Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *ФПМ*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
23.05.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

Направление подготовки *10.03.01 Информационная безопасность*

Профиль подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
8	**72 / 2**	**14**		**12**	**1,4**	**0,25**	**27,65**	**44,35**	**Зач. с оц.**
Итого	**72 / 2**	**14**		**12**	**1,4**	**0,25**	**27,65**	**44,35**	

Муром, 2023 г.

1. Цель освоения дисциплины

Цель дисциплины: Формирование профессиональных навыков, связанных с физическими и инженерными принципами обеспечения информационной защиты, с потенциальными возможностями нарушителя по несанкционированному доступу и съему информации по техническим каналам утечки информации, с методами и средствами инженерно-технической защиты информации, с принципом действия, характеристиками и функциональными возможностями технических средств защиты информации.

Задачи: подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации; подготовка базовых теоретических понятий, лежащих в основе инженерно-технической защиты информации; создание представления о роли технических средств добывания (разведки) и защиты конфиденциальной информации на объектах информатизации от утечки по техническим каналам, а также контроле за эффективностью мер защиты; развитие способностей к логическому и алгоритмическому мышлению, навыков использования методов и способов инженерно-технической защиты информации; использования современных технических средств для определения технических каналов утечки информации и защиты информационных ресурсов.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита информации от утечки по техническим каналам» является дисциплиной по направлению 10.03.01 «Информационная безопасность» (бакалавриат). Дисциплина «Защита информации от утечки по техническим каналам» базируется на знаниях, полученных в рамках изучения следующих дисциплин: «Теория информации», «Математика», «Физика».

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Применяет средства технической защиты информации для решения задач профессиональной деятельности	Знать виды, назначения и возможности средств технической защиты информации (ОПК-9.1) Уметь применять средства технической защиты информации (ОПК-9.1)	тест

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Основные концептуальные положения инженерно - технической защиты информации.	8	2							8	тестирование
2	Виды информации, защищаемой техническими средствами.	8	2							7	тестирование
3	Демаскирующие признаки объектов защиты.	8	2							7	тестирование
4	Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей.	8	2							7	тестирование
5	Виды угроз безопасности информации, защищаемой техническими средствами.	8	2		4					7	тестирование
6	Принципы добывания и обработки информации техническими средствами.	8	2		4						тестирование
7	Классификация и структура технических каналов утечки информации.по техническим каналам.	8	2		4					8,35	тестирование

Всего за семестр	72	14		12			1,4	0,25	44,35	Зач. с оц.
Итого	72	14		12			1,4	0,25	44,35	

4.1.2. Содержание дисциплины
4.1.2.1. Перечень лекций

Семестр 8

Раздел 1. Основные концептуальные положения инженерно - технической защиты информации.

Лекция 1.

Способы и принципы работы средств защиты информации от наблюдения. Способы и средства противодействия наблюдению в оптическом диапазоне волн. Способы информационного скрытия объектов от радиолокационного наблюдения (2 часа).

Раздел 2. Виды информации, защищаемой техническими средствами.

Лекция 2.

Классификация объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем (2 часа).

Раздел 3. Демаскирующие признаки объектов защиты.

Лекция 3.

Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке) (2 часа).

Раздел 4. Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей.

Лекция 4.

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгенотелевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации (2 часа).

Раздел 5. Виды угроз безопасности информации, защищаемой техническими средствами.

Лекция 5.

Способы и принципы работы средств защиты информации от перехвата. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей (2 часа).

Раздел 6. Принципы добывания и обработки информации техническими средствами.

Лекция 6.

Способы и принципы работы средств защиты информации от подслушивания. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей.Способы и средства предотвращения утечки информации с помощью закладных устройств. Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации (2 часа).

Раздел 7. Классификация и структура технических каналов утечки информации.по техническим каналам.

Лекция 7.

Организационные и технические меры инженерно-технической защиты информации. Контроль эффективности защиты информации. рекомендации по выбору средств защиты (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 8

Раздел 5. Виды угроз безопасности информации, защищаемой техническими средствами.

