Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности	20	4	6	-	10
2	Тема 2 Терминологические основы информационной безопасности	16	2	6	-	8
3	Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности	16	2	6	-	8
4	Тема 4 Модель угроз, модель нарушителя	14	2	4	-	8
5	Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности	14	2	4	-	8
6	Тема 6 Функции и задачи защиты информации	14	2	4	-	8
7	Тема 7 Проблемы региональной информационной безопасности	14	2	4	-	8
	Итого	**108**	**16**	**34**	**-**	**58**

(заочная форма обучения)

№ п/п раздела	Наименование разделов и тем	Количество часов по учебному плану				
		Всего	Виды учебной работы			
			Аудиторная работа			Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные занятия	
1	**2**	**3**	**4**	**5**	**6**	**7**
1	Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности	16	2	2	-	12
2	Тема 2 Терминологические основы информационной безопасности	16	2	2	-	12
3	Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности	14	-	2	-	12
4	Тема 4 Модель угроз, модель нарушителя	16	-	2	-	14
5	Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности	14	-	-	-	14
6	Тема 6 Функции и задачи защиты информации	14	-	-	-	14
7	Тема 7 Проблемы региональной информационной безопасности	14	-	-	-	14
	Итого	**104**	**4**	**8**	**-**	**92**

2.2. Тематический план лекций:

№ п/п раздела	Наименование разделов и тем	Количество часов
1	**2**	**3**
1	Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности	4/2
2	Тема 2 Терминологические основы информационной безопасности	2/2
3	Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности	2/-
4	Тема 4 Модель угроз, модель нарушителя	2/-
5	Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности	2/-
6	Тема 6 Функции и задачи защиты информации	2/-
7	Тема 7 Проблемы региональной информационной безопасности	2/-
	Итого	**16/4**

Содержание лекционных занятий

Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности

План:

1. Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи.
2. Национальные интересы Российской Федерации в информационной сфере. Приоритетные направления в области защиты информации в Российской Федерации.
3. Тенденции развития информационной политики государств и ведомств. Информационная война, проблемы.
4. Правовое обеспечение защиты информации.
5. Информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные.

Тема 2 Терминологические основы информационной безопасности

План:

1. Понятие информации и смежных ним: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Защита информации, тайна, средства защиты информации, угрозы — определения, сопоставление.
4. Идентификация, аутентификация, авторизация

Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности

План:

1. Понятие угрозы. Виды угроз.
2. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.
3. Характер происхождения угроз: умышленные факторы, естественные факторы.
4. Источники угроз.
5. Предпосылки появления угроз: объективные, субъективные.

Тема 4 Модель угроз, модель нарушителя

План:

1. Классы каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.
2. Причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.
3. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.
4. Формирование модели нарушителя.

Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности

План:

1. Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.
2. Модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием.
3. Последовательность решения задачи защиты информации.
4. Фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации.
5. Требования разделены на три группы: стратегия, подотчетность, гарантии.
6. Классификация автоматизированных систем и требований по защите информации. Факторы, влияющие на требуемый уровень защиты информации.

Тема 6 Функции и задачи защиты информации

План:

1. Методы формирования функций защиты. Скрытие информации о средствах, комплексах, объектах и системах обработки информации.
2. Дезинформация противника. Легендирование. Введение избыточности элементов системы. Резервирование элементов системы.
3. Регулирование доступа к элементам системы и защищаемой информации. Регулирование использования элементов системы и защищаемой информации.
4. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования.
5. Управление системой защиты информации. Обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.
6. Защита от информационного воздействия на технические средства обработки. Защита от информационного воздействия на общество. Защита от информационного воздействия на психику человека

Тема 7 Проблемы региональной информационной безопасности

План:

1. Региональные компоненты защиты информации.

2. Защита информации предприятия. Проведение анализа защищенности локального объекта.

Основная литература

Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Дополнительная литература

1. Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605 (Электронная библиотечная система «Университетская библиотека ONLINE»)

2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин : Директ-Медиа, 2015. - 105 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895 (Электронная библиотечная система «Университетская библиотека ONLINE»)

3. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т. Хаулет. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 566 с. : ил. - (Основы информационных технологий); То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429025 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Информационно-справочные системы,
профессиональные базы данных и интернет-ресурсы

1. Сайт Security Lab [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/ (новости, экспертные статьи, софты, форум, раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению)

2. Сайт Threatpost [Электронный ресурс]. – Режим доступа: https://threatpos (содержит новости об информационной безопасности от Kaspersky Lab)

3. Сайт Anti-Malware [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/ (содержит сравнительные тесты антивирусов, аналитические статьи)

