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
21.05.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью

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.)
6	**72 / 2**	**16**		**16**	**1,6**	**0,25**	**33,85**	**38,15**	**Зач. с оц.**
7	**324 / 9**	**32**		**64**	**5,2**	**0,35**	**101,55**	**186,8**	**Экз.(35,65)**
Итого	**396 / 11**	**48**		**80**	**6,8**	**0,6**	**135,4**	**224,95**	**35,65**

Муром, 2024 г.

1. Цель освоения дисциплины

Цель дисциплины: формирование знаний в области теоретических основ управления информационной безопасностью и навыков практического обеспечения защиты информации.

Задачами изучения дисциплины являются:

- формирование навыков организации и методологии обеспечения информационной безопасности;
- создание представления о функциях, структурах и штатах подразделения информационной безопасности;
- изучение организационных основ, принципов, методов и технологий управления информационной безопасностью;
- развитие способностей по использованию существующей системы управления информационной безопасности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы управления информационной безопасностью» базируется на знаниях, полученных в рамках изучения следующих дисциплин: "Математика", "Физика", "Методы научного исследования". Дисциплина «Основы управления информационной безопасностью» является теоретическим и методологическим основанием для дисциплины: "Защита информации от утечки по техническим каналам" входящей в ОПОП бакалавра по направлению 10.03.01 «Информационная безопасность».

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-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.1 Разрабатывает и внедряет политики управления доступом в компьютерных системах	Знать политику управления доступом в компьютерных системах (ОПК-1.1.1) Уметь разрабатывать и внедрять политики управления доступом в компьютерных системах (ОПК-1.1.1)	вопросы к устному опросу, тест
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и	ОПК-6.2 Оценивает и систематизирует информацию, обрабатываемую в информационных системах	Знать способы оценки и систематизации информации, обрабатываемой в информационных системах (ОПК-6.2) Уметь оценивать и систематизировать информацию, обрабатываемую в информационных системах (ОПК-6.2)	вопросы к устному опросу, тест

экспортному контролю			
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 Разрабатывает и внедряет политику информационной безопасности	Знать способы реализации политики информационной безопасности (ОПК-10.1) Уметь разрабатывать и внедрять политику информационной безопасности (ОПК-10.1)	вопросы к устному опросу, тест

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 11 зачетных единиц, 396 часов.

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	Стандарты и основы управления информационной безопасностью	6	14		16					26	устный опрос, тестирование
2	Методы и технологии управления информационной безопасностью	6	2							12,15	устный опрос, тестирование
Всего за семестр		72	16		16			1,6	0,25	38,15	Зач. с оц.
3	Методы и технологии управления информационной безопасностью	7	18		16					13,85	устный опрос, тестирование
4	Анализ рисков и угроз информационной безопасности	7	14		48					172,95	устный опрос, тестирование
Всего за семестр		324	32		64			5,2	0,35	186,8	Экз.(35,65)
Итого		396	48		80			6,8	0,6	224,95	35,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 6

Раздел 1. Стандарты и основы управления информационной безопасностью

Лекция 1.

Актуальность проблемы информационной безопасности (2 часа).

Лекция 2.

Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Основные понятия и определения (2 часа).

Лекция 3.

Политика государства в области информационной безопасности (2 часа).

Лекция 4.

Правовые основы обеспечения информационной безопасности (2 часа).

Лекция 5.

Угрозы безопасности информации (2 часа).

Лекция 6.

Модель угроз безопасности информации (2 часа).

Лекция 7.

Меры и методы обеспечения защиты информации (2 часа).

Раздел 2. Методы и технологии управления информационной безопасностью

Лекция 8.

Источники угроз. Модель нарушителя безопасности информации (2 часа).

Семестр 7

Раздел 3. Методы и технологии управления информационной безопасностью

Лекция 9.

Организационные (процедурные, административные) меры защиты информации (2 часа).

Лекция 10.

Инженерно-технические меры защиты информации (2 часа).

Лекция 11.

Идентификация и аутентификация. Управление доступом (2 часа).

Лекция 12.

Межсетевое экранирование. Обеспечение высокой доступности (2 часа).

Лекция 13.

Протоколирование и аудит. Системы обнаружения и предотвращения компьютерных атак (2 часа).

Лекция 14.

Криптографические методы защиты информации. Электронная цифровая подпись (2 часа).

Лекция 15.

Контроль целостности (2 часа).

Лекция 16.

Вредоносные программы и защита от них (2 часа).

Лекция 17.

Защита информации в компьютерных сетях (2 часа).

Раздел 4. Анализ рисков и угроз информационной безопасности

Лекция 18.

Тестирование на проникновение. Социальная инженерия (2 часа).

Лекция 19.

Меры по обеспечению безопасности данных при их обработке в информационных системах персональных данных и государственных информационных системах (2 часа).

Лекция 20.

Лицензирование и сертификация в области ИБ (2 часа).

Лекция 21.

Аттестация объектов информатизации (2 часа).

Лекция 22.

Выбор средств ИБ. Управление рисками ИБ (2 часа).

Лекция 23.

Компьютерные преступления, инциденты ИБ и их расследование. Форензика (2 часа).

Лекция 24.

Основные стандарты и спецификации в области информационной безопасности. Цифровая гигиена (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 6

Раздел 1. Стандарты и основы управления информационной безопасностью

Лабораторная 1.

Угрозы безопасности информации (4 часа).

Лабораторная 2.

Модель угроз безопасности информации (4 часа).

Лабораторная 3.

Источники угроз. Модель нарушителя безопасности информации (4 часа).

Лабораторная 4.

