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
16.06.2020

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

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	**216 / 6**	**32**		**64**	**3,2**	**0,25**	**99,45**	**116,55**	**Зач. с оц.**
Итого	**216 / 6**	**32**		**64**	**3,2**	**0,25**	**99,45**	**116,55**	

Муром, 2021 г.

1. Цель освоения дисциплины

Цель дисциплины: ознакомление студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач.

Задачами дисциплины являются:

- изучение основных угроз безопасности информации в автоматизированных системах и освоение методов защиты от данных угроз;
- изучение методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
- изучение основных мер по защите информации и программных продуктов от не-санкционированного доступа, модификации и изучения в автоматизированных системах;
- изучение современных технологий защищенных сетей передачи данных в автоматизированных системах.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Программно-аппаратные средства защиты информации» базируется на знаниях, полученных в рамках изучения следующих дисциплин: "Физика", "Сети и системы передачи информации", "Криптографические методы защиты информации" и "Организационное и правовое обеспечение информационной безопасности". Дисциплина «Программно-аппаратные средства защиты информации» является теоретическим и методологическим основанием для дисциплин, входящих в ОПОП бакалавра по направлению 10.03.01 «Информационная безопасность», использующих программно-аппаратные решения в области выявления угроз и обеспечения информационной безопасности.

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-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях;	ОПК-1.2.2 Администрирует основные программно-аппаратные средства защиты информации в компьютерных системах и сетях	знать виды, назначения и возможности средств защиты информации в компьютерных системах и сетях (ОПК-1.2.2) уметь администрировать средства защиты информации в компьютерных системах и сетях (ОПК-1.2.2) владеть навыками администрирования средств защиты информации в компьютерных системах и сетях (ОПК-1.2.2)	вопросы к устному опросу

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 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	Основные понятия программно-аппаратной защиты информации	6	6		64					10	устный опрос
2	Идентификация пользователей КС-субъектов доступа к данным	6	4								устный опрос
3	Средства и методы ограничения доступа к файлам	6	2							10	устный опрос
4	Аппаратно-программные средства криптографической защиты информации	6	4							10	устный опрос
5	Методы и средства ограничения доступа к компонентам ЭВМ	6	2							16	устный опрос
6	Защита программ от несанкционированного копирования	6	4							10	устный опрос
7	Криптографические средства защиты	6	4							40	устный опрос
8	Аппаратные средства защиты и контроля эффективности мер	6	6							20,55	устный опрос

	защиты										
Всего за семестр		216	32		64			3,2	0,25	116,55	Зач. с оц.
Итого		216	32		64			3,2	0,25	116,55	

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 6

Раздел 1. Основные понятия программно-аппаратной защиты информации

Лекция 1.

Предмет и задачи программно-аппаратной защиты информации (2 часа).

Лекция 2.

Основные понятия. Уязвимость компьютерных систем (2 часа).

Лекция 3.

Политика безопасности в компьютерных системах. Оценка защищенности (2 часа).

Раздел 2. Идентификация пользователей КС-субъектов доступа к данным

Лекция 4.

Понятие идентификации пользователя (2 часа).

Лекция 5.

Основные подходы к защите данных от НСД (2 часа).

Раздел 3. Средства и методы ограничения доступа к файлам

Лекция 6.

Организация доступа к файлам. Доступ к данным со стороны процесса (2 часа).

Раздел 4. Аппаратно-программные средства криптографической защиты информации

Лекция 7.

Построение программно-аппаратных комплексов шифрования (2 часа).

Лекция 8.

Проблема защиты отчуждаемых компонентов ПЭВМ (2 часа).

Раздел 5. Методы и средства ограничения доступа к компонентам ЭВМ

Лекция 9.

Надежность средств защиты компонент (2 часа).

Раздел 6. Защита программ от несанкционированного копирования

Лекция 10.

Несанкционированное копирование программ (2 часа).

Лекция 11.

Защита программ от исследования (2 часа).

Раздел 7. Криптографические средства защиты

Лекция 12.

Подходы к задаче защиты от копирования. Пароли и ключи (2 часа).

Лекция 13.

Управление криптографическими ключами (2 часа).

Раздел 8. Аппаратные средства защиты и контроля эффективности мер защиты

Лекция 14.

