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

А. Г. Жестовский

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент:
доцент кафедры информационной безопасности
института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»
Н.Я. Великите

Жестовский, А. Г.

Основы информационной безопасности: учеб.-метод. пособие по изучению дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / **А. Г. Жестовский** – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 49 с.

В учебно-методическом пособии приведены тематический план по дисциплине, основные понятия (дидактические единицы), рассматриваемые в каждой отдельной теме дисциплины, даны методические указания по её самостоятельному изучению, отражен порядок и сложность изучения, акцентируя внимание на важных понятиях. Даны основные методические рекомендации при подготовке к лабораторным занятиям. Приведены требования к оцениванию знаний при текущей и промежуточной аттестации студентов, проводимых в соответствии с учебным планом.

Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» 10.05.03 «Информационная безопасность автоматизированных систем».

Учебно-методическое пособие рассмотрено и одобрено в качестве электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», изучающих дисциплину «Основы информационной безопасности».

Цель освоения дисциплины – ознакомление с понятиями национальной безопасности; видами безопасности; информационной безопасности (ИБ) в системе национальной безопасности Российской Федерации; основными понятиями, общеметодологическими принципами теории ИБ; анализом угроз ИБ, проблемами информационной войны; государственной информационной политикой; видами информации; методами и средствами обеспечения ИБ; методами нарушения конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

Дисциплина «Основы информационной безопасности» является вводной в проблематику информационной безопасности, поэтому требования к входным знаниям, умениям и компетенциям студента, необходимым для ее изучения, формируются в процессе изучения дисциплин: «Физика», «Алгебра и геометрия», «Математический анализ», «Дискретная математика», «История», «Информатика», «Организация ЭВМ и вычислительных систем», «Языки программирования», «Технологии и методы программирования», «Иностранный язык», «Правоведение», «Политология», «Электроника и схемотехника».

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.

Реализация компетентностного подхода при изучении дисциплины «Основы информационной безопасности» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов.

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), а также 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.

Помимо данного пособия студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу. Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем:

- программное обеспечение: Microsoft Desktop Education (операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 от 2016-06-30 Open Value Subscription;

- антивирусное программное обеспечение: Kaspersky Total Space Security Russian Edition.

Электронная информационная образовательная среда ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Ресурсы информационно-телекоммуникационной сети «Интернет»:

– «Консультант Плюс» (www.consultant.ru);
– «Гарант» (www.garant.ru);
– http://www.rg.ru/dok/ [On-line] – опубликованные нормативные-правовые акты РФ;
– http://fstec.ru;
– http://www.confident.ru;
– http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/;
– http://www.iqlib.ru - электронная интернет библиотека;
– http://www.biblioclub.ru - полнотекстовая электронная библиотека;
– http://www.elibrary.ru - научная электронная библиотека.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с применением рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

В ходе самостоятельной работы, при подготовке к плановым занятиям и экзамену студенты анализируют поставленные преподавателем задачи с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет.

ТЕМАТИЧЕСКИЙ ПЛАН

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем СР, ч	Неделя																	Сессия
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
		Лекции																					
1	РАЗДЕЛ 1. Информационная безопасность в системе национальной безопасности РФ	Тема 1.1 Принципы обеспечения информационной безопасности	1	4	+																	
		Тема 1.2. Национальные интересы в информационной сфере	1	4		+																
2	РАЗДЕЛ 2. Государственная информационная политика	Тема 2.1. Определение, сущность и содержание государственной информационной политики	1	4			++	++														
		Тема 2.2. Объекты и субъекты государственной информационной политики	1	6					+													
3	РАЗДЕЛ 3. Виды информации, методы и средства обеспечения ИБ	Тема 3.1. Понятие «информация» и ее виды	1	6						+	+											
		Тема 3.2. Методы и средства обеспечения информационной безопасности	1	6								+										
4	РАЗДЕЛ 4. Анализ угроз информационной безопасности	Тема 4.1. Классификация угроз информационной безопасности	2	6									+	+								
		Тема 4.2. Классификация уязвимостей информационных систем	2	6											+							
		Тема 4.3. Угрозы нарушения конфиденциальности, целостности, доступности информации	2	6												+						
5	РАЗДЕЛ 5. Причины, виды, каналы утечки и искажения информации	Тема 5.1. Общая характеристика технического канала утечки информации	2	6													+	+				
		Тема 5.2. Классификация и характеристика технических каналов утечки информации, обрабатываемой техническими средствами приема информации	2	6															+	+		

6	РАЗДЕЛ 6 Организационное и правовое обеспечение информационной безопасности	Тема 6.1. Государственная система правового обеспечения защиты информации в РФ	1	4																	+	+	
			17	**66**																			
		Лабораторные занятия																					
1	РАЗДЕЛ 1. Информационная безопасность в системе национальной безопасности РФ	1.Законодательство РФ в области информационной безопасности	4	4	+	+	+																
2	РАЗДЕЛ 2. Государственная информационная политика	2. Лицензирование деятельности в области защиты информации	2	2			+	+															
3	РАЗДЕЛ 3. Виды информации, методы и средства обеспечения ИБ	3. Сертификация средств защиты информации по требованиям безопасности информации	2	2					+														
		4. Система сертификации средств криптографической защиты информации	2	2						+													
		5. Сертификации средств вычислительной техники и связи	2	2							+												
4	РАЗДЕЛ 4. Анализ угроз информационной безопасности	6. Аттестация объектов информатизации по требованиям безопасности информации	2	2								+											
		7. Аттестация помещений по требованиям безопасности информации	2	2										++	++	++	++	+					
5	РАЗДЕЛ 6. Организационно-правовое обеспечение информационной безопасности	8. Методика испытаний объектов информатики по требованиям безопасности информации	1	2															+	+	+	+	
			17	**18**																			

		Текущий и итоговый контроль																					
1	РАЗДЕЛ 1. Информационная безопасность в системе национальной безопасности РФ	доклад задание № 1					+																
2	РАЗДЕЛ 2. Государственная информационная политика	доклад задание № 2							+														
3	РАЗДЕЛ 3. Виды информации, методы и средства обеспечения ИБ	доклад задание № 3									+												
4	РАЗДЕЛ 4. Анализ угроз информационной безопасности	доклад задание № 4										+											
		контрольная работа задание № 5												+									
		защита лабораторного практикума задание №№ 4.4, 4.5											+										
5	РАЗДЕЛ 5. Причины, виды, каналы утечки и искажения информации	доклад задание № 6													+								
		контрольная работа задание № 7															+						
		защита лабораторного практикума задание №№ 5.3, 5.4														+							
6	РАЗДЕЛ 6. Организационно-правовое обеспечение информационной безопасности	тестирование задание № 8																	+				
		защита лабораторного практикума задание №№ 6.3, 6.4																		+			
		доклад задание № 9																			+		
	Итоговый контроль	**зачет с оценкой**		**24**																			+

Примечание: №№ заданий даны согласно фонда оценочных средств по дисциплине «Основы информационной безопасности»

	Всего	**72**	**72**																				

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Тема 1.1 Принципы обеспечения информационной безопасности

Перечень изучаемых вопросов: история становления теории информационной безопасности; предметная область теории информационной безопасности; основные термины и определения в области информационных отношений и защиты информации; понятия предметной области «Защита информации»; основные принципы построения систем защиты.