Меры и методы обеспечения защиты информации (4 часа).

Семестр 7

Раздел 3. Методы и технологии управления информационной безопасностью

Лабораторная 5.

Организационные (процедурные, административные) меры защиты информации (4 часа).

Лабораторная 6.

Инженерно-технические меры защиты информации (4 часа).

Лабораторная 7.

Идентификация и аутентификация. Управление доступом (4 часа).

Лабораторная 8.

Межсетевое экранирование. Обеспечение высокой доступности (4 часа).

Раздел 4. Анализ рисков и угроз информационной безопасности

Лабораторная 9.

Протоколирование и аудит. Системы обнаружения и предотвращения компьютерных атак (4 часа).

Лабораторная 10.

Криптографические методы защиты информации. Электронная цифровая подпись (4 часа).

Лабораторная 11.

Контроль целостности (4 часа).

Лабораторная 12.

Вредоносные программы и защита от них (4 часа).

Лабораторная 13.

Защита информации в компьютерных сетях (4 часа).

Лабораторная 14.

Тестирование на проникновение. Социальная инженерия (4 часа).

Лабораторная 15.

Меры по обеспечению безопасности данных при их обработке в информационных системах персональных данных и государственных информационных системах (4 часа).

Лабораторная 16.

Лицензирование и сертификация в области ИБ (4 часа).

Лабораторная 17.

Аттестация объектов информатизации (4 часа).

Лабораторная 18.

Выбор средств ИБ (4 часа).

Лабораторная 19.

Управление рисками ИБ (4 часа).

Лабораторная 20.

Компьютерные преступления, инциденты ИБ и их расследование. Форензика (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Идентификация и установление подлинности (аутентификация).
2. Основные меры предосторожности при работе с паролями.
3. Биометрические средства и технологии установления подлинности.
4. Способы разграничения прав доступа и их модели.
5. Технологии предотвращения сетевых атак на информационные системы.
6. Стандарты защищенности. Основные виды угроз.
7. Интегрированная защита сети.
8. Специфика защиты линий связи (каналов передачи данных).
9. Особенности защиты баз данных.
10. Подсистема управления сети.
11. Защита подсистемы управления сети.
12. Ресурсы и их целостность.
13. Логическая модель архитектуры сети.
14. Контекстная защита данных и ее специфика.
15. Суть и назначение криптографического протокола.
16. Специфика проблем безопасности в глобальных сетях.
17. Понятие цифровых сертификатов.
18. Депонирование ключей и защита цифровой подписи.
19. Представление о моделях доверия.
20. Примеры и особенности защищенных сетевых протоколов.
21. Причины использования протоколов прикладного уровня, обеспечивающих безопасность информации и ее эффективную защищенность.
22. Особенности и проблемы применения биометрических средств защиты.

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 изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении лабораторных работ применяется имитационный подход.

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. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. - https://www.iprbookshop.ru/87643.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. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. - https://www.iprbookshop.ru/72444.html

2. Абденов, А. Ж. Современные системы управления информационной безопасностью : учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск : Новосибирский государственный технический университет, 2017. — 48 с. — ISBN 978-5-7782-3236-5. - https://www.iprbookshop.ru/91427.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:

Национальный открытый университет ИНТУИТ - http://www.intuit.ru/

Информационно-аналитический ресурс "Портал ISO27000" - http://www.iso27000.ru/

Образовательный портал "Единое окно доступа к образовательным ресурсам" - http://window.edu.ru/

Программное обеспечение:

LibreOffice (Mozilla Public License v2.0)

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

Google Chrome (Лицензионное соглашение Google)

Mozilla Firefox (MPL)

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)

Oracle VirtualBox (GNU GPL)

StegHideUI (GNU GPL v.2)

Sysinternals Suite (Лицензионное соглашение Sysinternals)

Apache OpenOffice (Apache License)

Kaspersky Virus Removal Tools (Лицензионное соглашение ООО "Лаборатория Касперского")

Python 3.9.4 (Python Software Foundation License)

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

iprbookshop.ru
intuit.ru
iso27000.ru
window.edu.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.

Компьютерный класс

ПК CPU-Intel Core i5-4460 BOX - 12 шт.; ПК — 1шт.; экран DRAPPER Apex STAR; видеопроектор InFocus; коммутатор. Доступ к сети Интернет.

Помещение для самостоятельной работы обучающихся

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 Х6-В; 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;М/Опт.PS/2;19"TFT)-1 шт.. Доступ к сети Интернет.

Лекционная аудитория

Доска меловая 3-х элементная; системный блок IC 2.8; проектор мультимедийный NEC Projector V302XG; экран настенный LMP-100109; доступ к сети Интернет.

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся необходимо ознакомится со списком рекомендуемой основной и дополнительной литературы: https://www.mivlgu.ru/iop/course/view.php?id=2863

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 – экзамен. 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 № 21 от 02.05.2024 года.
Заведующий кафедрой *ФПМ* _____*Орлов А.А.*
(Подпись)

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

протокол № 9 от 17.05.2024 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине
Основы управления информационной безопасностью

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Темы для устного опроса (рейтинг-контроль №1):

1. Назовите уровни правовой основы защиты информации?
2. Какие меры по охране конфиденциальности информации, составляющей коммерческую тайну вы знаете?
3. Назовите основные объекты защиты информации?
4. Что такое угроза информационной безопасности?
5. Перечислите классификацию угроз информационной безопасности?
6. Какие вы знаете методы анализа и оценки угроз?
7. Что такое утечка информации?
8. Назовите каналы утечки информации, и их характеристики.
9. Какие вы знаете меры по предотвращению прямых каналов утечки информации?
10. Какие вы знаете меры по предотвращению косвенных (технических) каналов утечки информации?