Защита информации в IP-сетях (2 часа).

Лекция 15.

Скрытие и защита информации от утечки по техническим каналам (2 часа).

Лекция 16.

Контроль эффективности мер защиты информации. Аттестация объектов информатизации (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 6

Раздел 1. Основные понятия программно-аппаратной защиты информации

Лабораторная 1.

Установка и первоначальная настройка Windows Server 2016 и Windows 10 (4 часа).

Лабораторная 2.

Установка ролей «Доменные службы Active Directory» и «Сервер DNS» (4 часа).

Лабораторная 3.

Установка роли «Сервер DHCP» (4 часа).

Лабораторная 4.

Роль «Файловые службы и службы хранилища». Пространства имен DFS» (4 часа).

Лабораторная 5.

Роль «Windows Server Update Services» (4 часа).

Лабораторная 6.

Диспетчер ресурсов файлового сервера (4 часа).

Лабораторная 7.

Реализация безопасности Windows Server 2016 (4 часа).

Лабораторная 8.

Методы организации отказоустойчивых каналов связи. Технология STP (4 часа).

Лабораторная 9.

Методы организации отказоустойчивых каналов связи. Технология STP (4 часа).

Лабораторная 10.

Статическое агрегирование каналов EtherChannel (4 часа).

Лабораторная 11.

Динамическое агрегирование каналов EtherChannel (4 часа).

Лабораторная 12.

Фильтрация трафика с использованием стандартных Access Control List в Cisco IOS (4 часа).

Лабораторная 13.

Фильтрация трафика с использованием расширенных Access Control List в Cisco IOS (4 часа).

Лабораторная 14.

Технология NAT (4 часа).

Лабораторная 15.

Сетевая разведка (4 часа).

Лабораторная 16.

Аудит информационной безопасности (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Идентификация пользователей КС – объектов доступа к данным. Часть 1.
2. Средства и методы ограничения доступа к файлам.
3. Программно-аппаратные средства шифрования.
4. Методы и средства ограничения доступа к компонентам ЭВМ.
5. Защита программ от несанкционированного копирования.
6. Хранение ключевой информации.
7. Защита программ от изучения.
8. Организация хранения ключей (с примерами реализации).
9. Типовые решения в организации ключевых систем.
10. Изучение и обратное проектирование ПО.
11. Компоненты ПЭВМ.

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 или симуляционный подход. Шаги решения задач студентам демонстрируются при помощи мультимедийной техники. В дальнейшем студенты самостоятельно решают аналогичные задания.

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. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/124242.html. — Режим доступа: для авторизир. пользователей - https://www.iprbookshop.ru/124242.html

2. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/120489.html. — Режим доступа: для авторизир. пользователей - https://www.iprbookshop.ru/120489.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Формализация подхода к определению актуальности угроз информационной безопасности : монография / О. М. Голембиовская, М. Ю. Рытов, М. М. Голембиовский [и др.]. — Саратов : Вузовское образование, 2022. — 147 с. — ISBN 978-5-4487-0840-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/121143.html. — Режим доступа: для авторизир. пользователей - https://www.iprbookshop.ru/121143.html

2. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: . — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/108227 - https://www.iprbookshop.ru/108227.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)

Google Chrome (Лицензионное соглашение Google)

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))

Oracle VirtualBox (GNU GPL)

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

Cisco Packet Tracer (EULA)

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 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.

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.

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 Астафьев А.В.*_____

Программа рассмотрена и одобрена на заседании кафедры *ФПМ*

протокол № 17 от 22.05.2020 года.
Заведующий кафедрой *ФПМ* _____*Орлов А.А.*
(Подпись)

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

протокол № 10 от 10.06.2020 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине
Программно-аппаратные средства защиты информации

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

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

1. Виды информации в компьютерных системах.
2. Информационные потоки в КС.
3. Понятие исполняемого модуля.
4. Уязвимость компьютерных систем.
5. Понятие доступа, субъект и объект доступа.
6. Понятие несанкционированного доступа (НСД), классы и виды НСД.
7. Несанкционированное копирование программ как особый вид НСД.
8. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
9. Политика безопасности в компьютерных системах.
10. Оценка защищенности.
11. Способы защиты конфиденциальности, целостности и доступности в КС.
12. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.
13. Понятие идентификации пользователя. Задача идентификации пользователя.
14. Понятие протокола идентификации.
15. Локальная и удаленная идентификация.
16. Идентифицирующая информация (понятие, способы хранения, связь с ключевыми системами).