Методические указания к изучению: последовательно рассматриваем понятие национальной безопасности, виды безопасности: экономическая внутриполитическая, социальная, военная, международная, информационная, экологическая и другие, соотношение безопасности личности, общества и государства, виды защищаемой информации, роль информационной безопасности в обеспечение национальной безопасности государства; систематизируем понятия в области защиты информации.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС/ А.В. Кузнецов, В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.
2. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – М.: Издательский центр «Академия», 2008. – 256 с.
3. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с
4. Расторгуев, С. П. Основы информационной безопасности: учеб. пособие для вузов / С. П. Расторгуев. – Москва: Академия, 2007. – 129 с.
5. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - Москва : ЮНИТИ-ДАНА, 2017. - 287 с.

Контрольные вопросы:

1. Дать определение понятию «угроза».
2. Задачи обеспечения информационной безопасности РФ.
3. Дать определение понятию «информатизация».
4. Дать определение понятию «информация».
5. Какие два основных элемента включает в себя информация?
6. Какие функции выполняют сведения?
7. Перечислите свойства информации.
8. Дать определение понятию «информационная безопасность».
9. Принципы государственной политики обеспечения информационной безопасности.

Тема 1.2 Национальные интересы в информационной сфере

Перечень изучаемых вопросов: классификация национальных интересов; содержание интересов личности в информационной сфере; содержание интересов общества в информационной сфере; содержание интересов государства в информационной сфере; составляющие интересов РФ в информационной сфере.

Методические указания к изучению: последовательно рассматриваются основные принципы соблюдения конституционных прав и свобод человека и гражданина в получении информации и пользования ею и подходы к информационному обеспечению государственной политики РФ.

Литература:

1. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.
2. Расторгуев, С. П. Основы информационной безопасности: учеб. пособие для вузов / С. П. Расторгуев. – Москва: Академия, 2007. – 129 с.
3. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - Москва : ЮНИТИ-ДАНА, 2017. - 287 с.

4. Жестовский, А. Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с.
5. Галушкин, А. А. К вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. – 2015. - № 2. – С. 8.

Контрольные вопросы:

1. Дать определение понятию «национальные интересы».
2. Какую роль национальные интересы играют во внутриполитической сфере?
3. Какую роль национальные интересы играют в социально сфере?
4. Какую роль национальные интересы играют в духовной сфере?
5. Какую роль национальные интересы играют в международной сфере?
6. Какую роль национальные интересы играют в информационной сфере?
7. Какую роль национальные интересы играют в военной сфере?
8. Какую роль национальные интересы играют в экологической сфере?
9. Дать определение понятию «национальные интересы».
10. Классификация национальных интересов в информационной сфере.

РАЗДЕЛ 2. ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА

Тема 2.1 Определение, сущность и содержание государственной информационной политики

Перечень изучаемых вопросов: цель государственной политики в области обеспечения информационно-психологической безопасности РФ; правовая база государственной информационной политики; приоритетные направления деятельности по реализации государственной информационной политики; базовые принципы построения государственной политики; цели и задачи государственной информационной политики**.**

Методические указания к изучению: последовательное изучение основ государственной политики РФ в области информационной безопасности: национальные интересы РФ в информационной сфере и их обеспечение, виды угроз национальной безопасности РФ. источники угроз информационной безопасности РФ.

Литература:

1. Воронцова, Л. В. История и современность современного противоборства / Л. В. Воронцова, Л. Б. Фролов // Горячая линия - телеком, 2006.

2. Прохожев, А.А. Общая теория национальной безопасности: учебник / А. А. Прохожев - Москва: РАГС, 2005.

3. Скиба В.Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба. – Санкт-Петербург: Питер, 2008

4. Семкин, С.Н.. Основы организационного обеспечения информационной безопасности объектов / С.Н. Семкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок. Москва: Гелиос АРВ, 2005.

5. Стрельцов А. А. Обеспечение информационной безопасности России / А. А. Стрельцов. – Москва: МЦНМО, 2002

6. Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. - Москва: Горячая линия. - Телеком, 2003.

7. Расторгуев, С.П. Информационная война. Проблемы и модели/ С. П. Расторгуев. - Гелиос АРВ, 2006.

Контрольные вопросы:

1. Дать определение понятию «государственная информационная политика».

2. Какие документы составляют правовую базу государственной информационной политики?

3. Перечислите направления деятельности по реализации государственной информационной политики.

4. Принципы государственной политики в области обеспечения информационно-психологической безопасности Российской Федерации.

5. Охарактеризовать принцип законности.

6. Охарактеризовать принцип соблюдения и баланса интересов личности, общества и государства.

7. Охарактеризовать принцип открытости.

8. Охарактеризовать принцип приоритетности национальных интересов Российской Федерации.

9. Основные задачи государственной информационной политики.

10. Цель государственной информационной политики.

Тема 2.2 Объекты и субъекты государственной информационной политики

Перечень изучаемых вопросов: информационные ресурсы; психологические ресурсы; информационно-телекоммуникационная инфраструктура; поли-

тика в области массовой информации; государственная информационная политика как часть системы государственного управления.

Методические указания к изучению: последовательно изучаем основные направления государственной информационной политики в области защиты информации, государственное регулирование развития информационно-телекоммуникационной инфраструктуры; государственные субъекты государственной информационной политики; субъекты массового информирования и коммуникации.

Литература:

1. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.
2. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В. А. Тихонов, В. В. Райх. - Москва: Гелиос АРВ, 2006.
3. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.
4. Жестовский, А. Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с
5. Расторгуев, С.. П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. – Москва: Академия, 2007. – 129 с.
6. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - М. : ЮНИТИ-ДАНА, 2017. - 287 с.

Контрольные вопросы:

1. Что является объектом государственной политики?
2. Основные направления государственной информационной политики в области информационных ресурсов.
3. Какие мероприятия государственной информационной политики в области формирования, развития и использования информационных ресурсов?
4. По каким основным направлениям осуществляется государственное регулирование развития информационно-телекоммуникационной инфраструктуры?

5. Основные направления государственной информационной политики в области массовой информации.

6. Субъекты государственной информационной политики.

7. Категории субъектов государственной информационной политики.

РАЗДЕЛ 3. ВИДЫ ИНФОРМАЦИИ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 3.1. Понятие «информация» и ее виды

Перечень изучаемых вопросов: понятия «информация», «информационная сфера», «информационная безопасность»; понятийная характеристика основных элементов «информации» - сведения и сообщения; общий закон обращения информации.

Методические указания к изучению: последовательно изучаем процесс сбора и переработки информации, принятия на ее основе решений и их выполнения; формы представления информации; свойства информации; характеристика информации.

Литература:

1. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.
2. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В. А. Тихонов, В. В. Райх. - Москва: Гелиос АРВ, 2006.
3. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.
4. Жестовский, А. Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с
5. Расторгуев, С.. П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. – Москва: Академия, 2007. – 129 с.
6. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое

обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - М. : ЮНИТИ-ДАНА, 2017. - 287 с.