Темы для устного опроса (рейтинг-контроль №2):

1. Что такое режим секретности?
2. Что такое государственная тайна?
3. Назовите признаки государственной тайны?
4. Назовите главные элементы режима секретности?
5. Что такое аудит?
6. Назовите модели активного аудита?
7. Основная цель защиты конфиденциальной информации.
8. Что относится к административному уровню информационной безопасности?
9. Что такое политика безопасности административного уровня?
10. Что такое внутриобъектовый режим?
11. Что такое пропускной режим?
12. Назовите основные задачи пропускного режима?
13. Что включает в себя обеспечение защиты конфиденциальной информации?

Темы для устного опроса (рейтинг-контроль №3):

1. Что такое риск? Анализ рисков?
2. Назовите цели анализа рисков?
3. Назовите методы оценки рисков?
4. Как происходит организация контроля доступа к конфиденциальной и секретной информации?
5. Назовите этапы процесса управления рисками?
6. Назовите основные направления международного сотрудничества РФ в области обеспечения информационной безопасности?
7. Какие объекты международного информационного обмена указываются в Законе «Об участии в международном информационном обмене»?
8. Что является целью Закона «Об участии в международном информационном обмене»?
9. Назовите основные правовые источники в сфере информационных отношений защиты объектов и субъектов информационных технологий?

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	устный опрос 5 вопросов	15
Рейтинг-контроль 2	устный опрос 5 вопросов	15
Рейтинг-контроль 3	устный опрос 5 вопросов	15
Посещение занятий студентом		5
Дополнительные баллы (бонусы)		5
Выполнение семестрового плана самостоятельной работы	устный опрос 5 вопросов	5

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)

Тест для промежуточной аттестации.

1. Информацию по степени доступа разделяют на:

a) открытую и ограниченного доступа;

b) открытую;

c) закрытую;

d) тайную и ограниченную;

2. К информации ограниченного доступа относятся:

a) государственная тайна;

b) конфиденциальная информация;

c) персональные данные;

d) все ответы верны

3. Информационная безопасность являются переводом на русский язык английского термина:

a) informationsecurity;

b) informationsystem;

c) informationcurrency;

d) informationcrypto;

4. Защитой информации называют:

a) деятельность по предотвращению утечки любой информации;

b) деятельность по предотвращению утечки защищаемой информации;

c) деятельность по предотвращению утечки доступной информации;

d) все ответы верны;

5. Под утечкой понимают:

a) неконтролируемое распространение защищаемой информации путём её разглашения или несанкционированного доступа к ней;

b) неконтролируемое распространение скрытой информации путём её разглашения или несанкционированного доступа к ней;

c) неконтролируемое распространение конфиденциальной информации путём её разглашения или несанкционированного доступа к ней;

d) все верно;

6. Под непреднамеренным воздействием на защищаемую информацию понимают:

a) воздействие на неё из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;

b) воздействие на неё из-за ошибок пользователя, сбоя технических средств;

c) воздействие на неё из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;

d) все ответы верны;

7. Что не является характеристикой информации:

a) статичность;

b) тип доступа;

c) время отклика;

d) стоимость создания;

8. К наиболее распространённым правонарушениям в сети Internet не относится:

a) мошенническая деятельность;

b) перлюстрация частной переписки;

c) нарушение авторских и смежных прав;

d) нелегальное получение товаров и услуг;

9. Что не относится к задачам информационной безопасности:

a) целостность и секретность;

b) электронная подпись и датирование;

c) устойчивость связи и определение трафика;

d) неотказуемость и анонимность;

Блок 2 (уметь).

10.К методам обеспечения информационной безопасности не относятся:

a) корпоративные;

b) административные;

c) правовые;

d) технические;

11.Какие методы не относятся к обеспечению информационной безопасности:

a) принуждение и побуждение;

b) управление доступом и регламентация;

c) маскировка и препятствие;

d) скрытый доступ и копирование сообщений;

12.Методы защиты информации можно разбить:

a) на три большие группы;

b) на две большие группы;

c) на четыре большие группы;

d) на пять больших групп;

13.Методы, не имеющие математического обоснования стойкости, часто называют методами:

a) С чёрным ящиком;

b) С белым квадратом;

c) С желтым кругом;

d) Нет верного ответа;

14.Методы, функционирующие по принципу "черного ящика", называют

a) SecurityThroughObscurity;

b) System ThroughObscurity;

c) SecurityThrough;

d) SystemObscurity;

15.Метод физического преграждения пути злоумышленнику к информации:

a) управление доступом;

b) маскировка;

c) принуждение;

d) побуждение;

16.Метод защиты информации путем ее криптографического преобразования:

a) Принуждение;

b) Побуждение;

c) Маскировка;

d) управление доступом;

17.Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:

a) Уполномочивание;

b) Контроль доступа;

c) Сертификация;

d) Нет верного ответа;

18.Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:

a) уязвимость;

b) атака;

c) угроза;

d) нет верного ответа;

19. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:

a) атака;

b)угроза;

c)уязвимость;

d) статичность;

20. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:

a)статичность;

b)атака;

c)угроза;

d)изъян;

Блок 3 (владеть).

21. Какая угроза отказа служб устраняется административно-правовыми методами:

a) отказ пользователей;

b) отказ программного обеспечения;

c) нарушение работ систем связи;

d) разрушение и повреждение помещений

22. К каналам, предполагающим изменение элементов информационной структуры относится:

a) намеренное копирование файлов и носителей информации;

b) маскировка под других пользователей, путём похищение идентифицирующей их информации;

c) хищение носителей информации;

d) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.