Лабораторная 1.

Способы и принципы работы средств защиты информации от перехвата. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей (4 часа).

Раздел 6. Принципы добывания и обработки информации техническими средствами.

Лабораторная 2.

Способы и принципы работы средств защиты информации от подслушивания. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей.Способы и средства предотвращения утечки информации с помощью закладных устройств. Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации (4 часа).

Раздел 7. Классификация и структура технических каналов утечки информации.по техническим каналам.

Лабораторная 3.

Организационные и технические меры инженерно-технической защиты информации. Контроль эффективности защиты информации. рекомендации по выбору средств защиты (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Способы и средства защиты информации от наблюдения.
2. Теоретические вопросы обеспечения информационной безопасности.
3. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
4. Методы и средства выявления электронных устройств негласного получения информации.
5. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.
6. Организационные и технические меры инженерно-технической защиты информации. Контроль эффективности защиты информации.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе освоения дисциплины используются методы обучения, способствующие обеспечению положительного мотивационного настроя студентов на изучение учебного материала, формирование умений находить и применять информацию в области физики для успешного освоения профессионально ориентированных дисциплин и объектов будущей профессиональной деятельности: проблемного изложения, профессионального контекста, управления самостоятельной работой.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Ворожейкин, В. Н. Технические средства и методы защиты информации – дополнительные главы : лабораторный практикум / В. Н. Ворожейкин. — 2-е изд. — Самара : Самарский государственный технический университет, ЭБС АСВ, 2019. — 336 с. - https://www.iprbookshop.ru/111432.html

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. - https://www.iprbookshop.ru/97562.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 194 с. - https://www.iprbookshop.ru/13989.html

2. Солонская, О. И. Средства защиты информации : учебное пособие для СПО / О. И. Солонская. — Саратов : Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. - https://www.iprbookshop.ru/125578.html

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

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

http://e.lib.vlsu.ru/

http://www.uisrussia.msu.ru/is4/main.jsp

http://elibrary.ru

Программное обеспечение:

Mathcad Education – University Edition (100 pack) v.15 (Государственный контракт №1 от 10.01.2012 года)

Google Chrome (Лицензионное соглашение Google)

Mozilla Firefox (MPL)

Zoom (Свободно распространяемое ПО Freemium)

Free Commander XE (Лицензионное соглашение FreeCommander)

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal (продление) (Гражданско-правовой договор бюджетного учреждения №2020.526633 от 23.11.2020 года)

Microsoft Windows 10 Professional (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Pascal PascalABC.NET (GNU Lesser General Public License v.3)

Apache OpenOffice (Apache License)

Lazarus (GNU GPL, GNU LGPL)

Microsoft Access (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft SQL Server (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Adobe Acrobat Reader DC (Общие условия использования продуктов Adobe)

Python 3.9.4 (Python Software Foundation License)

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru

e.lib.vlsu.ru

uisrussia.msu.ru

elibrary.ru

mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория сетей и систем передачи информации

Стенд «Криптография» CRYPTO; стойка с телекоммуникационным оборудованием, системой питания и вентиляции; ПК CPU-Intel Core i5-4460 BOX - 12 шт.; ПК — 1шт.; экран DRAPPER Apex STAR; видеопроектор InFocus; коммутатор. Доступ к сети Интернет.

Лаборатория программно-аппаратных средств защиты информации

Программно-аппаратный комплекс RadioInspector WIFI 2 ; портативный RFID считыватель cipherLab 1862; компьютер для проведения мультимедиалекций Raspberry; персональный компьютер Mini PC Android MK808 B; ПК CPU-Intel Core i5-4460 BOX - 12 шт.; ПК — 1шт.; экран DRAPPER Apex STAR; видеопроектор InFocus; коммутатор. Доступ к сети Интернет.