Контрольные вопросы:

1. Дать определение понятию «информация».
2. Дать определение понятию «сигнал».
3. Дать определение понятию «сообщение».
4. Дать определение понятию «данные».
5. Формы представления информации.
6. Свойства информации.

Тема 3.2. Методы и средства обеспечения информационной безопасности

Перечень изучаемых вопросов: правовые, организационно-технические и экономические методы обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; методы и средства обеспечения ИБ автоматизированных систем.

Методические указания к изучению: последовательно изучаем правовые, организационно-технические и экономические методы обеспечения ИБ.

Литература:

1. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.
2. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В. А. Тихонов, В. В. Райх. - Москва: Гелиос АРВ, 2006.
3. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.
4. Жестовский, А. Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с
5. Расторгуев, С.. П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. – Москва: Академия, 2007. – 129 с.
6. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки

«Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - М. : ЮНИТИ-ДАНА, 2017. - 287 с.

Контрольные вопросы:

1. Виды методов обеспечения информационной безопасности.
2. Правовые методы обеспечения информационной безопасности.
3. Организационно-технические методы обеспечения информационной безопасности РФ.
4. Экономические методы обеспечения информационной безопасности.

РАЗДЕЛ 4. АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 4.1. Классификация угроз информационной безопасности.

Перечень изучаемых вопросов: виды угроз информационной безопасности; классификация источников угроз информационной безопасности.

Методические указания к изучению: последовательно изучаем угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России; угрозы информационному обеспечению государственной политики РФ; угрозы развитию отечественной индустрии информации; угрозы безопасности информационных и телекоммуникационных средств и систем; группы источников угроз информационной безопасности.

Литература:

1. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.
2. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В. А. Тихонов, В. В. Райх. - Москва: Гелиос АРВ, 2006.
3. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.

4. Жестовский, А. Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с
5. Расторгуев, С.. П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. – Москва: Академия, 2007. – 129 с.
6. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - Москва : ЮНИТИ-ДАНА, 2017. - 287 с.
7. Пархоменко, Н. Г. Выявление угроз информационной безопасности в реальном времени / Н. Г. Пархоменко, Н. М. Боташев, П. М. Колбанов, Е. С. Григоренко // Известия ЮФУ. Технические науки. – 2016. - № 4. – С. 325-326.

Контрольные вопросы:

1. Дать определение понятию «угроза».
2. Дать определение понятию «источник угроз».
3. Дать определение понятию «уязвимость».
4. Дать определение понятию «последствия».
5. Классификация угроз информационной безопасности.
6. Классификация источников угроз информационной безопасности.

Тема 4.2. Классификация уязвимостей информационных систем.

Перечень изучаемых вопросов: методологические подходы к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический; анализ уязвимостей информационной системы; оценка уязвимости системы; неформальная модель нарушителя.

Методические указания к изучению: последовательно изучаем классификационные признаки уязвимостей – объективные, субъективные, случайные; классификация нарушителей; основные варианты построения защитной оболочки и оценки её прочности.

Литература:

1. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.

2. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.

3. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с.

4. Расторгуев, С. П. Основы информационной безопасности: учеб. пособие для вузов / С. П. Расторгуев. – Москва: Академия, 2007. – 129 с.

5. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - Москва : ЮНИТИ-ДАНА, 2017. - 287 с.

6. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш, 3-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: http://znanium.com

Контрольные вопросы:

1. Причины возникновения уязвимостей.
2. Объективные уязвимости.
3. Субъективные уязвимости.
4. Случайные уязвимости.
5. Классификация уязвимостей программного обеспечения.

Тема 4.3. Угрозы нарушения конфиденциальности, целостности, доступности информации.

Перечень изучаемых вопросов: модель защиты — модель системы с полным перекрытием*;* угрозы нарушения конфиденциальности, угрозы нарушения целостности, угрозы нарушения доступности информации*;* классификация автоматизированных систем и требований по защите информации; факторы, влияющие на требуемый уровень защиты информации.

Методические указания к изучению: последовательно изучаем решения задачи защиты информации; фундаментальные требования, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации; требования разделены на три группы: стратегия, подотчетность, гарантии.

Литература:

1. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.

2. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.

3. Расторгуев, С. П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. – Москва: Академия, 2007. – 129 с.

4. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - Москва : ЮНИТИ-ДАНА, 2017. - 287 с.

5. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш, 3-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: http://znanium.com

Контрольные вопросы:

1. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4. В каких системах на первом месте стоит обеспечение доступности информации?
5. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
7. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
8. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.

РАЗДЕЛ 5. ПРИЧИНЫ, ВИДЫ, КАНАЛЫ УТЕЧКИ И ИСКАЖЕНИЯ ИНФОРМАЦИИ

Тема 5.1. Общая характеристика технического канала утечки информации

Перечень изучаемых вопросов: теория и практика защиты информации техническими средствами; задачи систем защиты информации; физическая природа возникновения информационных сигналов в каналах утечки информации; методы расчета параметров.

Методические указания к изучению: последовательно изучаем виды, источники и носители защищаемой информации; классификацию иностранной технической разведки; возможности видов технической разведки; основные этапы и процедуры добывания информации технической разведкой.

Литература:

1. ГОСТ РВ 50170-92. Противодействие ИТР. Термины и определения. Москва: Госстандарт России.
2. ГОСТ Р 50992-96. Защита информации. Термины и определения. М.: Госстандарт России.
3. Зайцев, А. П. Техническая защита информации: учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А.А. Шелупанова. – Москва: Горячая линия-Телеком, 2009. – 616 с.
4. Конеев, И.Р. Информационная безопасность предприятия / И. Р. Конеев, А.В. Беляев. – Санкт-Петербург: БХВ-Петербург, 2003.
5. Ярочкин, В. И. Информационная безопасность учеб. для вузов / В. И. Ярочкин. – Москва: Академпроект, 2004.
6. Хорев, А.А Защита информации от утечки по техническим каналам. Ч. I. Технические каналы утечки информации: учебное пособие / А.А. Хорев. - Москва: Гостехкомиссия России, 1998. - 320 с.
7. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с

Контрольные вопросы:

1. Причины утечки информации.
2. Виды утечки информации.
3. Дать определению понятию «разглашению информации».
4. Дать определение понятию «несанкционированный доступ».
5. Дать определение понятию «канал утечки информации».
6. Виды каналов утечки информации.

Тема 5.2. Классификация и характеристика технических каналов утечки информации, обрабатываемой техническими средствами приема информации.

Перечень изучаемых вопросов:

Отдельный раздел посвящен технически средствам защиты объектов. Приведена классификация основных технических каналов утечки информации, имеющих место в реальных условиях. Рассмотрены вопросы технического контроля эффективности мер защиты информации и аттестации объектов информатизации.

Методические указания к изучению: подробно рассмотрены средства выявления технических каналов утечки информации и защита информации от утечки; предложены варианты практических заданий; приводятся технические характеристики некоторых устройств выявления и защиты каналов утечки информации.