23. Что относится к каналам, не требующим изменение элементов ИС

a) намеренное копирование файлов и носителей информации;

b) незаконное подключение специальной регистрирующей аппаратуры;

c) злоумышленное изменение программ;

d) злоумышленный вывод из строя средств защиты информации;

24. Какая направленность атак неверно сформулирована?

a) атаки на уровне операционной системы;

b) атаки на уровне системного администратора;

c) атаки на уровне сетевого программного обеспечения;

d) атаки на уровне систем управления базами данных.

25. К какому типу атак относится прослушивание передаваемых сообщений:

a) Пассивная атака;

b) Модификация потока данных;

c) Повторное использование;

d) Отказ в обслуживании.

26. Защита информации это:

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

27. Шифрование информации это:

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

28. Доступ к информации это:

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

1. Режим секретности – это:

a) совокупность определяемых органами власти и управления правил, которыми ограничивается допуск лиц к секретным материалам и работам, регламентируется порядок пользования секретных материалов, соответствующим образом регулируется поведение людей, имеющих отношение к секретам, и предусматриваются другие меры;

b) совокупность определяемых органами власти и управления правил, по которым лица имеют неограниченный допуск к секретным материалам и работам, регламентируется порядок пользования секретных материалов, соответствующим образом регулируется поведение людей, имеющих отношение к секретам, и предусматриваются другие меры;

c) нет верного ответа;

2. Назначение режима секретности заключается, в том, чтобы:

a) ограничить сферу обращения секретных данных только кругом лиц, связанных с производством секретных работ;

b) ограничить сферу обращения секретных данных всех лиц, имеющих доступ к какой-либо информации;

c) ограничить частично сферу обращения секретных данных только кругом лиц, связанных с производством секретных работ;

3. Государственная тайна — это:

a) информация, сведения, несанкционированный доступ к которым может причинить вред интересам страны, государства;

b) информация, сведения, несанкционированный доступ к которым может причинить вред интересам только жителям страны, но всего государства;

c) информация, сведения, несанкционированный доступ к которым может причинить вред интересам только руководству страны, государства;

4. Как называется закон, регулирующий деятельность государственной тайны на территории РФ?

a) «О коммерческой тайне»;

b) «О государственной тайне»;

c) «О служебной тайне»;

d) «О врачебной тайне»;

5. Какие сферы деятельности относятся к государственной тайне?

a) военная, внешнеполитическая, экономическая;

b) только военная и внешнеполитическая;

c) только военная и экономическая;

d) только военная, внешнеполитическая, экономическая;

6. Какие сферы деятельности относятся к государственной тайне?

a) разведывательная и оперативно-розыскная деятельность;

b)разведывательная и деятельность, связанная со стихийными бедствиями;

c) нет верного ответа;

7. Правовой основой режима секретности являются?

a)Конституция, законы Российской Федерации «О безопасности», «О государственной тайне»;

b) только Конституция и закон Российской Федерации «О безопасности»;

c) только Конституция и закон Российской Федерации «О государственной тайне».

Блок 2 (уметь).

8. Назовите признаки государственной тайны?

a) это очень важные сведения; их разглашение может причинить ущерб государственным интересам; перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом;

b) это очень важные сведения и их разглашение может причинить ущерб государственным интересам;

c) это очень важные сведения и перечень сведений, которые могут быть отнесены к государственной тайне, закрепляется федеральным законом.

9. Что такое засекречивание сведений?

a) предусмотренное Конституцией ограничение закрепленного ее ст. 25 права граждан «свободно искать, получать, производить и распространять информацию любым законным способом»;

b) предусмотренное Конституцией ограничение закрепленного ее ст. 26 права граждан «свободно искать, получать, производить и распространять информацию любым законным способом»;

c) предусмотренное Конституцией ограничение закрепленного ее ст. 27 права граждан «свободно искать, получать, производить и распространять информацию любым законным способом»;

10. Конфиденциальная информация может быть разделена на:

a) предметную и служебную;

b) служебную и закрытую;

c) предметную и открытую;

d) открытую и закрытую;

11. Целостность информации может быть разделена на:

a) статическую и динамическую;

b) статическую и служебную;

c) служебную и динамическую;

d) все верно;

12. Примером нарушения статической целостности не является:

a) ввод неверных данных;

b) несанкционированное изменение данных;

c) изменение программного модуля вирусом;

d) внесение дополнительных пакетов в сетевой трафик;

13. Примером нарушения динамической целостности не является:

a) нарушение атомарности транзакций;

b) внесение дополнительных пакетов в сетевой трафик;

c) несанкционированное изменение данных;

d) дублирование данных;

14. Угроза отказа служб может быть разбита на следующие типы:

a) отказ пользователей;

b) внутренний отказ информационной системы;

c) отказ поддерживающей инфраструктуры;

d) все ответы верны;

15. Назовите главные элементы режима секретности?

a) правила засекречивания; рассекречивания; защита государственной тайны;

b) правила засекречивания и защита государственной тайны;

c) правила засекречивания и рассекречивания;

d)защита государственной тайны и рассекречивания;

16. Не подлежат засекречиванию сведения о:

a) чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях;

b) сведения о военных разработках;

c) сведения о технических разработках;

Блок 3 (владеть).