Лаборатория технической защиты информации

Подавитель телефона Троян X6-B; генератор шума Штора-1; блок помех генераторный SEL SP-157G с вибрационным преобразователем и колонкой; комбинированное устройство защиты от утечки информации ЛГШ-513; детектор жучков Баг Хантер «Профессионал»; сканер отпечатков пальцев Eikon; сканер глаза EyeLock; офисный электронный замок EM-Marine, PROXIMITY (125kHz) AYT 930-6-DI; дубликатор KeyMaster PRO 4 RF (с комплектом ключей); аппаратно-программный модуль доверенной загрузки "Соболь" с сертификатом ФСТЭК; квадрокоптер DJI Phantom 3 Professional (в комплекте дисплей-планшет Samsung Galaxy Tab 4 10.1 SM-T530 16Gb; пульт управления и рюкзак); камера D-Link DCS-930L; IP камера Beward BD2570; анализатор спектра; система видеонаблюдения Orient; видеопроектор

NEC Projector V260XG (переносной); ноутбук ASUS (переносной); экран мобильный Classic Solution Premier Vela Express; ПК ПЭВМ «Хопер» -2 шт.; ПК - 5 шт.;ПК:(mATX350W;IC2,8;1Gb;DVD-R;3,5"S775PCI-E;К-ра PS/2;M/Опт.PS/2;19"TFT)-1 шт.. Доступ к сети Интернет.

Защищаемое помещение

Помещение оборудовано для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений , составляющих государственную тайну

Библиотека литературы ограниченного доступа

Помещение оборудовано для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторная работа проводятся в компьютерном классе. Обучающиеся выполняют индивидуальную задачу компьютерного моделирования в соответствии с заданием на лабораторную работу. Полученные результаты исследований сводятся в отчет и защищаются по традиционной методике в классе на следующем лабораторном занятии. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы и требование к отчету приведены в методических указаниях, размещенных на информационно-образовательном портале института.: https://www.mivlgu.ru/iop/course/view.php?id=2863

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – зачет с оценкой. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *10.03.01 Информационная безопасность* и профилю подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*
Рабочую программу составил *к.т.н., доцент Штыков Р. А.*_____

Программа рассмотрена и одобрена на заседании кафедры *ФПМ*

протокол № 19 от 26.04.2023 года.
Заведующий кафедрой *ФПМ* _____*Орлов А.А.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 9 от 19.05.2023 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине

Защита информации от утечки по техническим каналам

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Задание 1

Вопрос 1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

1) политическая разведка;

2) промышленный шпионаж;

3) добросовестная конкуренция;

4) конфиденциальная информация;

5) правильного ответа нет.

Вопрос 2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности ?

1) любая информация;

2) только открытая информация;

3) запатентованная информация;

4) закрываемая собственником информация;

5) коммерческая тайна.

Вопрос 3. Кто может быть владельцем защищаемой информации?

1) только государство и его структуры;

2) предприятия акционерные общества, фирмы;

3) общественные организации;

4) только вышеперечисленные;

5) кто угодно.

Вопрос 4. Какие сведения на территории РФ могут составлять коммерческую тайну?

1) учредительные документы и устав предприятия;

2) сведенья о численности работающих, их заработной плате и условиях труда;

3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;

4) другие;

5) любые.

Вопрос 5. Какие секретные сведения входят в понятие «коммерческая тайна»?

1) связанные с производством;

2) связанные с планированием производства и сбытом продукции;

3) технические и технологические решения предприятия;

4) только 1 и 2 вариант ответа;

5) три первых варианта ответа.

Задание 2

Вопрос 1. Что называют источником конфиденциальной информации?

1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;

2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;

3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;

4) это защищаемые предприятием сведения в области производства и коммерческой деятельности;

5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

Вопрос 2. Как называют процессы обмена информацией с помощью официальных, деловых документов?

1) непосредственные;

2) межличностные;

3) формальные;

4) неформальные;

5) конфиденциальные.

Вопрос 3. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?

1) хищение носителей информации;

2) использование технических средств для перехвата электромагнитных ПЭВМ;

3) разглашение;

4) копирование программой информации с носителей;

5) другое.