4. Сайт Научного журнал «Вопросы кибербезопасности» [Электронный ресурс]. – Режим доступа: http://cyberrus.com/ (содержит статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации)

5. Профессиональная база данных по бизнес-информатике [Электронный ресурс]. - Режим доступа: http://dorlov.blogspot.ru/p/blog-page_3151.html

6. СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г

2.3. Тематический план практических (семинарских) занятий

№ п/п раздела	Наименование разделов и тем	Количество часов
1	**2**	**3**
1	Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности	6/2
2	Тема 2 Терминологические основы информационной безопасности	6/2
3	Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности	6/2
4	Тема 4 Модель угроз, модель нарушителя	4/2
5	Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности	4/-
6	Тема 6 Функции и задачи защиты информации	4/-
7	Тема 7 Проблемы региональной информационной безопасности	4/-
	Итого	**34/8**

Семинарские занятия по темам

Тема 2 Терминологические основы информационной безопасности

План:

1. Анализ терминов и определений информационной безопасности.
2. ГОСТы и руководящие документы.

Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности

План:

1. Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации.

Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности

План:

1. Построение модели угроз для выбранного объекта информатизации.

Тема 6 Функции и задачи защиты информации

План:

1. Оценка безопасности информации на объектах ее обработки.

Практические задания

Задание 1. Методы поиска и сбора информации.

Цель работы: Приобретение навыков поиска информации используя поисковые системы.

Задачи:

1. Поисковые системы. Методика поиска.
2. Рассылки, тематические форумы.
3. Возможности использования иноязычных ресурсов.

Задание 2. Методика устранения компьютерной информации.

Цель работы: Приобретение навыков устранения и восстановления информации на различных носителях.

Задачи:

1. Физическая организация жестких дисков.
2. Методы восстановления информации.
3. Обзор современных средств устранения компьютерной информации.

Задание 3. Уязвимости Windows.

Цель работы: Приобретение навыков настройки Windows для уменьшения уязвимостей.

Задачи:

1.Недостатки архитектуры операционных систем семейства Windows .

2.Основные виды уязвимостей: статистика их обнаружения и устранения.

3.Описание методик атак, использующих уязвимости операционной системы семейства Windows.

4.Настройка операционной системы для увеличения обороноспособности вычислительной системы.

Задание 4. Защита от копирования переносных носителей.

Цель работы: Приобретение навыков защиты от копирования переносных носителей.

Задачи:

1. Методика защиты программных и установочных дисков.
2. Методика защиты дисков с данными.
3. Современные средства защиты видеодисков.

Задание 4. Аппаратные ключи защиты.

Цель работы: Приобретение навыков защиты данных с помощью аппаратных ключей.

Задачи:

1. Основные виды аппаратных ключей.
2. Методики обхода аппаратных ключей.
3. Недостатки аппаратных ключей

Задание 5. Навесная защита

Цель работы: Приобретение навыков защиты информации используя программое обеспечение.

Задачи:

1. Методика установки протекторов.
2. Работа протекторов.
3. Недостатки протекторов.

Задание 6. Антивирусное программное обеспечение.

Цель работы: Приобретение навыков защиты информации используя антивирусное программное обеспечение.

Задачи:

1. Программы-шпионы. Защита от программ шпионов.
2. Троянские программы.
3. "Черви", методики проникновения.
4. Вирусы, алгоритмы работы.
5. Антивирусное программное обеспечение: рекомендуемые настройки, правила использования.

Задание 7. Особенности защиты информации при работе в сети.

Цель работы: Приобретение навыков защиты информации при работе в сети.

Задачи:

1. Средства управления сетями.
2. Программные средства обеспечения защиты информации в локальной сети.

3. Обязанности администратора сети, относящиеся к безопасности информации.
4. Средства обнаружения сетевых атак.

Задание 8. Безопасная работа в Internet.

Цель работы: Приобретение навыков безопасной работы в сети интернет.

Задачи:

1. Выбор сайтов для посещения.
2. Настройка встроенных средств защиты информации современных браузеров.
3. Обработка сообщений электронной почты. Спам-фильтры.
4. Ограничение доступа из локальной сети в Internet с помощью proxy- серверов.
5. Типы межсетевых экранов, их достоинства и недостатки

Основная литература

Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Дополнительная литература

1. Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605 (Электронная библиотечная система «Университетская библиотека ONLINE»)

2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин : Директ-Медиа, 2015. - 105 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895 (Электронная библиотечная система «Университетская библиотека ONLINE»)

3. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т. Хаулет. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 566 с. : ил. - (Основы информационных технологий); То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429025 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Информационно-справочные системы, профессиональные базы данных и интернет-ресурсы