17. Что такое аудит?

a) анализ накопленной информации, проводимый только оперативно;

b) анализ накопленной информации, проводимый оперативно или периодически;

c) оба ответы верны;

18. Выработку политики безопасности и ее содержание рассматривают на ___ горизонтальных уровнях детализации?

a) трех;

b) двух;

c) четырех;

19. Наибольшую угрозу ИС составляют:

a) Юзер;

b) Агент;

c) Хакер;

d) Крякер;

20. Внутриобъектовый режим это?

a) комплекс мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия;

b) Только 1 мероприятие, направленное на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия;

c) нет верного ответа;

21. Какая угроза отказа служб устраняется административно-правовыми методами:

a) отказ пользователей;

b) отказ программного обеспечения;

c) нарушение работ систем связи;

d) разрушение и повреждение помещений

22. Пропускной режим — это?

a) совокупность норм и правил, регламентирующих порядок входа на территорию предприятия и выхода лиц, въезда и выезда транспортных средств, вноса и выноса, ввоза и вывоза носителей сведений конфиденциального характера, а также мероприятий по реализации названных норм и правил с использованием имеющихся сил и средств;

b) совокупность норм и правил, регламентирующих порядок выхода из территории предприятия, выезда транспортных средств, вноса и выноса, ввоза и вывоза носителей сведений конфиденциального характера, а также мероприятий по реализации названных норм и правил с использованием имеющихся сил и средств

c) нет верного ответа

24. Что относится к каналам, не требующим изменение элементов ИС

a) намеренное копирование файлов и носителей информации;

b) незаконное подключение специальной регистрирующей аппаратуры;

c) злоумышленное изменение программ;

d)злоумышленный вывод из строя средств защиты информации;

24. Какая направленность атак неверно сформулирована?

a) атаки на уровне операционной системы;

b) атаки на уровне системного администратора;

c) атаки на уровне сетевого программного обеспечения;

d) атаки на уровне систем управления базами данных.

ОПК-6

Блок 1 (знать).

1. К какому типу атак относится прослушивание передаваемых сообщений:

a) Пассивная атака;

b) Модификация потока данных;

c) Повторное использование;

d) Отказ в обслуживании.

2. Для чего в системах обнаружения вторжений используется сенсорная подсистема?

a) для просмотра выявленных инцидентов

b) для настройки системы обнаружения вторжений

c) для выявления атак и подозрительных действий

d) для сбора событий, связанных с безопасностью защищаемой системы

e) для накопления первичных событий и результатов анализа

3. Вы получили по электронной почте письмо с вложением "От отдела IT". В тексте письма говорится, что ваш компьютер был заражен вирусом. Поэтому вам необходимо открыть вложение и следовать инструкциям, чтобы избавиться от вируса. Что необходимо сделать? (Выберите все подходящие варианты). Можно выбрать 1 или несколько вариантов ответа.

a) связаться с IT-отделом для уточнения информации о полученном письме.

b) откройте вложение, чтобы увидеть его содержание.

c) удалить сообщение из неизвестного источника.

d) следуйте инструкциям, чтобы удалить вирус.

e) написать письмо отправителю с просьбой удалить из списка рассылки.

4. Какая проблема безопасности возникает в операционной системе в отсутствии механизма удаления файлов при смене пользователя на одном компьютере (один пользователь вышел из системы, а второй - зашел)?

a) утечки данных по скрытым каналам

b) несанкционированное получение привилегий первого пользователя

c) никаких проблем с безопасностью системы и в частности данных не возникнет

d) отказ в обслуживании

e) раскрытие остаточной информации вторым пользователем

5. Для защиты информации, содержащейся в базе данных, требуется следующее действие со стороны физической защиты:

a) предупреждение несанкционированного доступа персонала

b) эвакуация

c) контроль модернизируемого оборудования

d) защита от стихийных бедствий

e) ничего из перечисленного

6. Какой гриф секретности необходимо установить (в соответствии с законодательством РФ) для сведений о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях?

a) секретно

b) особой важности

c) совершенно секретно

d) никакой из перечисленных. Данные сведения, не подлежат к засекречиванию

e) для служебного пользования

7. На каком уровне сетевой модели OSI работает сетевой мост?

a) канальный

b) сеансовый

c) физический

d) транспортный

e) сетевой

8. На компьютере хранится документ GovSecret.doc, к которому имеет доступ только определенный круг лиц (отдел статистики). Сотрудник отдела аудита во время общения в обеденное время с сотрудником отдела статистики сел за его рабочее место и прочитал содержимое документа GovSecret.doc. Определите нарушаемое свойство защищенной информации.

a) конфиденциальность

b) узнаваемость

c) массовость

d) целостность

e) доступность

Блок 2 (уметь).

9. Принятие каких мер из перечисленных не представляет собой защиту информации согласно законодательству РФ? Можно выбрать 1 или несколько вариантов ответа.

a) организационные

b) экономические

c) технические

d) физические

e) правовые

10. Какой международный стандарт оценки степени защищенности информационных систем позволяет признавать произведенную сертификацию продукта в другой стране по данному стандарту?

a) BS 31100:2008

b) ISO/IEC 27005

c) ISO/IEC 27001

d) Оранжевая книга ("Orange Book")

e) Общие критерии ("Common Criteria", ISO/IEC 15408)

11. Как называется получение информации с более высоким уровнем чувствительности (например, секретная информация) путем комбинирования информации с более низким уровнем чувствительности (например, открытая информация)?

a) декомбинация

b) инференция

c) валидация

d) агрегация

e) утечка информации

12. Чем отличаются пассивные системы обнаружения вторжений (СОВ) от активных?

a) Пассивные СОВ ограничивают поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и, в отличии от активных, не отслеживают вторжения, происходящие внутри сети.

b) Для работы пассивных СОВ (в отличии от активных) необходим дополнительный модуль, который будет выполнять фильтрацию трафика.

c) В архитектуру пассивных СОВ не входит сенсорная подсистема, а активные СОВ - содержат сенсоры.

d) Пассивные СОВ (в отличии от активных) работают только на хостах (узлах сети).

e)Пассивные СОВ информацию о нарушении безопасности записывают в лог и сигнализирует о факте нарушения.

f) Активные СОВ ведут ответные действия на нарушение.