Литература:

1. ГОСТ РВ 50170-92. Противодействие ИТР. Термины и определения. - Москва: Госстандарт России.
2. ГОСТ Р 50992-96. Защита информации. Термины и определения. - Москва: Госстандарт России.
3. Зайцев, А.П. Техническая защита информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – Москва : Горячая линия-Телеком, 2009. – 616 с.
4. Ворона, В. А. Технические системы охранной и пожарной сигнализации: учеб. пособие / В. А. Ворона М.В., В. А. Тихонов. – Москва : Горячая линия-Телеком, 2012. – 376 с.
5. Конеев, И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – Санкт-Петербург: БХВ-Петербург, 2003.
6. Ярочкин, В.И. Информационная безопасность / учеб. для вузов / В. И. Ярочкин. – Москва: Академпроект, 2004.
7. Хорев, А.А Защита информации от утечки по техническим каналам. Ч. I. Технические каналы утечки информации: учебное пособие / А.А. Хорев. - Москва: Гостехкомиссия России, 1998. - 320 с.
8. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с.

Контрольные вопросы:

1. Классификация электромагнитных излучений по диапазонам частот и длинам волн
2. Характеристика электромагнитных каналов утечки информации.
3. Классификация демаскирующих признаков объектов
4. Классификация технических признаков радиоизлучений
5. Основные задачи охраны и принципы обеспечения безопасности объектов
6. Организация контроля доступа к защищаемым помещениям
7. Классифицировать основные методы защиты от радиоперехвата

РАЗДЕЛ 6. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 6.1. Информация как объект юридической защиты.

Перечень изучаемых вопросов: основные функции организационно-правовой базы информационной безопасности; юридические аспекты организационно-правового обеспечения защиты информации; модели безопасности личности и безопасности информации; классификация информации.

Методические указания к изучению: рассматриваем последовательно совокупность законов и других нормативно-правовых актов в области защиты информации; основные группы информационных ресурсов государства; виды защищаемой информации; виды, содержание и размеры ущерба при утечке конфиденциальной информации.

Литература:

1. Ищейнов, В. Я. Защита конфиденциальной информации: учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва : ФОРУМ, 2013. – 256 с.
2. Кузнецов, А. В. Основы защиты информации: учеб. пособие / В. А. Иванов, О.П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с.
3. Организационно-правовое обеспечение информационной безопасности: учеб. пособие / А. А. Стрельцов [и др.] ; под общ. ред. А. А. Стрельцова. – Москва: Академия, 2008. – 256 с.
4. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие для студентов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев. – Санкт-Петербург : Питер, 2008. - 272 с.

5. Просис, Крис. Расследование компьютерных преступлений / К. Просис, К. Мандиа ; пер. О. Труфанов. – Москва: ЛОРИ, 2013. – 76 с.

6. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с.

Контрольные вопросы:

1. Дать определение понятию «информационная безопасность».
2. Что представляет собой организационно-правовое обеспечение информационной безопасности?
3. Функции организационно-правовой базы.
4. Концептуальные модели безопасности продукции, личности и информации.
5. Группы информационных ресурсов государства.
6. Какую информацию относят к защищаемой?
7. Какая информация называется защищаемой?
8. Дать определение понятию «тайна».
9. Классификация информации.
10. Признаки защищаемой информации.
11. Кто может быть владельцем защищаемой информации?
12. Дать определение понятию «государственная тайна».
13. Виды ущерба при утечке сведений, составляющих государственную тайну.

Тема 6.2. Государственная система правового обеспечения защиты информации в РФ.

Перечень изучаемых вопросов: система органов и должностных лиц, ответственных за обеспечение информационной безопасности; содержание интересов личности, общества, государства в информационной сфере; структура государственной системы информационной безопасности; направления разработки правого обеспечения защиты информации.

Методические указания к изучению: последовательно изучаем основные положения правового обеспечения защиты информации согласно Доктрины информационной безопасности РФ, а также другие законодательные акты в этой области; основные задачи в области обеспечения информационной безопасности ФСТЭК, ФСБ, СВР, МО России и других органов государственного управления.

Литература:

1. Ищейнов, В. Я. Защита конфиденциальной информации: учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва : ФОРУМ, 2013. – 256 с.

2. Кузнецов, А. В. Основы защиты информации: учеб. пособие / А.В. Кузнецов, В. А. Иванов, О.П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с.

3. Организационно-правовое обеспечение информационной безопасности: учеб. пособие / А. А. Стрельцов [и др.] ; под общ. ред. А. А. Стрельцова. – Москва : Академия, 2008. – 256 с.

4. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие для студентов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев. – Санкт-Петербург : Питер, 2008. - 272 с.

5. Просис, Крис. Расследование компьютерных преступлений / К. Просис, К. Мандиа ; пер. О. Труфанов. – Москва : ЛОРИ, 2013. – 76 с.

6. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с

Контрольные вопросы:

1. Структура государственной системы информационной безопасности.
2. Основная задача государственной системы защиты информации.
3. Назвать службу, которая ведет общую организацию и координации работ в стране по защите информации, обрабатываемой техническими средствами.
4. Функции ФСТЭК России в области государственной безопасности.
5. Задачи ФСТЭК России в области обеспечения информационной безопасности.
6. Какими нормативно-правовыми документами руководствуется ФСТЭК России?
7. Какие функции выполняет ФСБ России?

ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Текущий контроль успеваемости

Оценивание поэтапного формирования результатов освоения дисциплины осуществляется в процессе текущего контроля, который представляет собой единый непрерывный процесс оценки знаний, умений, формирования и сформированности компетенций у обучающихся.

Текущий контроль предназначен для проверки хода и качества усвоения обучающимися учебного материала и стимулирования учебной работы студентов. Он может осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины. Текущий контроль предполагает постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Результаты контроля учитываются выставлением оценок в журнале учета успеваемости.

Для текущего контроля успеваемости используются следующие оценочные средства:

- тестовые задания;
- задания и контрольные вопросы по лабораторным работам;
- задания по подготовке докладов;
- задания на контрольные работы.

ТИПОВЫЕ ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Раздел. 1 Информационная безопасность в системе национальной безопасности.

1. Обосновать соотношение информационной безопасности человека и общества, государства и предпринимательских структур.
2. Классифицировать информационные ресурсы, определить свойства классификационных групп.
3. Дать определение информационной безопасности и проанализировать ее цели, задачи и структуру.
4. Проанализировать содержание концепции информационной безопасности.
5. Обосновать необходимость информационной безопасности человека и общества.
6. Определить место информационной безопасности в структуре информационного права.

7. Проанализировать современные проблемы информационной безопасности предпринимательской деятельности.
8. Дать определение информационным ресурсам, охарактеризовать их основные свойства, взаимосвязь с материальными и иными ресурсами.

Раздел. 2 Государственная информационная политика.