1. Сайт Security Lab [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/ (новости, экспертные статьи, софты, форум, раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению)
2. Сайт Threatpost [Электронный ресурс]. – Режим доступа: https://threatpos (содержит новости об информационной безопасности от Kaspersky Lab)
3. Сайт Anti-Malware [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/ (содержит сравнительные тесты антивирусов, аналитические статьи)
4. Сайт Научного журнал «Вопросы кибербезопасности» [Электронный ресурс]. – Режим доступа: http://cyberrus.com/ (содержит статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации)
5. Профессиональная база данных по бизнес-информатике [Электронный ресурс]. - Режим доступа: http://dorlov.blogspot.ru/p/blog-page_3151.html

6. СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г

2.4. Тематический план для самостоятельной работы

№ п/п раздела	Наименование разделов и тем	Количество часов
1	**2**	**3**
1	Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности	10/12
2	Тема 2 Терминологические основы информационной безопасности	8/12
3	Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности	8/12
4	Тема 4 Модель угроз, модель нарушителя	8/14
5	Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности	8/14
6	Тема 6 Функции и задачи защиты информации	8/14
7	Тема 7 Проблемы региональной информационной безопасности	8/14
	Итого	**58/92**

Вопросы для самостоятельной работы

Тема 1 Понятие информационной безопасности, ее роль в национальной безопасности

План:

1. Назовите органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи.
2. Охарактеризуйте национальные интересы Российской Федерации в информационной сфере. Каковы приоритетные направления в области защиты информации в Российской Федерации?
3. Каковы тенденции развития информационной политики государств и ведомств? Что такое информационная война?
4. Охарактеризуйте правовое обеспечение защиты информации.
5. Что такое информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные?

Тема 2 Терминологические основы информационной безопасности

План:

1. Что такое информация? Дайте характеристику смежным с ним понятиям: информационная безопасность, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации.
2. Кто такое автор и собственник информации? Как взаимодействуют субъекты в информационном обмене?
3. Что такое защита информации, тайна, средства защиты информации, угрозы?
4. Что такое идентификация, аутентификация, авторизация?

Тема 3 Угрозы. Классификация и анализ угроз информационной безопасности

План:

1. Что такое угроза? Перечислите виды угроз.
2. Охарактеризуйте три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной

(случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

3. Назовите особенности происхождения угроз: умышленные факторы, естественные факторы.

4. Каковы источники угроз?

5. Назовите предпосылки появления угроз: объективные, субъективные.

Тема 4 Модель угроз, модель нарушителя

План:

1. Дайте характеристику классам каналов несанкционированного получения информации: 1) непосредственно с объекта; 2) с каналов отображения информации; 3) получение по внешним каналам; 4) подключение к каналам получения информации.

2. Назовите причины нарушения целостности информации: субъективные преднамеренные, субъективные непреднамеренные, объективные непреднамеренные.

3. Назовите потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.

4. Как происходит формирование модели нарушителя?

Тема 5 Модели оценки угроз конфиденциальности, целостности, доступности

План:

1. Назовите три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

2. Какова модель затрат, разработанная специалистами американской фирмы IBM. Модель защиты — модель системы с полным перекрытием.

3. Какова последовательность решения задачи защиты информации?

4. Назовите фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации.

5. Дайте классификацию автоматизированных систем и требований по защите информации. Назовите факторы, влияющие на требуемый уровень защиты информации.

Тема 6 Функции и задачи защиты информации

План:

1. Перечислите методы формирования функций защиты. Как происходит скрытие информации о средствах, комплексах, объектах и системах обработки информации?

2. Что такое дезинформация противника? Что такое легендирование? Как происходит резервирование элементов системы?

3. Как происходит регулирование доступа к элементам системы и защищаемой информации. Как происходит регулирование использования элементов системы и защищаемой информации?

4. Что такое маскировка информации? Как происходит регистрация сведений? Как уничтожается информация? Обеспечение сигнализации. Обеспечение реагирования.

5. Что такое управление системой защиты информации? Как происходит обеспечение требуемого уровня готовности обслуживающего персонала к решению задач информационной безопасности.

6. Как осуществляется защита от информационного воздействия на технические средства обработки? Что такое защита от информационного воздействия на общество? Как осуществляется защита от информационного воздействия на психику человека?

Тема 7 Проблемы региональной информационной безопасности

План:

1. Что такое региональные компоненты защиты информации?
2. Как осуществляется защита информации предприятия?
3. Как проводится анализ защищенности локального объекта?