13. Какую ответственность в соответствии с законодательством Российской Федерации не влекут за собой правонарушения в сфере информации, информационных технологий и защиты информации (согласно законодательству РФ)?

a) нарушения влекут за собой все перечисленные виды ответственности

b) гражданско-правовая

c) уголовная

d) дисциплинарная

e) административная

Блок 3 (владеть).

14. Какой тип системы обнаружения вторжений необходимо использовать для проведения анализа деятельности системы, используя событие или множество событий на соответствие заранее определенному образцу, который описывает известную атаку?

a) Host-based (HIDS)

b) Network-based (NIDS)

c) Policy-based

d) Signature-based

e) Anomaly-based

15. У какого протокола основной функцией является передача директорий и файлов между двумя компьютерами?

a) HTTP

b) TFTP

c) Telnet

d) FTP

e) SMTP

16. Что означает понятие "защита информации"? (выберите две формулировки)

a) последовательность действий для обеспечения защищенности информационной среды

b) управление системой защиты информации

c) состояние защищенности информационной среды

d) процесс, направленный на достижение информационной безопасности

e) деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию среды

ОПК-10:

Блок 1 (знать).

1. Риск – это:

a) функция вероятности реализации определенной угрозы (использующей некоторые уязвимости) и величины возможного ущерба;

b) функция вероятности реализации определенной угрозы и величины возможного ущерба;

c) нет верного ответа.

2. Анализ рисков - это:

a) процесс идентификации информационных рисков, определение вероятности их осуществления и потенциального воздействия, а также имеющихся контрмер, уменьшающих это воздействие (угроз и уязвимостей);

b) процесс аутентификации информационных рисков, определение вероятности их осуществления и потенциального воздействия, а также имеющихся контрмер, уменьшающих это воздействие (угроз и уязвимостей);

c) нет верного ответа;

3. Управление рисками – это:

a) процесс, включающий анализ рисков, выбор, реализация и оценка эффективных и экономичных контрмер, проверка, что риски установлены на приемлемом уровне;

b) процесс, включающий только анализ рисков и риски, установленные на приемлемом уровне;

c) процесс, включающий только реализацию и оценку эффективных и экономичных контрмер.

4. Целями анализа рисков являются:

a) определение цели управления ИБ и оценивания основных критичных областей, отрицательно влияющих на ключевые бизнес-процессы компании;

b) выработку малоэффективных и обоснованных решений для контроля или минимизации выявленных рисков;

c) нет верного ответа;

5. Этапом процесса управления рисками не является?

a) Идентификация активов;

b) Оценка рисков;

c) Выбор защитных мер;

d) Аутентификация активов.

6. Этапом процесса управления рисками не является?

a) Идентификация активов;

b) Оценка рисков;

c) Выбор защитных мер;

d) Оценка нормативного риска.

7. Постановка задачи оценки рисков позволяет задать?

a) требования к методике оценки информационных рисков организации;

b) урегулирование информационных рисков организации;

c) нет верного ответа;

Блок 2 (уметь).

8. Центральный элемент системы защиты, который идентифицирует субъекты, объекты и параметры запрашиваемого доступа субъектов к объектам:

a) сканер безопасности;

b) монитор безопасности;

c) модем безопасности;

d) шина безопасности;

9. К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые:

a) руководством организации

b) Персоналом организации

c) Пользователями

d) Нет верного ответа

10. Из скольких уровней детализации состоит политика безопасности ИС:

a) Трех

b) Четырех

c) Двух

d) Пяти

11. Политика безопасности верхнего уровня, затрагивающая все организацию в целом, включает в себя:

a) решение сформировать или изменить комплексную программу обеспечения информационной безопасности;

b) формулирование целей организации в области информационной безопасности, определение общих направлений в достижении данных целей;

c) обеспечение нормативной базы для соблюдения законов и правил;

d) все ответы верны;

12. Назовите метод оценки рисков?

a) экспертных оценок;

b) аналитических оценок;

c) регулируемых оценок;

d) нет верного ответа.

13. Какая из методик оценки рисков является лишней?

a) NIST;

b) FAIR;

c) BSI;

d) BSB.

14. Какая из методик оценки рисков является лишней?

a) OCTAVE;

b) IRAM;

c) ISO 27005;

d) ISO 27000.

Блок 3 (владеть).

15. При передаче документов, содержащих коммерческую тайну, в органы государственной власти и органы местного самоуправления гриф «Коммерческая тайна» или «Конфиденциально» проставляется:

a) в обязательном порядке;

b) в желательном порядке

c) в не обязательном порядке

16. Из скольких уровней состоит правовое обеспечение информационной безопасности:

a) двух уровней;

b) трех уровней;

c) четырех уровней;

d) пяти уровней;

17. Что из перечисленного не входит в первый уровень правового обеспечения информационной безопасности:

a) Конституция РФ (ст. 23, право на тайну переписки);

b) Гражданский кодекс РФ (ст. 139, возмещение убытков от утечек);

c) Федеральный закон "О государственной тайне";

d) постановления Правительства РФ;

18. Что из перечисленного не входит во второй уровень правового обеспечения информационной безопасности:

a) указы Президента РФ;

b) постановления Правительства РФ;

c) Уголовный кодекс РФ (ст. 272-274, неправомерный доступ, распространение вирусов, нарушение правил эксплуатации);

d) постановления пленумов Верховного Суда РФ;

19. Структурные элементы национальной безопасности:

a) Политическая;

b) Экономическая;

c) Военная;

d) все ответы верны;

20. Когда был принят Федеральный закон «Об участии в международном информационном обмене»?

a) 5 июня 1992 г.

b) 5 июня 1994 г.

c) 5 июня 1995 г.

d) 5 июня 1996 г.