1. Описать порядок охраны информационных ресурсов открытого доступа.
2. Охарактеризовать порядок защиты информационных ресурсов ограниченного доступа.
3. Выявить соотношение понятий ценности, полезности и достоверности информационных ресурсов.
4. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
5. Понятие конфиденциальности, дать его определение, классификацию конфиденциальной информации по объектам владения.
6. Дать классификацию источников конфиденциальной информации, охарактеризовать каждый источник.
7. Обосновать сущность разведки в бизнесе, легальных методов получения ценной информации.
8. Дать классификацию нелегальных методов промышленного шпионажа.

Раздел.3 Виды информации, методы и средства обеспечения информационной безопасности.

1. Определить сущность несанкционированного канала утраты конфиденциальной информации.
2. Классифицировать организационные каналы утраты конфиденциальной информации.
3. Классифицировать технические каналы утраты конфиденциальной информации.
4. Показать соотношение организационных и технических каналов утраты информации в компьютерах и локальных сетях.
5. Обосновать необходимость защиты информационных ресурсов от несанкционированного доступа.
6. Концептуальные особенности защиты информации, ее органическая связь с информационной безопасностью.
7. Содержание Федерального Закона "Об информации, информатизации и защите информации".

8. Дать определение термину "защита информации", специфики его использования.
9. Определить понятие "система защиты информации", обосновать ее цель, задачи и принципы построения.
10. Обосновать структуру системы защиты информации, охарактеризовать ее комплексность.

Раздел.4 Анализ угроз информационной безопасности

1. Определить понятие угрозы информации, классифицировать угрозы по различным основаниям.
2. Назначение и содержание правового элемента системы защиты.
3. Назначение и содержание организационного элемента системы защиты.
4. Назначение и содержание инженерно-технического элемента системы защиты.
5. Назначение и содержание программно-аппаратного элемента системы защиты.
6. Назначение и содержание криптографического элемента системы защиты.
7. Критерии формирования системы защиты в зависимости от ценности информации, размера прибыли или убытков и стоимости системы защиты.
8. Определить состав простейших методов защиты информации в некрупных фирмах.
9. Концепция использования конфиденциальной информации в практической работе фирмы.
10. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
11. Дать соотношение понятий "допуск" и "доступ" к конфиденциальной информации.
12. Дать перечень методов расчленение (дробления) тайны фирмы на составные элементы.
13. Обосновать принципы практической реализации системы доступа персонала к конфиденциальной информации.
14. Проанализировать обязанности руководителей и специалистов в сфере персональной ответственности за сохранность носителя и конфиденциальность информации.
15. Определить порядок классификации конфиденциальных информационных ресурсов в предпринимательских структурах различного типа.
16. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.

Раздел.5 Причины, виды, каналы утечки и искажения информации

1. Сравнить способы учета конфиденциальных документов, изготовленных на дискете, выявить критерии определения эффективности каждого из способов.
2. Сравнить способы учета электронных конфиденциальных документов, передаваемых по линии защищенной компьютерной связи, выявить критерии определения эффективности каждого из способов.
3. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
4. Составить план подготовки совещания по конфиденциальному вопросу.
5. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети проанализировать степень опасности каждого канала.
6. Составить схему рекомендуемых рубежей охраны фирмы и проанализировать эффективность системы охраны.
7. Проанализировать сферы использования различных направлений и методов аналитической работы по выявлению каналов утраты конфиденциальной информации.
8. Графически (схематически) описать технологию выполнения процедур и операций конкретной части того или иного элемента системы защиты информации (по выбору преподавателя).
9. Проанализировать ситуационный вариант и выработать меры противодействия угрозам конфиденциальной информации.

Критерии оценки

«5 (отлично)»

- глубокое и прочное усвоение программного материала;
- полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания;
- свободно справляющиеся с поставленными задачами, знания материала;
- правильно обоснованные принятые решения;
- владение разносторонними навыками и приемами выполнения практических работ.

«4 (хорошо)»

- знание программного материала;
- грамотное изложение, без существенных неточностей в ответе на вопрос;
- правильное применение теоретических знаний;
- владение необходимыми навыками при выполнении практических задач.

«3 (удовлетворительно)»

- усвоение основного материала;
- при ответе допускаются неточности;
- при ответе недостаточно правильные формулировки;
- нарушение последовательности в изложении программного материала;
- затруднения в выполнении практических заданий;

«2 (неудовлетворительно)»

- не знание программного материала;
- при ответе возникают ошибки;
- затруднения при выполнении практических работ.

ТИПОВЫЕ ТЕМЫ ДОКЛАДОВ

1. Понятие, проблемы и структура информационной безопасности (на примере фирм различных типов).
2. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3. Информационная безопасность, история формирования.
4. Концепция информационной безопасности.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Правовые основы защиты конфиденциальной информации.
7. Организационные основы защиты конфиденциальной информации.
8. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.
9. Построение и функционирование защищенного документооборота.
10. Анализ инструкции по обработке и хранению конфиденциальных документов.
11. Направления и методы защиты документов на бумажных носителях.
12. Направления и методы защиты машиночитаемых документов.
13. Направления и методы защиты электронных документов.
14. Направления и методы защиты аудио и визуальных документов.
15. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
16. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
17. Соотношение источников, каналов распространения и каналов утечки информации.
18. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

19. Основы технологии обработки и хранения конфиденциальных документов.
20. Назначение, виды, структура и технология функционирования системы защиты информации.
21. Направления и методы защиты профессиональной тайны.
22. Направления и методы защиты служебной тайны.
23. Направления и методы защиты персональных данных о гражданах.
24. Методы защиты личной и семейной тайны.
25. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.
26. Порядок подбора персонала для работы с конфиденциальной информацией.
27. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.
28. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
29. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.
30. Задачи, функции и графическая структура служб конфиденциальной документации в фирмах различных типов, нормативно-методическое обеспечение их деятельности.
31. Направления защиты компьютеров и локальных сетей от несанкционированного доступа к информации.
32. Аналитический обзор различных технологий хранения конфиденциальных документов.
33. Назначение, виды и технология учета конфиденциальных документов.
34. Аналитический обзор российского и зарубежного исторического опыта в предотвращении утраты ценной информации по вине сотрудников.
35. Анализ существующих правил поведения персонала и охраны фирмы в экстремальных ситуациях различного типа.
36. Проблемы управления персоналом и защиты информации в предпринимательской деятельности (теоретический очерк).
37. Цели, задачи, стадии и методы работы с персоналом, обладающим конфиденциальной информацией.
38. Классификация персонала фирмы и окружающих фирму людей по степени их осведомленности в тайнах фирмы, анализ каждой классификационной группы.
39. Классификация экстремальных ситуаций, угрожающих персоналу фирмы в рабочее и нерабочее время, анализ выделенных классификационных групп и методов локализации опасности.

40. Порядок и методика проведения служебного расследования по фактам нарушения правил защиты информации фирмы.
41. Классификация противоправных действий персонала фирмы с конфиденциальной информацией.
42. Принципы построения, организация и совершенствование пропускного режима на фирме, методика идентификации различных категорий сотрудников и посетителей.