Основная литература

Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Дополнительная литература

1. Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605 (Электронная библиотечная система «Университетская библиотека ONLINE»)

2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин : Директ-Медиа, 2015. - 105 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895 (Электронная библиотечная система «Университетская библиотека ONLINE»)

3. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т. Хаулет. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 566 с. : ил. - (Основы информационных технологий); То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429025 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Информационно-справочные системы,
профессиональные базы данных и интернет-ресурсы

1. Сайт Security Lab [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/ (новости, экспертные статьи, софты, форум, раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению)
2. Сайт Threatpost [Электронный ресурс]. – Режим доступа: https://threatpos (содержит новости об информационной безопасности от Kaspersky Lab)
3. Сайт Anti-Malware [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/ (содержит сравнительные тесты антивирусов, аналитические статьи)
4. Сайт Научного журнал «Вопросы кибербезопасности» [Электронный ресурс]. – Режим доступа: http://cyberrus.com/ (содержит статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации)
5. Профессиональная база данных по бизнес-информатике [Электронный ресурс]. - Режим доступа: http://dorlov.blogspot.ru/p/blog-page_3151.html
6. СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г

Перечень тем рефератов по дисциплине «Основы информационной безопасности»

1.Методы борьбы с фишинговыми атаками.

2.Законодательство о персональных данных.

3.Защита авторских прав.

4.Назначение, функции и типы систем видеозащиты.

5.Как подписывать с помощью ЭЦП электронные документы различных форматов.

6.Обзор угроз и технологий защиты Wi-Fi-сетей.

7.Проблемы внедрения дискового шифрования.

8.Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

9.Особенности процессов аутентификации в корпоративной среде.

10.Квантовая криптография.

11.Утечки информации: как избежать. Безопасность смартфонов.

12.Безопасность применения пластиковых карт - законодательство и практика.

13.Защита CD- и DVD-дисковот копирования.

14.Современные угрозы и защита электронной почты.

15.Программные средства анализа локальных сетей на предмет уязвимостей.

16.Безопасность применения платежных систем - законодательство и практика.

17.Аудит программного кода по требованиям безопасности.

18.Антишпионское ПО (antispyware).

19.Обеспечение безопасности Web-сервисов.

20.Защита от внутренних угроз.

21.Технологии RFID.

22.Уничтожение информации на магнитных носителях.

23.Ботнеты - плацдарм современных кибератак.

24.Цифровые водяные знаки в изображениях.

25.Электронный документооборот. Модели нарушителя.

26.Идентификация по голосу. Скрытые возможности.

27.Безопасность океанских портов.

28.Безопасность связи.

29.Безопасность розничной торговли.

30.Банковская безопасность.

31.Информатизация управления транспортной безопасностью.

32.Биопаспорт.

33.Обзор современных платформ архивации данных.

34.Что такое консалтинг в области ИБ.

35.Бухгалтерская отчетность как источник рассекречивания информации.

36.Управление рисками: обзор употребительных подходов.

37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38.Распределенные атаки на распределенные системы.

39.Оценка безопасности автоматизированных систем.

40.Windows и Linux: что безопаснее?

41.Функциональная безопасность программных средств.

42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43.Информационная безопасность: экономические аспекты.

Средство оценивания: реферат

Шкала оценивания:

Реферат оценивается по 100-балльной шкале. Баллы переводятся в оценки успеваемости следующим образом:

86-100 баллов – «отлично»;

70- 85 баллов – «хорошо»;

51-69 баллов – «удовлетворительно;

менее 51 балла – «неудовлетворительно».

Критерии	Показатели
1. Новизна реферированного текста. Максимальная оценка – 20 баллов	актуальность проблемы и темы; – новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; – наличие авторской позиции, самостоятельность суждений.
2. Степень раскрытия сущности проблемы. Максимальная оценка – 30 баллов	– соответствие плана теме реферата; – соответствие содержания теме и плану реферата; – полнота и глубина раскрытия основных понятий проблемы; – обоснованность способов и методов работы с материалом; – умение работать с историческими источниками и литературой, систематизировать и структурировать материал; – умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы
3. Обоснованность выбора источников и литературы. Максимальная оценка – 20 баллов	круг, полнота использования исторических источников и литературы по проблеме; – привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов, интернет-ресурсов и т. д.).
4. Соблюдение требований к оформлению. Максимальная оценка – 15 баллов.	правильное оформление ссылок на использованные источники и литературу; – грамотность и культура изложения; – использование рекомендованного количества исторических источников и литературы; – владение терминологией и понятийным аппаратом проблемы; – соблюдение требований к объему реферата; – культура оформления: выделение абзацев, глав и параграфов
5. Грамотность. Максимальная оценка – 15 баллов.	– отсутствие орфографических и синтаксических ошибок, стилистических

	погрешностей; – отсутствие опечаток, сокращений слов, кроме общепринятых; – литературный стиль.