1. Основные подходы к защите данных от НСД.
2. Шифрование.
3. Контроль доступа.
4. Разграничение доступа.
5. Файл как объект доступа.
6. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
7. Организация доступа к файлам.
8. Иерархический доступ к файлам.
9. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
10. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
11. Способы фиксации факторов доступа.

Блок 3 (Владеть)

1. Журналы доступа и критерии их информативности.
2. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
3. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).
4. Понятие и примеры скрытого доступа.
5. Надежность систем ограничения доступа.
6. Защита массивов информации от изменения (имитозащита).
7. Криптографическая постановка защиты от изменения данных.
8. Подходы к решению задачи защиты данных от изменения.
9. Защита от разрушающих программных воздействий.
10. Вирусы как особый класс разрушающих программных воздействий.
11. Необходимые и достаточные условия недопущения разрушающего воздействия.

12. Понятие изолированной программной среды.
13. Построение программно-аппаратных комплексов шифрования.

Темы для устного опроса (рейтинг-контроль №2):
1. Аппаратные и программно-аппаратные средства криптозащиты данных.
2. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.
3. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
4. Необходимые и достаточные функции аппаратного средства криптозащиты.
5. Проектирование модулей криптопреобразований на основе сигнальных процессов.
6. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
7. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей.
8. Механизмы расширения BIOS.
9. Преимущества и недостатки программных и аппаратных средств.
10. Способы защиты информации на съемных дисках.
11. Организация прозрачного режима шифрования.
12. Надежность средств защиты компонент.
13. Понятие временной и гарантированной надежности.

1. Несанкционированное копирование программ.
2. Юридические аспекты несанкционированного копирования программ.
3. Несанкционированное копирование программ как тип НСД.
4. Защита программ от несанкционированного копирования (общее понятие защиты от копирования).
5. Разновидности задач защиты от копирования.
6. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.
7. Привязка программ к гибким машинным дискам (ГМД).
8. Структура данных на ГМД.
9. Управление контроллером ГМД.
10. Способы создания некопируемых меток.
11. Точное измерение характеристик форматирования дорожки.
12. Технология «слабых битов».
13. Физические метки и технология работы с ними.

Блок 3 (Владеть)
1. Привязка программ к жестким магнитным дискам (ЖМД).
2. Особенности привязки к ЖМД.
3. Виды меток на ЖМД.
4. Привязка к прочим компонентам штатного оборудования ПЭВМ.
5. Привязка к портовым ключам.
6. Использование дополнительных плат расширения.
7. Методы «водяных знаков» и методы «отпечатков пальцев».
8. Хранение ключей информации.
9. Секретная информация, используемая для контроля доступа: ключи и пароли.
10. Классификация средств хранения ключей и идентифицирующей информации.
11. Организация хранения ключей (с примерами реализации).
12. Магнитные диски прямого доступа.

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

1. Магнитные и интеллектуальные карты.
2. Средство TouchMemory.
3. Открытое распределение ключей.
4. Метод управляемых векторов.
5. Понятие изучения и обратного проектирования ПО.
6. Цели и задачи изучения работы ПО.
7. Способы изучения ПО: статистическое и динамическое изучение.
8. Роль программной и аппаратной среды.
9. Временная надежность (невозможность обеспечения гарантированной надежности).

Блок 2 (Уметь)
1. Задачи защиты от изучения и способы их решения.
2. Защита от отладки: итеративный программный замок.
3. Защита от отладки: принцип ловушек и избыточного кода.
4. Защита от дизассемблирования.
5. Принцип внешней загрузки файлов.
6. Динамическая модификация программы.
7. Защита от трассировки по прерываниям.
8. Способы ассоциирования защиты и программного обеспечения.
9. Оценка надежности защиты от отладки.