Критерии оценивания за устное выступление при обсуждении вопроса

5 «Отлично»	выступление (доклад) отличается последовательностью, логикой изложения. Легко воспринимается аудиторией. При ответе на вопросы выступающий (докладчик) демонстрирует глубину владения представленным материалом. Ответы формулируются аргументировано, обосновывается собственная позиция в проблемных ситуациях.
4 «Хорошо»	выступление (доклад) отличается последовательностью, логикой изложения. Но обоснование сделанных выводов недостаточно аргументировано. Неполно раскрыто содержание проблемы.
3 «Удовлетворительно»	выставляется, если выступающий (докладчик) передает содержание проблемы, но не демонстрирует умение выделять главное, существенное. Выступление воспринимается аудиторией сложно.
2 «Неудовлетворительно»	выступление (доклад) краткий, неглубокий, поверхностный.

Критерии оценивания доклада с презентацией

2 «Неудовлетворительно»	Студент демонстрирует первичное восприятие некоторых основных элементов медиаработы. Она проста и незакончена. Проблема не раскрыта. Отсутствуют выводы. Не использованы возможности визуализации материала в PowerPoint. Больше 4 ошибок в представляе-

	мой информации.
3 «Удовлетворительно»	Некоторая степень владения большинством элементов медиаработы. Частично присутствует гармоничная интеграция элементов в целое, но работа незавершенная. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Частично использованы возможности визуализации материала в PowerPoint. 3-4 ошибки в представляемой информации.
4 «Хорошо»	Студент показывает владение элементами медиаработы. В основном, она ясная и целостная. Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы. Использованы информационные технологии (PowerPoint). Не более 2 ошибок в представляемой информации.
5 «Отлично»	Студент продемонстрировал уверенное владение и интеграцию всех элементов медиаработы. Работа целостна, креативна. Использован творческий подход. Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы. Широко использованы информационные технологии (PowerPoint). Отсутствуют ошибки в представляемой информации.

ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ

1.	Каким свойством не обладает информация в форме сообщения? а) материальность б) измеримость г) простота д) проблемная ориентированность
2.	Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия, является угрозой: а) конституционным правам и свободам человека и гражданина в области

	духовной жизни и информационной деятельности б) информационному обеспечению государственной политики РФ г) развитию отечественной индустрии информации, включая индустрию телекоммуникации, связи и средств информатизации д) безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России
3.	Информационным ресурсом является: а) вся накопленная информация, в том числе и недостоверная, представленная сомнительными фактами, ложными положениями, потерявшая конкретность б) только достоверная информация из проверенных источников г) вся накопленная информация, в том числе и недостоверная, представленная сомнительными фактами, ложными положениями, но не потерявшая своей конкретности д) достоверная информация из проверенных источников, включая устаревшую информацию
4.	Утечка информации – это … а) несанкционированный процесс переноса информации от источника к злоумышленнику б) процесс раскрытия секретной информации в) процесс уничтожения информации г) непреднамеренная утрата носителя информации
5.	Информация, поступающая к человеку, обладает следующими свойствами: а) идеальность, объективность, динамичность б) идеальность, объективность, простота г) динамичность, субъективность, накапливаемость д) субъективность, не идеальность, информационная неуничтожаемость
6.	Преднамеренной угрозой безопасности информации является: а) наводнение б) повреждение кабеля, по которому идет передача, в связи с погодными условиями в) кража г) ошибка разработчика
7.	Концепция системы защиты от информационного оружия не должна включать… а) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры б) средства нанесения контратаки с помощью информационного оружия в) признаки, сигнализирующие о возможном нападении г) процедуры оценки уровня и особенностей атаки против национальной

	инфраструктуры в целом и отдельных пользователей
8.	В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на … а) соблюдение норм международного права в сфере информационной безопасности б) выявление нарушителей и привлечение их к ответственности в) разработку методов и усовершенствование средств информационной безопасности г) соблюдение конфиденциальности информации ограниченного доступа
9.	Информация, составляющая государственную тайну, не может иметь гриф… а) «для служебного пользования» б) «секретно» в) «совершенно секретно» г) «особой важности»
10.	Одной из основных угроз доступности информации является: а) злонамеренное изменение данных б) хакерская атака в) непреднамеренные ошибки пользователей г) перехват данных
11.	Что не относится к компьютерной преступности? а) подделка компьютерной информации б) хищение информации в) распространение вирусов г) согласованное копирование данных
12.	Как называется комплекс мероприятий, направленных на обеспечение информационной безопасности? а) защитой информации б) авторизацией в) информационной безопасностью г) безопасным состоянием
13.	Кто отвечает за защиту автоматизированной системы от несанкционированного доступа к информации? а) пользователь б) аутентификатор в) авторизатор г) администратор защиты
14.	Перехват данных является угрозой…

	а) доступности б) целостности в) конфиденциальности г) для администратора
15.	Сбор и накопление информации о событиях, происходящих в информационной системе, называется… а) протоколированием б) аудитом в) экранированием г) криптографией
16.	Как называется набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию? а) эффективность защиты б) политика безопасности в) гарантированность г) гармонизированность безопасности
17.	Что не входит в аспекты информационной безопасности? а) доступность б) целостность в) стойкость г) конфиденциальность
18.	Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем б) объективных проблем современной технологии программирования в) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы г) постоянные атаки хакеров
19.	В число принципов управления персоналом входит: а) разделяй и властвуй б) разделение обязанностей в) метод кнута и пряника г) разделение доступа
20.	Меры информационной безопасности направлены на защиту от: а) нанесения неприемлемого ущерба б) нанесения любого ущерба в) подглядывания в замочную скважину г) нанесения морального вреда
21.	На межсетевые экраны целесообразно возложить следующие функции: а) антивирусный контроль "на лету"

	б) антивирусный контроль компьютеров внутренней сети в) антивирусный контроль компьютеров внешней сети г) антивирусный контроль всех съемных носителей
22.	На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют: а) меры ограниченной направленности б) меры направляющие и координирующие в) меры по обеспечению информационной независимости г) меры по поддержанию государственной безопасности
23.	Системы анализа защищенности помогают: а) оперативно пресечь известные атаки б) предотвратить известные атаки в) восстановить ход известных атак г) восстановить логические связи
24.	Сложность обеспечения информационной безопасности является следствием: а) невнимания широкой общественности к данной проблематике б) все большей зависимости общества от информационных систем в) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним г) обширной структуры предмета информационная безопасность
25.	Уровень безопасности С, согласно "Оранжевой книге", характеризуется: а) произвольным управлением доступом б) принудительным управлением доступом в) верифицируемой безопасностью г) комплексным управлением доступом
26.	Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что: а) с программно-технической точки зрения, информационная безопасность - ветвь информационных технологий и должна развиваться по тем же законам б) объектно-ориентированный подход популярен в академических кругах в) объектно-ориентированный подход поддержан обширным инструментарием г) объектно-ориентированный подход широко применяется в государственных структурах
27.	В число принципов физической защиты входят: а) беспощадный отпор б) непрерывность защиты в пространстве и времени в) минимизация защитных средств

	г) наличие охранника
28.	Что из перечисленного не относится к числу основных аспектов информационной безопасности: а) доступность б) конфиденциальность в) целостность г) масштабируемость
29.	Совместно с криптографическими сервисами туннелирование может применяться для достижения следующих целей: а) обеспечение гарантированной полосы пропускания б) обеспечение высокой доступности сетевых сервисов в) обеспечение конфиденциальности и целостности передаваемых данных г) обеспечение максимального уровня защищенности хранимых данных

Критерии оценивания выполнения тестирования

а) типовые задания к тесту

Формы тестовых заданий:

- выбор правильных ответов из перечисленных;
- установление правильной последовательности;
- установление соответствия.