21. Систему национальной безопасности образует:

a) органы законодательной, исполнительной и судебной властей;

b) государственные, общественные и иные организации и объединения;

c) граждане, принимающие участие в обеспечении безопасности в соответствии с законом;

d) все ответы верны;

ОПК-10:

Блок 1 (знать).

1. В каком году утверждена Доктрина информационной безопасности Российской Федерации:

a) 1998;

b) 2000;

c) 2002;

d) 2004;

2. Что не относится к основным принципам обеспечения национальной безопасности:

a) законность;

b) соблюдение баланса жизненно важных интересов личности, общества и государства;

c) взаимная ответственность личности, общества и государства по обеспечению безопасности;

d) системность;

3. К правовым методам обеспечения информационной безопасности относят:

a) разработка современных методов и средств защиты информации;

b) определение ответственности физических и юридических лиц;

c) усиление контроля за развитием информационного рынка России;

d) повышение степени защищенности законных интересов граждан;

4. Когда был принят Федеральный закон "Об информации, информатизации и защите информации:

a) 2004;

b) 2006;

c) 2008;

d) 2010;

5. Как называется вид атаки, при которой производятся незаконные изменения сайта (часто главной страницы на что-то другое)?

a) Refactoring

b) Compiling

c) Defacement

d) Decomposition

e) Injecting

6. На каких двух проблемах не основана несимметричная криптография? Можно выбрать 1 или несколько вариантов ответа.

a) проблема возведения больших чисел в степень

b) проблема разложения большого числа на простые множители

c) проблема нахождения квадратичного вычета

d) проблема факторизации

f) проблема дискретного логарифмирования

7. Дайте определение типу вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия.

a) троян

b) вирус
c) эксплоит
d) червь
e) логическая бомба

Блок 3 (владеть).

8. Что из перечисленного происходит при использовании RAID-массивов?
a) повышается надёжность хранения данных
b) обеспечивается более высокий уровень защиты от вирусов
c) ничего из перечисленного
d) увеличивается максимальная пропускная способность сети
e) производится полное шифрование данных

9. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?
a) информация про личность
b) государственная тайна
c) конфиденциальная информация
d) информация с ограниченным доступом
e) персональные данные

10. Как называется процент субъектов неверно разрешенных в системе (иначе: ситуация, когда нарушители классифицируются как авторизованные пользователи)?
a) False User Access Rate (FUAR)
b) True Acceptance Rate (TAR) или ошибка 3 рода
c) False Acceptance Rate (FAR) или ошибка 2 рода
d) False Rejection Rate (FRR) или ошибка 1 рода
e) Crossover Error Rate (CER)

11. Что из перечисленного не используется в биометрической аутентификации? Можно выбрать 1 или несколько вариантов ответа.
a) пластиковая карта с магнитной полосой
b) клавиатурный почерк
c) PIN-код
d) рисунок папиллярного узора
e) радужная оболочка глаза

12. Какое устройство в сети обязано собирать фрагментированные IP-пакеты?
a) мост
b) конечный получатель пакета
c) повторитель
d) коммутатор 2 уровня
e) точка доступа

13. Кто из следующих лиц несет основную ответственность за определение уровня классификации информации?
a) пользователь
b) администратор
c) менеджер по безопасности
d) владелец
e) аудитор

14. Какой механизм необходимо использовать для трансляции локальной сети с диапазоном адресов, например, 172.11.10.0/24 в глобальную сеть через один внешний IP-адрес (адрес маршрутизатора, выполняющего трансляцию)?
a) TCP/IP
b) Proxy
c) DNS
d) DMZ
e) NAT

Блок 2 (уметь).

1. Определите, принятие каких мер не представляет собой защита информации? Можно выбрать 1 или несколько вариантов ответа.

a) тактические
b) организационные
c) правовые
d) технические
e) экономические

2. Что такое "HoneyPot" в информационной безопасности?

a) сетевой протокол
b) симметричный криптографический алгоритм
c) антивирусное программное обеспечение
d) тип сетевой атаки на прокси-сервера
e) средство безопасности, используемое для поимки хакеров и анализа их методов

3. В каком виде хранятся данные о пользователях UNIX?

a) файл с расширением *.usr
b) нет правильного ответа
c) текстовый файл
d) бинарный файл
e) исполняемый файл

4. На каком устройстве обычно используют технологию VLAN с целью разделения сети на сегменты?

a) повторитель
b) коммутатор
c) точка доступа
d) брандмауер
e) маршрутизатор

5. Почему оптоволоконные коммуникационные технологии имеют значительное преимущество (в значении безопасности) перед другими технологиями передачи данных?

a) высокая скорость передачи данных
b) возможность исправления ошибок в передаваемых данных
c) более дешевые в применении
d) мультиплексирование препятствует анализу трафика
e) перехват трафика является более сложным

6. Что является иерархическим (логическим) адресом компьютера в сети?

a) маска подсети
b) MAC-адрес
c) символьное имя компьютера
d) нет верного ответа
e) IP-адрес

7. Каким термином называется способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ?

a) линейное шифрование
b) простое шифрование
c)"One-key" шифрование
d) симметричное шифрование
e) одноуровневое шифрование

Методические материалы, характеризующие процедуры оценивания

На основе перечня тестовых вопросов программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов: восемь вопросов из блока 1, четыре вопроса из блока 2 и три вопроса

из блока 3. Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Каждый ответ из блока 1 оценивается в 2 балла, из блока 2 - в 3 балла, из блока 3 - в 4 балла. Результатом тестирования является сумма баллов, которая складывается с индивидуальным семестровым рейтингом студента и определяет получение зачета.