1. Программно-аппаратные средства реализации блочных шифров с секретным ключом в различных режимах функционирования: базовые режимы простой замены, электронной кодовой книги, режимы гаммирования, сцепления блоков.
2. Ключи на базе перепрограммируемой постоянной памяти.
3. Ключи на базе заказных чипов.
4. Примеры реализации ключей (Aktivator, HASP, Alladin и другие).
5. Ключи на базе микропроцессоров.
6. Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности.
7. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
8. Программно-аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	устный опрос 5 вопросов	20
Рейтинг-контроль 2	устный опрос 5 вопросов	20
Рейтинг-контроль 3	устный опрос 5 вопросов	20
Посещение занятий студентом		10
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)

Блок 1 (Знать):

1) Аппаратно-программные средства криптографической защиты информации выполняют функции:

1. Аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.

2. Организовывают реализацию политики безопасности информации на этапе эксплуатации КС.

3. Проверяют на отсутствие закладок приборов, устройств.

2) Надежность защиты информации в компьютерной системе определяется:

1. Конкретным перечнем и свойствами функций КС;

2. Используемыми в функциях КС методами;

3. Варианты a) и b)

3) Использование аппаратных средств снимает проблему:

1. Обеспечения целостности системы.

2. Разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

3. Использования строго определенного множества программ.

4) Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются

1. Аппаратно

2. Программно

3. Аппаратно и программно

5) К частично контролируемым компьютерным системам можно отнести современные КС, использующие

1. ОС Windows 95/98, Windows NT, различные версии UNIX

2. Windows NT, Windows XP

3. Различные версии UNIX

6) Безопасность в частично контролируемым компьютерных системамах может быть обеспечена

1. Изоляцией от злоумышленника ненадежной компьютерной среды, отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.

2. Схемой идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

3. Внешней аутентификацией объекта, не принадлежащего системе;

7) Платы серии КРИПТОН, обеспечивают защиту:

1. Ключей шифрования и электронной цифровой подписи (ЭЦП), так и неизменность их алгоритмов.

2. Аппаратно-программных механизмов

3. Реализации механизма виртуальной памяти с разделением адресных пространств;

8) К основным компонентам сети относятся:

1. Центры коммутации пакетов, маршрутизаторы, шлюзы и сетевые экраны;

2. Субъекты доступа

3. Платы серии КРИПТОН

9) В качестве ключевых носителей устройств криптографической защиты данных серии КРИПТОН используются:

1. Дискеты, смарт-карты и Touch-Memory.

2. Смарт-карты, Touch-Memory

3. Дискеты, смарт-карты

10) Средства серии КРИПТОН независимо от операционной среды обеспечивают:

1. Защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.

2. Криптомаршрутизацию

3. Функции шифрования и электронной цифровой подписи.

11) В системе Secret Disk используется:

1. Смешанная программно-аппаратная схема защиты с возможностью выбора

2. Реализация механизма виртуальной памяти с разделением адресных пространств;

3. Механизм RUN-файлов позволяет в процессе работы запускать любые программы с предварительной проверкой их целостности.

12) В чем заключается особенность системы Secret Disk:

1. Для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор.

2. Для доступа к защищенной информации необходим только вводимый пользователем пароль.

3. Для доступа к защищенной информации необходим только электронный идентификатор.

13) Мастер-ключ в Устройствах криптографической защиты данных серии КРИПТОН загружается:

1. До загрузки операционной системы

2. После загрузки операционной системы

3. Вообще не загружается

14) Криптографических функций в устройствах криптографической защиты данных серии КРИПТОН выполняются:

1. Внутри платы

2. В операционной системе

3. В блоке загрузки операционной системы

15) Абонентские места, персональные компьютеры или терминалы клиента являются основными компонентами сети?

1. Да

2. Нет

3. Не знаю

1) Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации – это:

1. Угроза безопасности информации

2. Атака

3. Идентификация

4. Санкционированный доступ к информации

2) Защита документов (традиционные документы на бумажном носителе) от подделки – типичная задача защиты информации, решаемая в настоящее время методом:

1. Защиты носителя

2. Криптографической защиты

3. Внедрения идеологии

4. Массового гипноза

3) В структуру канала утечки информации входит:

1. Источник сигнала

2. Среда распространения

3. Приемник сигнала

4. Высокочастотный генератор

4) К физической инфраструктуре относятся:

1. Инженерные коммуникации

2. Средства связи

3. Оргтехника

4. Программы и данные

5) Антропогенные источники угроз безопасности информации делятся на:

1. Внутренние и внешние

2. Техногенные и стихийные

3. Случайные и преднамеренные

6) Специальный информационный объект (обычно представленный в виде набора букв, цифр и символов), который реализуют доступ к шифрованию/дешифрованию –

1. Криптографический ключ

2. Открытый ключ

3. Открытый канал

4. Закрытый ключ

7) Согласно Конституции РФ:

1. каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

2. каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом.