Вопрос 4. Каким образом происходит разглашение конфиденциальной информации?

1) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;

2) опубликование материалов в печати;

3) сообщение, передача, предоставление в ходе информационного обмена;

4) все вышеперечисленные способы;

5) правильного варианта ответа нет.

Задание 3

Вопрос 1. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

1) получить, изменить, а затем передать ее конкурентам;

2) размножить или уничтожить ее;

3) получить, изменить или уничтожить;

4) изменить и уничтожить ее;

5) изменить, повредить или ее уничтожить.

Вопрос 2. Какой самый прямой и эффективный способ склонения к сотрудничеству?

1) психическое давление;

2) подкуп;

3) преследование;

4) шантаж;

5) угрозы.

Вопрос 3. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?

1) инициативное сотрудничество;

2) выпытывание;

3) наблюдение;

4) хищение;

5) копирование.

Вопрос 4. Какое из утверждений неверно?

1) подкуп — сложный процесс, требует долгой и кропотливой работы;

2) выпытывание — это стремление путем внешне наивных вопросов получить определенные сведения;

3) процесс наблюдения не сложен, так как не требует затрат сил и средств;

4) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;

5) негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.

Вопрос 5. Завершающим этапом любого сбора конфиденциальной информации является

1) копирование;
2) подделка;
3) аналитическая обработка;
4) фотографирование;
5) наблюдение.

Задание 4

Вопрос 1. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?

1) ненадежность;
2) угроза;
3) несчастный случай;
4) авария;
5) правильного ответа среди перечисленных нет.

Вопрос 2. Что в скором времени будет являться главной причиной информационных потерь?

1) материальный ущерб, связанный с несчастными случаями;
2) кража и преднамеренная порча материальных средств;
3) информационные инфекции;
4) аварии и выход из строя аппаратуры, программ и баз данных;
5) ошибки эксплуатации.

Вопрос 3. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

1) логические бомбы, троянский конь, червь, вирус;
2) червь, вирус логические бомбы, троянский конь;
3) червь логические бомбы вирус, троянский конь;
4) логические бомбы, вирус, троянский конь червь;
5) вирус, логические бомбы, троянский конь червь.

Вопрос 4. Причины связанные с информационным обменом приносящие наибольшие убытки?

1) остановка или выход из строя информационных систем;
2) потери информации;
3) неискренность;
4) проникновение в информационную систему;
5) перехват информации.

Вопрос 5. Какие цели преследуются при активном вторжении в линии связи?

1) анализ информации(содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;
3) инициализация ложных соединений;
4) варианты 1 и 2;
5) варианты 2 и 3.

Задание 5

Вопрос 1. Что определяет модель нарушителя?

1) категории лиц, в числе которых может оказаться нарушитель;
2) возможные цели нарушителя и их градации по степени важности и опасности;
3) предположения о его квалификации и оценка его технической вооруженности;
4) ограничения и предположения о характере его действий;
5) все выше перечисленные.

Вопрос 2. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.

1) ознакомление с информационной системой или вычислительной сетью;

2) похитить программу или иную информацию;

3) оставить записку, выполнить, уничтожить или изменить программу;

4) вариант 2 и 3;

5) вариант 1, 2 и 3.

Вопрос 3. Какое из утверждений неверно?

1) наблюдается тенденция к стремительному росту попыток получить несанкционированный доступ к информационным системам или вычислительным сетям;

2) недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования;

3) считается, что компьютерные преступления, более легкий путь добывания денег, чем ограбление банков;

4) очень малое число фирм могут пострадать от хакеров;

5) к категории хакеров-профессионалов обычно относят: преступные группировки, преследующие политические цели.

Вопрос 4. Какое из утверждений неверно?