Распределение трудоемкости СРС при изучении дисциплины

Вид самостоятельной работы	Трудоемкость (час)
Подготовка к зачету	10/16
Проработка конспекта лекций	12/22
Подготовка к практическим (семинарским) занятиям	12/22
Проработка учебной литературы	12/20
Написание рефератов	12/12

3. Оценочные средств и методические рекомендации по проведению промежуточной аттестации

Студенты ОП 38.03.05 Бизнес-информатика. Электронный бизнес проходят промежуточную аттестацию в форме зачета по дисциплине "Основы информационной безопасности" в 6/6 семестре.

При проведении зачета по дисциплине «Основы информационной безопасности» может использоваться устная или письменная форма проведения.

Примерная структура зачета по дисциплине «Основы информационной безопасности»

1. устный ответ на вопросы

Студенту на зачете дается время на подготовку вопросов теоретического характера

2. выполнение тестовых заданий

Тестовые задания выполняются в течение 30 минут и состоят из 25 вопросов разных типов. Преподаватель готовит несколько вариантов тестовых заданий.

3. выполнение практических заданий

Практических задания выполняются в течение 30 минут. Бланки с задачами готовит и выдает преподаватель.

Устный ответ студента на зачете должен отвечать следующим требованиям:

- научность, знание и умение пользоваться понятийным аппаратом;
- изложение вопросов в методологическом аспектах, аргументация основных положений ответа примерами из современной практики, а также из личного опыта работы;
- осведомленность в важнейших современных проблемах информационной безопасности, знание классической и современной литературы.

Выполнение практического задания должно отвечать следующим требованиям:

- Владение профессиональной терминологией;
- Последовательное и аргументированное изложение решения.

Критерии оценивания ответов

	Устный ответ	**Практическое задание**	**Тестовые задания**
зачтено	знание учебного материала в пределах программы; логическое, последовательное изложение вопроса; определение своей позиции в раскрытии различных подходов к рассматриваемой проблеме;	свободное владение профессиональной терминологией; умение высказывать и обосновать свои суждения; студент дает четкий, полный анализ ситуации.	50-100 % правильно выполненных заданий
не зачтено	пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в изложении материала	допущены ошибки в определении понятий, искажен их смысл; студент не может применять знания для решения практического задания.	До 50 % правильно выполненных заданий

Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

Оценка «не зачтено» соответствует критерию оценки «неудовлетворительно»

Отметка за зачет по предмету выставляется с учетом полученных отметок в соответствии с правилами математического округления.

Рекомендации по проведению зачета

1. Студенты должны быть заранее ознакомлены с требованиями к зачету, критериями оценивания.

2. Необходимо выяснить на зачете, формально или нет владеет студент знаниями по данному предмету. Вопросы при ответе по билету помогут выяснить степень понимания студентом материала, знание им связей излагаемого вопроса с другими изучавшимися им понятиями, а практические задания – умения применять знания на практике.

3. На зачете следует выяснить, как студент знает программный материал, как он им овладел к моменту зачета, как он продумал его в процессе обучения и подготовки к зачету.

4. При устном опросе целесообразно начинать с легких, простых вопросов, ответы на которые помогут подготовить студента к спокойному размышлению над дальнейшими более трудными вопросами и практическими заданиями.

5. Тестирование по дисциплине проводится либо в компьютерном классе, либо в аудитории на бланке с тестовыми заданиями.

Во время тестирования обучающиеся могут пользоваться калькулятором. Результат каждого обучающегося оценивается в соответствии с оценочной шкалой, приведённой в пункте 3.

6. Выполнение практических заданий осуществляется в учебной аудитории. Результат каждого обучающегося оценивается в соответствии с оценочной шкалой, приведённой в пункте 3.

Перечень вопросов к зачету

1. Теория защиты информации. Основные направления
2. Обеспечение информационной безопасности и направления защиты
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная)
4. Требования к системе защиты информации
5. Угрозы информации
6. Виды угроз. Основные нарушения
7. Характер происхождения угроз
8. Источники угроз. Предпосылки появления угроз
9. Система защиты информации
10. Классы каналов несанкционированного получения информации
11. Причины нарушения целостности информации
12. Методы и модели оценки уязвимости информации
13. Общая модель воздействия на информацию
14. Общая модель процесса нарушения физической целостности информации
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных
16. Методологические подходы к оценке уязвимости информации
17. Модель защиты системы с полным перекрытием
18. Рекомендации по использованию моделей оценки уязвимости информации
19. Допущения в моделях оценки уязвимости информации
20. Методы определения требований к защите информации
21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации
22. Классификация требований к средствам защиты информации

23. Требования к защите, определяемые структурой автоматизированной системы обработки данных

24. Требования к защите, обуславливаемые видом защищаемой информации

25. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации

26. Анализ существующих методик определения требований к защите информации

27. Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения

28. Руководящий документ Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации",выпущенном в 1992 году. Часть 1