б) критерии оценивания

Критерием оценивания теста является количество правильно выполненных тестовых заданий, свидетельствующих о полноте знаний теоретического материала.

в) описание шкалы оценивания

5 «Отлично» - процент правильно выполненных заданий составляет от 80 до 100 %.

4 «Хорошо» - процент правильно выполненных заданий составляет от 60 до 79 %.

3 «Удовлетворительно» - процент правильно выполненных заданий составляет от 50 до 59 %.

2 «Неудовлетворительно» - процент правильно выполненных заданий составляет менее 50 %.

Критерии оценивания отчета по лабораторным работам

а) разделы отчета

- наименование лабораторной работы;
- постановка задачи, исходные данные;
- описание методов и способов решения;
- этапы решения задачи и (или) ее алгоритмическое обеспечение;
- результаты, представленные в виде таблиц, графиков и т.п. с краткими пояснениями;
- выводы.

б) критерии оценивания

Студент должен продемонстрировать:

- умения применять математические методы для формализации и решения прикладных задач; строить модели процессов, исследовать их и вырабатывать рекомендации к их применению на практике; организовывать вычислительный эксперимент на компьютере для исследования поведения объектов, систем, процессов;
- владение навыками работы с пакетами прикладных программ для моделирования и анализа экономических процессов.

в) описание шкалы оценивания

- **«Зачтено»** выставляется в случае, если студент выполнил в полном объеме лабораторную работу, не допустил ошибок в расчетах, сделал выводы, свободно излагает этапы решения и результаты работы.
- **«Незачтено»** выставляется в случае, если студент не выполнил лабораторную работу, либо выполнил, но допустил существенные ошибки в расчетах и (или) не сделал выводы, и (или) не может изложить этапы решения и результаты работы.

Условия получения положительной оценки

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой: дифференцированный зачёт (зачёт с оценкой).

Зачет по дисциплине осуществляется при условии выполнения заданий всех практических занятий, самостоятельной работы, а также результатами проведенной оценки остаточных знаний.

Оценка «Зачтено» или «Удовлетворительно» выставляется по факту успешного прохождения текущей аттестации и выполнения обязательных лабораторных работ.

Критерии оценивания зачета

Критерии оценок на **дифференцированном зачете** 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» выставляется в случаях: правильных и четких ответов при незначительных замечаниях, неточностях.

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

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

Примерные вопросы к зачету* по дисциплине

1.	Определение и место информационной безопасности в общей совокупности информационных проблем современного общества
2.	Законодательная база Российской Федерации по обеспечению информационной безопасности
3.	Международные нормативно-правовые акты в области информационной безопасности
4.	Современная постановка задачи защиты информации
5.	Методологический базис решения задач защиты информации
6.	Система стандартизации в области защиты информации
7.	Моделирование процессов защиты информации
8.	Понятие угрозы безопасности информации. Риски и управление рисками
9.	Системная классификация угроз безопасности информации
10.	Методы оценки уязвимости информации. Формула оценки уязвимости информации
11.	Методы оценки достоверности информации
12.	Методы оценки ущерба от реализации угроз безопасности информации
13.	Способы несанкционированного доступа к данным. Методы обеспечения недоступности данных
14.	Анализ методик определения требований к защите информации
15.	Параметры защищаемой информации
16.	Принципы защиты информации от несанкционированного доступа
17.	Методы идентификации и аутентификации пользователей
18.	Методы контроля доступа
19.	Системы блочного шифрования: DES и ГОСТ

20.	Цифровая подпись и система шифрования с открытым ключом
21.	Средства антивирусной защиты
22.	Вирусное подавление как форма радиоэлектронной борьбы
23.	Защита информационно-программного обеспечения на уровне операционных систем
24.	Защита информации на уровне систем управления базами данных
25.	Способы защиты информации в локальных и глобальных компьютерных сетях
26.	Основные виды технических каналов и источников утечки информации в автоматизированных системах
27.	Физические основы утечки защищаемой информации по акустическому каналу, линиям связи и каналу побочного электромагнитного излучения
28.	Характеристики каналов утечки информации в автоматизированных системах
29.	Способы предотвращения утечки информации по техническим каналам
30.	Классификация средств вычислительной техники по защищенности от НСД
31.	Классификация автоматизированных систем по защищенности от НСД
32.	Классификация межсетевых экранов по защищенности от НСД
33.	Обобщенная схема обеспечения информационной безопасности. Структура унифицированной концепции защиты информации
34.	Классификация (критерии) технических средств защиты информации
35.	Общие принципы создания и функционирования системы обеспечения безопасностью предприятия
36.	Назначение политики безопасности и ее содержание
37.	Этапы создания систем защиты информации
38.	Назначение и функции службы безопасности предприятия
39.	Содержание деятельности службы безопасности
40.	Типовая структура службы безопасности предприятия. Обязанности сотрудников
41.	Определение и место информационной безопасности в общей совокупности информационных проблем современного общества
42.	Законодательная база Российской Федерации по обеспечению информационной безопасности
43.	Международные нормативно-правовые акты в области информационной безопасности

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.

Перед началом занятий преподаватель проводит инструктаж по технике электробезопасности и пожарной безопасности. Контроль знаний в ходе изучения дисциплины осуществляется в виде текущих контролей, а также итоговой аттестации в форме дифференцированного зачета по итогам учебного семестра.

В соответствии с рабочим учебным планом дисциплина «Основы информационной безопасности» включает следующие виды занятий: лекции, лабораторные занятия, самостоятельная работа студентов.

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Преподавателю, ведущему курс, рекомендуется на вводной лекции определить структуру курса, пояснить цели и задачи изучения дисциплины, сформулировать основные вопросы и требования к результатам освоения.

При рассмотрении темы важно выделить основные понятия и определения, желательна их визуализация. При подготовке и проведении занятий по данному курсу преподаватель должен руководствоваться как общими учебно-методическими принципами (научность, системность, доступность, последовательность, преемственность, наличие единой внутренней логики курса, его связь с другими предметами), так и специфическими особенностями дисциплины, которые находят выражение в агрегированности и комбинации подходов. В подборе материала к занятиям следует руководствоваться рабочей программой учебной дисциплины, обращая внимание на компетенции, указанные в федеральном государственном образовательном стандарте высшего образования.

На первом занятии преподаватель обязан довести до обучающихся порядок работы в аудитории и нацелить их на проведение самостоятельной работы с учетом количества часов, отведенных на нее учебным планом. Рекомендуя литературу для самостоятельного изучения, преподаватель должен максимально использовать возможности, предлагаемые библиотекой академии, в том числе ее электронными ресурсами.