1) хакеры могут почерпнуть много полезной информации изгазети других периодических изданий;

2) хакерами часто используется завязывание знакомств для получения информации о вычислительной системе или выявления служебных паролей;

3) один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации и доступа к ЭВМ — просто изучая черновые распечатки;

4) о перехвате сообщений в каналах связиречь может идти лишь в связи с деятельностью военных или секретных служб;

5) после получения необходимого объема предварительной информации, компьютерный хакер-профессионал осуществляет непосредственное вторжение в систему.

Вопрос 5. Какое из утверждений неверно?

1) наибольшие убытки (в среднем) приносит саботаж в нематериальной сфере;

2) убытки, связанные с забастовками не превышают убытков связанных с аварией оборудования;

3) уход ведущих специалистов опасен для малых центров;

4) хищения, в первую очередь осуществляются сотрудниками предприятия или пользователями;

5) аварии оборудования или основных элементов системы являются мало распространенными и определяются надежностью аппаратуры.

Задание 6

Вопрос 1. Метод скрытие — это...

1) максимальное ограничение числа секретов, из-за допускаемых к ним лиц;

2) максимального ограничения числа лиц, допускаемых к секретам;

3) уменьшение числа секретов неизвестных большинству сотрудников;

4) выбор правильного места, для утаивания секретов от конкурентов;

5) поиск максимального числа лиц, допущенных к секретам.

Вопрос 2. Что включает в себя ранжирование как метод защиты информации?

1) регламентацию допуска и разграничение доступа к защищаемой информации;

2) деление засекречиваемой информации по степени секретности;

3) наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;

4) вариант ответа 1 и 2;

5) вариант ответа 1, 2 и 3.

Вопрос 3. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?

1) скрытие;

2) дезинформация;

3) дробление;

4) кодирование;

5) шифрование.

Вопрос 4. Что в себя морально-нравственные методы защиты информации?

1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;

2) контроль работы сотрудников, допущенных к работе с секретной информацией;

3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;

4) вариант ответа 1 и 3;

5) вариант ответа 1, 2 и 3.

Вопрос 5. Какое из выражений неверно?

1) страхование — как метод защиты информации пока еще не получил признания;

2) кодирование — это метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации;

3) шифрование может быть предварительное и линейное;

4) дирекция очень часто не может понять необходимость финансирования безопасности;

5) безопасность предприятия — не стабильное состояние предприятия, не поддающееся прогнозированию во времени.

Задание 7

Вопрос 1. Какой должна быть защита информации с позиции системного подхода?

1) безопасной для сотрудников;

2) активной;

3) универсальной;

4) надежной;

5) непрерывной.

Вопрос 2. Что такое «служба безопасности»?

1) система внештатных формирований, предназначенных для обеспечения безопасности объекта;

2) структурное подразделение, предназначенное для охраны помещений и территорий предприятия;

3) система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации;

4) структурное подразделение, предназначенное для хранения и выдачи документов, носителей конфиденциальной информации;

5) структурное подразделение, задача которого: подбор персонала и работа с сотрудниками.

Вопрос 3. Кому подчиняется служба безопасности?

1) владельцу предприятия;

2) владельцу предприятия и лицу которому тот подчиняется;

3) руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;

4) заместителю руководителя предприятия по организационным вопросам;

5) только начальнику службы безопасности.

Вопрос 4. Какие задачи не входят в круг обязанностей службы безопасности ?

1) внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической безопасности предприятия;

2) определение участков сосредоточения сведений, составляющих коммерческую тайну;

3) определение на предприятии технологического оборудования, выход из строя которого может привести к большим экономическим потерям;

4) ограничение круга сторонних предприятий, работающих с данным предприятием, на которых возможен выход из-под контроля сведений составляющих коммерческую тайну предприятия;

5) определение круга сведений, составляющих коммерческую тайну.

Вопрос 5. Какие средства использует инженерно-техническая защита (по функциональному назначению)?

1) программные, аппаратные, криптографические, технические;

2) программные, физические, шифровальные, криптографические;

3) программные, аппаратные, криптографические физические;

4) физические, аппаратные, материальные, криптографические;

5) аппаратные, физические, программные, материальные.