29. Классы защищенности средств вычислительной техники от несанкционированного доступа – Функции защиты информации

30. Стратегии защиты информации

31. Способы и средства защиты информации

32. Способы "абсолютной системы защиты"

33. Архитектура систем защиты информации. Требования

34. Общеметодологических принципов архитектуры системы защиты информации

35. Построение средств защиты информации

36. Ядро системы защиты

37. Семирубежная модель защиты

38. Средства защиты информации. Антивирусы, средства анализа защищенности, средства обнаружения вторжений

39. Регуляторы в области защиты информации

Тест по дисциплине «Основы информационной безопасности»

0 вариант

Как называется умышленно искаженная информация?

+ Дезинформация

- Информативный поток

- Достоверная информация

- Перестает быть информацией

Как называется информация, к которой ограничен доступ?

+ Конфиденциальная

- Противозаконная

- Открытая

- Недоступная

Какими путями может быть получена информация?

+ проведением, покупкой и противоправным добыванием информации научных исследований

- захватом и взломом ПК информации научных исследований

- добыванием информации из внешних источников и скремблированием информации научных исследовании

- захватом и взломом защитной системы для информации научных исследований

Как называются компьютерные системы, в которых обеспечивается безопасность информации?

+ защищенные КС

- небезопасные КС

- Само достаточные КС

- Саморегулирующиеся КС

Основной документ, на основе которого проводится политика информационной безопасности?

+ программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

В зависимости от формы представления информация может быть разделена на?

+ Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

+ Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

Что называют защитой информации?

+ Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

Под непреднамеренным воздействием на защищаемую информацию понимают?

+ Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Шифрование информации - это

+ Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

Основные предметные направления Защиты Информации?

+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны

- Определение ценности информации
- Усовершенствование скорости передачи информации

Государственная тайна – это

+ защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Коммерческая тайна - это…

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

+ ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Банковская тайна - это…

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

+ защищаемые банками и иными кредитными организациями сведения о банковских операциях

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны

- ограничения доступа в отдельные отрасли экономики или на конкретные производства

- защищаемые банками и иными кредитными организациями сведения о банковских операциях

+ защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

К основным объектам банковской тайны относятся следующие:
+ Все ответы верны
- Тайна банковского счета
- Тайна операций по банковскому счету
- Тайна банковского вклада

Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
+ Тайна связи
- Нотариальная тайна
- Адвокатская тайна
- Тайна страхования

Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?
+ Нотариальная тайна
- Общедоступные сведения
- Нотариальный секрет
- Нотариальное вето

Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?
+ защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
- управление доступом
+ конфиденциальность
- аутентичность
- целостность
- доступность

Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем
- защита от сбоев в электропитании
+ защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных
- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
+ защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
+ защита от утечек информации электромагнитных излучений

Какая из перечисленных атак на поток информации является пассивной:

+ перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

К открытым источникам информация относятся.

+ Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа
- Украденная из правительственной организации

Технические каналы утечки информации делятся на…

+ Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

+ Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические
+ Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
+ Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
+ Оптические

- Радиоканалы

Примерный перечень практических заданий

Первое задание

Для выполнения первой части необходимо для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1. виды угроз;
2. характер происхождения угроз;
3. классы каналов несанкционированного получения информации;
4. источники появления угроз;
5. причины нарушения целостности информации;
6. потенциально возможные злоумышленных действий;
7. определить класс защиты информации.

Второе задание

Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

1. определить требования к защите информации;
2. классифицировать автоматизированную систему;
3. определить факторы, влияющие на требуемый уровень защиты информации;
4. выбрать или разработать способы и средства защиты информации;
5. построить архитектуру систем защиты информации;
6. сформулировать рекомендации по увеличению уровня защищенности.

Наименование объекта защиты информации:

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер в бухгалтерии.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть материальной группы.
6. Одноранговая локальная сеть без выхода в Интернет.
7. Одноранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выхода в Интернет.
10. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).
13. Банковские операции (внесение денег на счет и снятие).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
17. Материалы для служебного пользования на твердых носителях в производстве.
18. Материалы для служебного пользования на твердых носителях на закрытом предприятии.
19. Материалы для служебного пользования на твердых носителях в архиве.
20. Материалы для служебного пользования на твердых носителях в налоговой инспекции.
21. Комната для переговоров по сделкам на охраняемой территории.

22.Комната для переговоров по сделкам на неохраняемой территории.

23.Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).

24.Судебные материалы (твердая копия).

25.Паспортный стол РОВД.

26.Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).

27.Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).

28.Сведения по тоталитарным сектам и другим общественно-вредным организациям.

29.Сведения по общественно-полезным организациям (красный крест и др.).