0 - 50 балла – «не зачтено»;

51 – 100 баллов – «зачтено».

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:

1. В каком году утверждена Доктрина информационной безопасности Российской Федерации:

a) 1998;

b) 2000;

c) 2002;

d) 2004;

2. Что не относится к основным принципам обеспечения национальной безопасности:

a) законность;

b) соблюдение баланса жизненно важных интересов личности, общества и государства;

c) взаимная ответственность личности, общества и государства по обеспечению безопасности;

d) системность;

3. К правовым методам обеспечения информационной безопасности относят:

a) разработка современных методов и средств защиты информации;

b) определение ответственности физических и юридических лиц;

c) усиление контроля за развитием информационного рынка России;

d) повышение степени защищенности законных интересов граждан;

4. Когда был принят Федеральный закон "Об информации, информатизации и защите информации:

a) 2004;

b) 2006;

c) 2008;

d) 2010;

5. Как называется вид атаки, при которой производятся незаконные изменения сайта (часто главной страницы на что-то другое)?

a) Refactoring

b) Compiling

c) Defacement

d) Decomposition

e) Injecting

6. На каких двух проблемах не основана несимметричная криптография? Можно выбрать 1 или несколько вариантов ответа.

a) проблема возведения больших чисел в степень

b) проблема разложения большого числа на простые множители

c) проблема нахождения квадратичного вычета

d) проблема факторизации

f) проблема дискретного логарифмирования

7. Дайте определение типу вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия.

a) троян

b) вирус

c) эксплоит

d) червь

e) логическая бомба

Блок 3 (владеть).

8. Что из перечисленного происходит при использовании RAID-массивов?

a) повышается надёжность хранения данных

b) обеспечивается более высокий уровень защиты от вирусов

c) ничего из перечисленного

d) увеличивается максимальная пропускная способность сети

e) производится полное шифрование данных

9. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?

a) информация про личность

b) государственная тайна

c) конфиденциальная информация

d) информация с ограниченным доступом

e) персональные данные

10. Как называется процент субъектов неверно разрешенных в системе (иначе: ситуация, когда нарушители классифицируются как авторизованные пользователи)?

a) False User Access Rate (FUAR)

b) True Acceptance Rate (TAR) или ошибка 3 рода

c) False Acceptance Rate (FAR) или ошибка 2 рода

d) False Rejection Rate (FRR) или ошибка 1 рода

e) Crossover Error Rate (CER)

11. Что из перечисленного не используется в биометрической аутентификации? Можно выбрать 1 или несколько вариантов ответа.

a) пластиковая карта с магнитной полосой

b) клавиатурный почерк

c) PIN-код

d) рисунок папиллярного узора

e) радужная оболочка глаза

12. Какое устройство в сети обязано собирать фрагментированные IP-пакеты?

a) мост

b) конечный получатель пакета

c) повторитель

d) коммутатор 2 уровня

e) точка доступа

13. Кто из следующих лиц несет основную ответственность за определение уровня классификации информации?

a) пользователь

b) администратор

c) менеджер по безопасности

d) владелец

e) аудитор

14. Какой механизм необходимо использовать для трансляции локальной сети с диапазоном адресов, например, 172.11.10.0/24 в глобальную сеть через один внешний IP-адрес (адрес маршрутизатора, выполняющего трансляцию)?

a) TCP/IP

b) Proxy

c) DNS

d) DMZ

e) NAT

1. Определите, принятие каких мер не представляет собой защита информации? Можно выбрать 1 или несколько вариантов ответа.

a) тактические

b) организационные

c) правовые

d) технические

e) экономические

2. Что такое "HoneyPot" в информационной безопасности?

a) сетевой протокол

b) симметричный криптографический алгоритм

c) антивирусное программное обеспечение

d) тип сетевой атаки на прокси-сервера

e) средство безопасности, используемое для поимки хакеров и анализа их методов

3. В каком виде хранятся данные о пользователях UNIX?

a) файл с расширением *.usr

b) нет правильного ответа

c) текстовый файл

d) бинарный файл

e) исполняемый файл

4. На каком устройстве обычно используют технологию VLAN с целью разделения сети на сегменты?

a) повторитель

b) коммутатор

c) точка доступа

d) брандмауер

e) маршрутизатор

5. Почему оптоволоконные коммуникационные технологии имеют значительное преимущество (в значении безопасности) перед другими технологиями передачи данных?

a) высокая скорость передачи данных

b) возможность исправления ошибок в передаваемых данных

c) более дешевые в применении

d) мультиплексирование препятствует анализу трафика

e) перехват трафика является более сложным

6. Что является иерархическим (логическим) адресом компьютера в сети?

a) маска подсети

b) MAC-адрес

c) символьное имя компьютера

d) нет верного ответа

e) IP-адрес

7. Каким термином называется способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ?

a) линейное шифрование

b) простое шифрование

c)"One-key" шифрование

d) симметричное шифрование

e) одноуровневое шифрование

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=2864&cat=31088%2C92832

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