Задание 8

Вопрос 1. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?

1) в Конституции РФ;

2) в Законе об оперативно розыскной деятельности;

3) в Законе об частной охране и детективной деятельности;

4) в Законе об информации, информатизации и защите информации;

5) в Указе Президента РФ № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации».

Вопрос 2. На какую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны

1) Министерство Информатики РФ;

2) Комитет по Использованию Информации при Госдуме;

3) Росинформресурс;

4) все выше перечисленные;

5) правильного ответа нет.

Вопрос 3. На каком уровне защиты информации создаются комплексные системы защиты информации?

1) на организационно-правовом;

2) на социально политическом;

3) на тактическом;

4) на инженерно-техническом;

5) на всех вышеперечисленных.

Вопрос 4. Какие существуют наиболее общие задачи защиты информации на предприятии?

1) снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной;

2) предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;

3) документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;

4) создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;

5) все вышеперечисленные.

Вопрос 5. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?

1) воспитание понимания важности сохранения в тайне доверенных им секретных или конфиденциальных сведений;

2) подбор людей, допускаемых к секретным работам;

3) обучение лиц, допущенных к секретам, правилам их сохранения;

4) добровольное согласие на запрет работы по совместительству у конкурентов;

5) стимулирование заинтересованности работы с засекреченной информацией и сохранения этих сведений в тайне.

Задание 9

Вопрос 1. В каком документе содержаться основные требования к безопасности информационных систем в США?

1) в красной книге;

2) в желтой прессе;

3) в оранжевой книге;

4) в черном списке;

5) в красном блокноте.

Вопрос 2. Какое определение соответствует термину «Аутентификация»?

1) набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации;

2) распознавание имени объекта;

3) подтверждение того, что предъявленное имя соответствует объекту;

4) регистрация событий, позволяющая восстановить и доказать факт происшествия событий;

5) правильного определения нет.

Вопрос 3. Какое требование относится к термину «Подотчетность»?

1) субъекты индивидуально должны быть идентифицированы;

2) гарантированно защищенные механизмы, реализующие указанные базовые требования, должны быть постоянно защищены от "взламывания";

3) необходимо иметь явную и хорошо определенную политику обеспечения безопасности;

4) аудиторская информация должна храниться и защищаться так, чтобы имелась возможность отслеживать действия, влияющие на безопасность;

5) метки, управляющие доступом, должны быть установлены и связаны с объектами.

Вопрос 4. Какой уровень безопасности системы соответствует низшему?

1) A;

2) B;

3) C;

4) D;

5) E.

Вопрос 5. Какой класс присваивается системам которые не прошли испытания?

1) A1;

2) B2:

3) B3;

4) C4;

5) D.

Задание 10

Вопрос 1. Что включают в себя технические мероприятия по защите информации?

1) поиск и уничтожение технических средств разведки;

2) кодирование информации или передаваемого сигнала;

3) подавление технических средств постановкой помехи;

4) применение детекторов лжи;

5) все вышеперечисленное.

Вопрос 2. Какие устройства поиска технических средств разведки не относятся к устройствам поиска пассивного типа?

1) металлоискатели;

2) тепловизоры;
3) устройства и системы поиска по электромагнитному излучению;
4) аккустические корреляторы;
5) детекторы записывающей аппаратуры.

Вопрос 3 Какие устройства не относятся к устройствам поиска по электромагнитному излучению?

1) частотомер;
2) шумомер;
3) сканер;
4) нелинейный локатор;
5) анализатор спектра.

Вопрос 4. Какова цена самого дешевого японского компактного приемника-сканера?

1) 200 US$.
2) 300 US$.
3) 500 US$.
4) 700 US$.
5) 900 US$.

Вопрос 5. Какова дальность обнаружения звукозаписывающей аппаратуры?

1) 1 м.
2) более 1 м.
3) менее 1 м.
4) 3 м.
5) 5 м.