Во время лекционных занятий рекомендуется вести конспектирование

учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления или процессов, научные выводы и практические рекомендации.

Проблемная лекция побуждает аудиторию к активному включению в усвоение и обсуждение материала. Нахождение ответов на неоднозначные вопросы стимулирует развитие творческого мышления. Вопросы, предлагаемые аудитории для размышления, должны побуждать студентов использовать имеющиеся знания.

По окончании лекции необходимо делать выводы и ставить задачи на самостоятельную работу.

Лабораторные занятия направлены на закрепление лекционного материала. При подготовке к лабораторным занятиям руководствоваться методическими указаниями по выполнению лабораторных работ [39].

Самостоятельная работа студентов заключается в подготовке к практическим и лекционным занятиям и выполнении заданий для самостоятельной работы, выдаваемых преподавателем по каждому из разделов дисциплины. В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими.

Следует рассматривать задачи, возникающие в самых различных отраслях и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете.

В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к практической работе по результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы, представляет теоретическую часть решения задачи, практический расчет.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

При самостоятельной проработке материала дисциплины обучающиеся должны: просматривать основные определения и факты; повторить законспек-

тированный на лекционном занятии материал и дополнить его с учётом рекомендованной по данной теме литературы; изучить рекомендованную и дополнительную литературу; выполнять задания для самостоятельной подготовки; использовать для самопроверки материалы фонда оценочных средств по дисциплине «Основы информационной безопасности».

Литература

1. Конституция РФ (http://constitutionrf.ru/).

2. Доктрина информационной безопасности Российской Федерации (утв. Утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.) (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html).

3. Указ правительства РФ №188 об утверждении перечня сведений конфиденциального характера 1997г. (с изм. и доп. от 23 сентября 2005 г., 13 июля 2015 г.) (http://base.garant.ru/10200083/#ixzz4bCt8H6TU).

4. Трудовой кодекс РФ – глава 14 «Защита персональных данных работника» (от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (http://www.consultant.ru/document/cons_doc_LAW_34683/).

5. Гражданский кодекс Ч. №4 Раздел 7 «Права на результаты интеллектуальной деятельности и средства индивидуализации» (18 декабря 2006 года N 230-ФЗ) (http://www.consultant.ru/document/cons_doc_LAW_64629/).

6. Федеральный Закон от 21 июля 1993г. №5485 «О государственной тайне» (Федеральный закон "О внесении изменений в статью 5 Закона Российской Федерации "О государственной тайне" от 15.11.2010 N 299-ФЗ (последняя редакция) (http://www.consultant.ru/document/cons_doc_LAW_106802/).

7. Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне") (ред. От 12.03.14 г.) (http://yconsult.ru/zakony/zakon-rf-98-fz/);Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации» (http://base.garant.ru/12148555/).

8. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями вступивших в силу 01.03.17 г.) (http://kodeks.systecs.ru/zakon/fz-152/).

9. Федеральный закон от 06 апреля 2011 №63 «Об электронной подписи» (с изменениями на 23.06.16 г.) (http://docs.cntd.ru/document/902271495).

10. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. Журнал «Вопросы кибербезопасности», №5(8) – 2014.

11. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Введ. 2016-04-01. Москва: Стандартинформ. 2015. 22 с.

12. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Введ. 2015-08-19. Москва: Стандартинформ. 2015. 17 с.

13. ГОСТ РВ 50170-92. Противодействие ИТР. Термины и определения. Москва: Госстандарт России.

14. ГОСТ Р 50992-96. Защита информации. Термины и определения. Москва: Госстандарт России.

15. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС/ А.В. Кузнецов, В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

16. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2008. – 256 с.

17. Расторгуев, С.. П. Основы информационной безопасности: учеб. пособие для вузов / С.П. Расторгуев. – Москва: Академия, 2007. – 129 с.

18. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - Москва : ЮНИТИ-ДАНА, 2017. - 287 с.

19. Галушкин, А. А. К вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» / А. А. Галушкин // Правозащитник. – 2015. - № 2. – С. 8.

20. Воронцова, Л.В. История и современность современного противоборства / Л.В. Воронцова, Л.Б. Фролов. - Горячая линия - телеком, 2006.

21. Прохожев, А. А. Общая теория национальной безопасности: учебник / А. А. Прохожев. - Москва: РАГС, 2005.

22. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба. – Санкт-Петербург: Питер, 2008.

23. Семкин, С.Н. Основы организационного обеспечения информационной безопасности объектов / С.Н. Семкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок. - Москва: Гелиос АРВ, 2005.

24. Стрельцов, А.А. Обеспечение информационной безопасности России/ А.А. Стрельцов. - МЦНМО, 2002.

25. Манойло, А.В. Государственная информационная политика в условиях информационно-психологической войны / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. - Москва: Горячая линия - Телеком, 2003.

26. Расторгуев, С.П. Информационная война. Проблемы и модели / С.П. Расторгуев. - Гелиос АРВ, 2006.

27. Белов, Е. Б. Основы информационной безопасности/ Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Телеком - Горячая линия, 2006.

28. Тихонов, В.А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В.А. Тихонов, В.В. Райх. - Москва: Гелиос АРВ, 2006.

29. Пархоменко, Н. Г. Выявление угроз информационной безопасности в реальном времени / Н. Г. Пархоменко, Н. М. Боташев, П. М. Колбанов, Е. С. Григоренко // Известия ЮФУ. Технические науки. – 2016. - №4. – С. 325-326.

30. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш, 3-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: http://znanium.com

31. Зайцев, А.П. Техническая защита информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – Москва : Горячая линия-Телеком, 2009. – 616 с.

32. Конеев, И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – Санкт-Петербург: БХВ-Петербург, 2003.

33. Ярочкин, В.И. Информационная безопасность учеб. для вузов / В.И. Ярочкин. – Москва: Академпроект, 2004.

34. Хорев, А.А Защита информации от утечки по техническим каналам. Ч. I. Технические каналы утечки информации: учебное пособие / А.А. Хорев. - Москва: Гостехкомиссия России, 1998. - 320 с.

35. Ищейнов, В. Я. Защита конфиденциальной информации: учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва: ФОРУМ, 2013. – 256 с.

36. Организационно-правовое обеспечение информационной безопасности: учеб. пособие / А. А. Стрельцов [и др.] ; под общ. ред. А. А. Стрельцова. – Москва : Академия, 2008. – 256 с.

37. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие для студентов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев. – Санкт-Петербург : Питер, 2008. - 272 с.

38. Просис, Крис. Расследование компьютерных преступлений / К. Просис, К. Мандиа ; пер. О. Труфанов. – Москва : ЛОРИ, 2013. – 76 с.

39. Жестовский, А.Г. Основы информационной безопасности: метод. указания по выполнению лабораторных работ / сост.: А. Г. Жестовский. – Калининград: Изд-во БГАРФ, 2020. - 28 с.

Локальный электронный методический материал

Александр Георгиевич Жестовский

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор Г. А. Смирнова

Уч.-изд. л. 3,5 Печ. л. 3,0

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