30.Партийные списки и руководящие документы.

4. Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Дополнительная литература

1. Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605 (Электронная библиотечная система «Университетская библиотека ONLINE»)

2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин : Директ-Медиа, 2015. - 105 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895 (Электронная библиотечная система «Университетская библиотека ONLINE»)

3. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т. Хаулет. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 566 с. : ил. - (Основы информационных технологий); То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429025 (Электронная библиотечная система «Университетская библиотека ONLINE»)

Информационно-справочные системы, профессиональные базы данных и интернет-ресурсы

7. Сайт Security Lab [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/ (новости, экспертные статьи, софты, форум, раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению)

8. Сайт Threatpost [Электронный ресурс]. – Режим доступа: https://threatpos (содержит новости об информационной безопасности от Kaspersky Lab)

9. Сайт Anti-Malware [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/ (содержит сравнительные тесты антивирусов, аналитические статьи)

10. Сайт Научного журнал «Вопросы кибербезопасности» [Электронный ресурс]. – Режим доступа: http://cyberrus.com/ (содержит статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации)

11. Профессиональная база данных по бизнес-информатике [Электронный ресурс]. - Режим доступа: http://dorlov.blogspot.ru/p/blog-page_3151.html

12. СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г

5. Материально-техническое обеспечение дисциплины

Материально-техническую базу для проведения лекционных и практических занятий по дисциплине составляют:

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (в соответствии с расписанием)	Специализированная мебель, технические средства обучения: переносной ноутбук, мультимедийный проектор, экран	СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г., Windows 10 Education, Windows 8, Windows 7 Professional (Microsoft Open License), Office Standart 2007, 2010 (Microsoft Open License), Office Professional Plus 2016 (Microsoft Open License), Kaspersky Endpoint Security (Лицензия №17E0-171117-092646-487-711, договор №Tr000171440 от 17.07.2017 г.).
Компьютерный класс, каб. 303	Специализированная мебель, технические средства обучения: Автоматизированные рабочие места (ASUSTeK Computer INC. P5KPL-AM SE/Pentium (R) Dual-Core CPU E5300 2.60GHz/512)	СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г. Windows 7 Professional (Microsoft Open License). Sys Ctr Endpoint Protection ALNG Subscriptions VL OLVS E 1Month AcademicEdition Enterprise Per User (Сублиц. договор № Tr000171440 17.07.2017). Office Prosessional 2010 (Microsoft Open License). Архиватор 7-zip (GNU LGPL). Adobe Acrobat Reader DC (Бесплатное ПО). Adobe Flash Player (Бесплатное ПО). Deductor Academic (Бесплатное ПО). FreeCommander (Бесплатное ПО). Inkscape (GNU GPL 2). Notepad++ (GNU GPL 2). freePascal (Бесплатное ПО). Lazarus (Бесплатное ПО). Microsoft Visual Studio 2010 (Бесплатно в рамках подписки Imagine Premium T89-00394 от 10.02.2017). Система виртуализации Oracle VM VirtualBox (GNU LGPL).
Помещение для самостоятельной работы, каб. 114	Специализированная мебель, технические средства обучения: автоматизированные рабочие места, с возможностью подключения к сети «Интернет» и обеспечением	СПС «Консультант Плюс», СПС «Гарант» (договор о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант)), регистрационный лист зарегистрированного пользователя ЭПС

	доступа в электронную информационную образовательную среду организации (AsusTeK COMPUTER INC H110M-R/ Itnel(R) Core(TM) i3-7100 CPU @ 3.90GHz/8192.00 Gb)	«Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договоры с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г. Windows 7 Professional (Microsoft Open License). Sys Ctr Endpoint Protection ALNG Subscriptions VL OLVS E 1Month AcademicEdition Enterprise Per User (Сублиц. договор № Tr000171440 17.07.2017). Office Standart 2010 (Microsoft Open License). Архиватор 7-zip (GNU LGPL). Adobe Acrobat Reader DC (Бесплатное ПО). Adobe Flash Player (Бесплатное ПО). 1С:Бухгалтерия государственного учреждения 8 ПРОФ (Лиценз. договор 011/216 от 01.09.2017). 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях (Лиценз. договор 011/216 от 01.09.2017)

6. Методические указания для обучающихся по освоению дисциплины

Методические указания для подготовки к лекционным занятиям

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные для понимания темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на семинарское занятие и указания на самостоятельную работу.

В ходе лекционных занятий необходимо:

–вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

–задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

–дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой – в ходе подготовки к семинарам изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы.

–подготовить тезисы для выступлений по всем учебным вопросам, выносимым на семинар. Готовясь к докладу или реферативному сообщению, обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с реальной жизнью.

–своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении рекомендованной литературы. Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании контрольных (РГР), курсовых и выпускных квалификационных работ.

Методические указания для подготовки к практическим (семинарским) занятиям

Начиная подготовку к семинарскому занятию, необходимо, прежде всего, обратить внимание на конспект лекций, разделы учебников и учебных пособий, которые способствуют общему представлению о месте и значении темы в изучаемом курсе. Затем следует поработать с дополнительной литературой, сделать записи по рекомендованным источникам. Подготовка к семинарскому занятию включает 2 этапа:

- 1й этап - организационный;

- 2й этап - закрепление и углубление теоретических знаний. На первом этапе студент планирует свою самостоятельную работу, которая включает:

- уяснение задания, выданного на самостоятельную работу:

- подбор рекомендованной литературы;

- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная её часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения

рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Готовясь к консультации, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале занятия студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные положения выступления.

Записи имеют первостепенное значение для самостоятельной работы обучающихся. Они помогают понять построение изучаемого материала, выделить основные положения и проследить их логику. Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память, Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе. Важно развивать умение сопоставлять источники, продумывать изучаемый материал.

Большое значение имеет совершенствование навыков конспектирования. Преподаватель может рекомендовать студентам следующие основные формы записи план (простой и развернутый), выписки, тезисы. Результаты конспектирования могут быть представлены в различных формах.

План - это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект.

Конспект - это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов.

План-конспект - это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.

Текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника.

Свободный конспект - это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.

Тематический конспект составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

Ввиду трудоемкости подготовки к семинару следует продумать алгоритм действий, еще раз внимательно прочитать записи лекций и уже готовый конспект по теме семинара, тщательно продумать свое устное выступление.

На семинаре каждый его участник должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении Выступление должно строиться свободно, убедительно и аргументировано Необходимо следить, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускать и простое чтение конспекта. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного.

Выступления других обучающихся необходимо внимательно и критически слушать, подмечать особенное в суждениях обучающихся, улавливать недостатки и ошибки. При этом обратить внимание на то, что еще не было сказано, или поддержать и развить интересную мысль, высказанную выступающим студентом. Изучение студентами фактического материала по теме практического занятия должно осуществляться заблаговременно. Под фактическим материалом следует понимать специальную литературу по теме занятия, систему нормативных правовых актов, а также арбитражную практику по рассматриваемым проблемам. Особое внимание следует обратить на дискуссионные теоретические вопросы в системе изучаемого вопроса: изучить различные точки зрения ведущих ученых, обозначить противоречия современного законодательства. Для систематизации основных положений по теме занятия рекомендуется составление конспектов.

Обратить внимание на:

- составление списка нормативных правовых актов и учебной и научной литературы по изучаемой теме;
- изучение и анализ выбранных источников;
- изучение и анализ арбитражной практики по данной теме, представленной в информационно- справочных правовых электронных системах и др.;
- выполнение предусмотренных программой заданий в соответствии с тематическим планом;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы;

Семинарские занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности обучающихся по изучаемой дисциплине.

Методические указания для обучающихся по освоению дисциплины дли самостоятельной работы

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных особенностей студентов и условий учебной деятельности.

При этом преподаватель назначает студентам варианты выполнения самостоятельной работы, осуществляет систематический контроль выполнения студентами графика самостоятельной работы, проводит анализ и дает оценку выполненной работы.

Самостоятельная работа обучающихся осуществляется в аудиторной и внеаудиторной формах. Самостоятельная работа обучающихся в аудиторное время может включать:

- конспектирование (составление тезисов) лекций, выполнение контрольных работ;
- решение задач;
- работу со справочной и методической литературой;
- работу с нормативными правовыми актами;
- выступления с докладами, сообщениями на семинарских занятиях;
- защиту выполненных работ;

- участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;

- участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;

- участие в тестировании и др.

Самостоятельная работа обучающихся во внеаудиторное время может состоять из:

- повторение лекционного материала;

- подготовки к семинарам (практическим занятиям);

- изучения учебной и научной литературы;

- изучения нормативных правовых актов (в т.ч. в электронных базах данных);

- решения задач, выданных на практических занятиях;

- подготовки к контрольным работам, тестированию и т.д.;

- подготовки к семинарам устных докладов (сообщений);

- подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;

- выполнения курсовых работ, предусмотренных учебным планом;

- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов;

- написания рефератов и эссе по отдельным вопросам изучаемой темы.

- подготовки к семинарам устных докладов (сообщений);

- подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;

- выполнения курсовых работ, предусмотренных учебным планом;

- выполнения выпускных квалификационных работ и др.

- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов;

- написания рефератов и эссе по отдельным вопросам изучаемой темы.