Задание 11

Вопрос 1. Какова скорость перемешивания частотных интервалов при частотном скремблировании?

1) 1 цикл в сек.
2) 20 циклов в сек.
3) От 20 до 30 циклов в сек.
4) От 2 до 16 циклов в сек.
5) От 30 до 40 циклов в сек.

Вопрос 2. С какого расстояния можно считать информацию с монитора компьютера?

1) 200 м.
2) менее 200 м.
3) 500 м.
4) 750 м.
5) 1 км.

Вопрос 3. Какие материалы не применяются при экранировании помещения?

1) листовая сталь;
2) медная сетка;
3) алюминиевая фольга;
4) все вышеперечисленные;
5) фтористая сетка.

Вопрос 4. Какое устройство позволяет обеспечивать защищенность от разного рода сигналов генерируемых устройствами, которые могут служить источником утечки информации?

1) приемник-сканер;
2) телефонный адаптер;
3) скремблер;
4) сетевой фильтр;
5) все вышеперечисленные.

Вопрос 5. Какие существуют основные типы детекторов лжи?

1) полиграф;

2) сигнализатор психологического стресса;
3) анализатор стресса по голосу;
4) все вышеперечисленные;
5) правильного ответа нет.

Задание 12

Вопрос 1. Какие основные направления в защите персональных компьютеров от несанкционированного доступа Вы знаете?

1) недопущение нарушителя к вычислительной среде;
2) защита вычислительной среды;
3) использование специальных средств защиты информации ПК от несанкционированного доступа;
4) все вышеперечисленные;
5) правильного ответа нет.

Вопрос 2. По скольким образцам почерка определяются параметры при опознавании пользователей ПК по почерку?

1) 1-3;
2) 3-5;
3) 5-10;
4) 10-15;
5) 15-18.

Вопрос 3. Какие средства защиты информации в ПК наиболее распространены?

1) применение различных методов шифрования, не зависящих от контекста информации;
2) средства защиты от копирования коммерческих программных продуктов;
3) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
4) защита от компьютерных вирусов и создание архивов;
5) все вышеперечисленные.

Вопрос 4. Какой программный продукт предназначен для защиты жесткого диска от несанкционированного доступа?

1) MAWR, ver. 5.01;
2) PROTEST.COM, ver. 3.0:
3) PASSW, ver. 1.0;
4) ADM, ver. 1.03;
5) Все вышеперечисленные.

Вопрос 5. Какое утверждение неверно?

1) чтобы уменьшить потери по эксплуатационным причинам, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов;
2) программы-архиваторы позволяют не только сэкономить место на архивных дискетах, но и объединять группы совместно используемых файлов в один архивный файл, что заметно облегчает ведение архивов:
3) информация на жестком диске может разрушиться только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя;
4) единственно надежным способом уберечь информацию от любых разрушительных случайностей является четкая, неукоснительно соблюдаемая система резервного копирования;
5) одним из основных симптомов, возникновения серьезных дефектов на диске, является замедление работы дисковода.

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	тесты	16
Рейтинг-контроль 2	тесты	16

Рейтинг-контроль 3	тесты	32
Посещение занятий студентом		16
Дополнительные баллы (бонусы)		5
Выполнение семестрового плана самостоятельной работы		15

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

Пример заданий для выполнения тестов:

1. Что представляет собой ресурс системы защиты информации ?

А - количество специалистов по защите информации

В - состав инженерно-технических сооружений

С - выделенные денежные средства

Д – все вместе

2. Что надо определить перед выбором мер защиты информации ?

А – квалификацию персонала

В – угрозы безопасности информации

С – систему пожарно-охранной сигнализации

3. Локальные показатели эффективности защиты информации подразделяются на :

А – тактические и стратегические

В – оперативные и постоянные

С – функциональные и экономические

Д – территориальные и пространственные

4. Что означает принцип экономичности защиты информации?

А – минимизация затрат на защиту информации

В – затраты на защиту информации не должны превышать возможный ущерб от реализации угроз

С – численность службы защиты информации не должна превышать 7 чел.

Д – комплексное использование различных способов и средств защиты информации

5. Что означает принцип рациональности защиты информации?

А – использование только сертифицированных средств защиты

В – системный подход к инженерно—технической защите информации

С – минимизацию ресурсов на обеспечение необходимого уровня безопасности информации

Д – все вместе

Методические материалы, характеризующие процедуры оценивания

Индивидуальный семестровый рейтинг студента формируется на основе действующего в ВУЗе Положения "О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся".

В течение семестра студент получает баллы успеваемости за выполнение всех видов учебных поручений: посещение лекций, выполнение практических работ.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

Примеры заданий в тестовой форме для контроля остаточных знаний:

1 Технические средства охраны это

1 сочетание организационных и технических мер, направленных на обеспечение сохранности материальных средств и носителей информации

2 оснащенные техническими средствами подразделения охраны

3 устройства и системы, а также сооружения, предназначенные для создания физических препятствий нарушителю, своевременного его обнаружения и блокирования его действий

2 В акустических каналах связи используют

1 только инфразвук и ультразвук

2 звук, лежащий в полосе ультразвукового, слышимого и инфразвукового диапазонов

3 только слышимый звук

3 Что относится к активным методам защиты от акустической разведки

1 звукоизоляция помещений

2 формирование маскирующих вибрационных и акустических помех

3 выявление несанкционированных подключений к телефонным линиям связи

4 Что может использовать злоумышленник, если он хочет снять информацию с оконного стекла, которое вибрирует под воздействием акустических волн внутри помещения

1 Плоский микрофон

2 Стетоскоп

3 Лазерный микрофон

4 Трубчатый микрофон

5 Какие параметры электрических цепей чаще всего изменяются под воздействием акустической волны в пассивных акустоэлектрических преобразователях

1 Индуктивность

2 Сопротивление

3 Длина

4 Емкость

6 Оптическая разведка включает

1 Фотографическую

2 Визуальную

3 Инфракрасную

4 Лазерную

7 По цилиндрической трубе диаметром d = 20 см и длиной l = 5 м, заполненной сухим воздухом, распространяется звуковая волна средней за период интенсивностью j = 50 мВт/м². Найти энергию звукового поля, заключенного в трубе.

Энергия поля, заключенного в некотором обьеме W <w> v где

v=(πd^2)/4*l - объем цилиндрической трубы

Объемную плотность энергии определим из формулы j <w>Vзв

<w> j/Vзв , где Vзв = 332 м/с табличное значение

Следовательно энергия звукового поля в трубе будет равна

W=(jπd^2 l)/(Vзв*4) = (5*〖 10〗 ^(-2)*3,14*〖 0,2〗 ^2*5)/(4*332) = 23,6 мкДж

Ответ: 23,6

8 Найдите какую длину волны показывает приемник, если ёмкость конденсатора в его колебательном контуре равна C2 = 500 пФ, а индуктивность катушки L = 20 мкГн?

Длина волны, которую воспринимает радиоприемник, равна

λ=2πc√LC

Соответственно, чтобы узнать диапазон, нужно найти максимальную и минимальную длины волн, соответствующие минимальной и максимальной емкостям конденсатора:

λ2=2πc√LC=2*3,14*3*〖 10〗 ^8*√(500*〖 10〗 ^(-12)*20*〖 10〗 ^(-6))=188 м

Ответ: 188

9 Определить длину электромагнитных волн в воздухе, излучаемых колебательным контуром с емкостью 3 нФ и индуктивностью 0,012 Гн. Активное сопротивление контура принять равным нулю.

Применим формулу для периода колебаний колебательного контура:

T=2π√LC

А теперь вспомним, как длина волны связана с периодом колебаний:

λ=cT

Отсюда: λ=2πc√LC=2*3,14*3*〖 10〗 ^8*√(0,012*3*〖 10〗 ^(-9))=11304 м

Ответ: 11304

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?courseid=2961&cat=31361%2C100302

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.