3. каждый имеет право на достоверную информацию о состоянии окружающей среды.

4. каждый имеет право на создание, использование и распространение вредоносных программ для ЭВМ

8) Способ преобразования открытой информации в закрытую и обратно –

1. Шифрование

2. Дешифрование

3. Криптоанализ

4. Взлом

9) Принято считать, что телевидение оказывает на ребенка влияние:

1. физическое

2. психологическое

3. инфекционное

10) «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» является:

1. Статьей Конституции РФ

2. Статьей уголовного кодекса РФ

3. Статьей гражданского кодекса РФ

4. Нормативно-правовым актом Правительства Российской Федерации

11) К внутренним антропогенным источникам угроз безопасности информации относятся:

1. Основной персонал (пользователи, программисты, бухгалтера)

2. Вспомогательный персонал (уборщики, охрана)

3. Технический персонал для жизнеобеспечения и эксплуатации

4. Представители надзорных организаций и аварийных служб

5. Недобросовестные партнеры

12) Источники, обусловленные техническими средствами – это:

1. Антропогенные источники

2. Техногенные источники

3. Стихийные источники

4. Случайные источники

13) Набор методов и средств для выполнения (или сам процесс) дешифрования информации без обладания необходимым ключом –

1. Шифрование

2. Криптоанализ

3. Расшифрование

14) Техногенные источники угроз безопасности информации делятся на:

1. Внутренние

2. Внешние
3. Стихийные
4. Случайные
5. Преднамеренные

15) Источники угроз такого типа практически не поддаются прогнозированию:
1. Антропогенные источники
2. Техногенные источники
3. Стихийные источники

1) К основным источникам материально-вещественного канала утечки информации относятся:
1. Черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации;
2. Нечитаемые дискеты ЭВМ из-за их физических дефектов и искажений загрузочных или других кодов
3. Бракованная продукция и ее элементы
4. Электромагнитное поле в диапазоне 0,46–0,76 мкм (видимый свет)

2) На этапе закупки информационного сервиса:
1. Оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис
2. Определяется, какими характеристиками и какой функциональностью сервис должен обладать
3. Оцениваются финансовые и иные ограничения приобретения или модернизации сервиса
4. Окончательно формулируются требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика

3) В случае обработки защищаемой информации на компьютере преобладают:
1. Умышленные утечки информации
2. Случайные утечки информации
3. Объективные утечки информации
4. Стихийные утечки информации

4) Политика безопасности строится на основе:
1. Анализа рисков
2. Фактов проникновения вредоносно программного обеспечения
3. Фактов жалоб сотрудников предприятия на ошибки работы компьютеров
4. Макроэкономических показателей

5) Принцип разделения обязанностей предписывает:
1. Так распределять роли и ответственность, что бы один человек не мог нарушить критически важный для организации процесс
2. Выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей
3. Начальнику не вмешиваться в работу подчиненного и наоборот

6) Для защиты документов активно используются следующие средства:
1. Оттиск печати
2. Водяные знаки
3. Рельефная печать
4. Люминесцентные метки
5. Симметричные алгоритмы шифрования

7) В схеме шифрования симметричных алгоритмов используется:
1. Один ключ
2. Два ключа
3. Три ключа

8) В схеме шифрования асимметричных алгоритмов используется:
1. Один ключ

2. Два ключа

3. Три ключа

9) По информативности технические каналы утечки информации делятся на:

1. Информативные

2. Малоинформативные

3. Одноканальные

4. Составные

10) Принцип минимизации привилегий предписывает:

1. Так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс

2. Выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей

3. Некоторым сотрудникам существенно ограничивать возможности

11) К наиболее распространенным угрозам относятся:

1. Уничтожение информации

2. Отрицание подлинности информации

3. Навязывание ложной информации

4. Запись информации в другой кодировке

12) По времени функционирования технические каналы утечки информации делятся на:

1. Постоянные

2. Эпизодические

3. Случайные

4. Составные

13) К физической защите относятся:

1. Противопожарные меры

2. Защита от перехвата данных

3. Защита от вредоносных программ

4. Меры предотвращения спам-рассылок

14) К физической защите относятся:

1. Противопожарные меры

2. Защита мобильных систем

3. Защита от вредоносных программ

4. Настройка прав доступа (ролей) в операционной системе

15) Антропогенные источники угроз безопасности информации – это:

1. Источники, обусловленные действиями субъекта

2. Источники, обусловленные техническими средствами

3. Стихийные бедствия, или другие обстоятельства

16) Стихийные источники угроз безопасности информации – это:

1. Источники, обусловленные действиями субъекта

2. Источники, обусловленные техническими средствами

3. Стихийные бедствия, или другие обстоятельства

17) Несанкционированный доступ - это

1. доступ с выполнением правил разграничения доступа к информации

2. доступ с нарушением правил разграничения доступа субъекта к информации, с использованием штатных средств (программного или аппаратного обеспечения)

3. получение от субъекта доступа к сведениям (имя, учетный номер и т.д.), позволяющим выделить его из множества субъектов

4. получение от субъекта сведений (пароль, биометрические параметры и т.д.), подтверждающих, что идентифицируемый субъект является тем, за кого себя выдает

18) Санкционированный доступ к информации - это

1. доступ с выполнением правил разграничения доступа к информации

2. доступ с нарушением правил разграничения доступа субъекта к информации, с использованием штатных средств (программного или аппаратного обеспечения)

3. получение от субъекта доступа к сведениям (имя, учетный номер и т.д.), позволяющим выделить его из множества субъектов

4. получение от субъекта сведений (пароль, биометрические параметры и т.д.), подтверждающих, что идентифицируемый субъект является тем, за кого себя выдает

19) Уязвимость - это

1. любая характеристика, которая может привести к реализации угрозы

2. действия злоумышленника, предпринимаемые с целью обнаружения уязвимости системы защиты и получения несанкционированного доступа к информации

3. получение от субъекта доступа к сведениям (имя, учетный номер и т.д.), позволяющим выделить его из множества субъектов

4. доступ с выполнением правил разграничения доступа к информации

1. Что не входит к методам применительные к инженерно-технической защите информации

a) четкую постановку задачи,

b) разработку принципов и путей решения задачи;

c) разработку методов решения задач;

d) создание программного, технического и методического обеспечения решения задачи.

2. Силы и воздействия, изменяющие состояние системы является:

a) Входами

b) Системное мышление

c) Выходы

d) система защиты информации

e) модель

3. Представляют собой реакцию системы на входы.

a) Входами

b) Системное мышление

c) Выходы

d) система защиты информации

e) модель

4. Первичное понятие, используемое в понятийном аппарате информационной безопасности это.

a) угроз безопасности

b) Информация

c) информационные системы

d) Задачи инженерно-технической защиты

5. Под уровнем безопасности информации понимается

a) Задачи инженерно-технической защиты

b) Информационные ресурсы

c) Защищенности информации от угроз

d) Ресурсы защиты информации.

6. Не микро цели, как часто их определяют, а четкое и конкретное описание того, что надо сделать для достижения цели.

b) Изменения и хищения информации.

c) Предотвращение утечки.

d)Входы и выходы системы.

e) Задачи инженерно-технической защиты.

7. Состояния и действия субъектов и материальных объектов, которые могут привести к изменению, уничтожению и хищению информации.

a) Меры по их предотвращению.

b) Угрозы безопасности информации.

c) Ресурсы защиты информации.

d)Системы защиты информации.

8. Отличать угрозы изменение, уничтожение, хищение и блокирование информации это.

a) Результаты реализации угроз.

b) Меры защиты информации.

c) Задачи инженерно-технической защиты.

d) Информационные системы.

9. С позиции системного подхода рассматриваются как результаты функционирования системы защиты, они могут представлять собой конкретные действия персонала, предложения по приобретению и установке технических и программных средств.

a) Угрозы безопасности информации.

b)Системное мышление.

c) Меры по защите информации.

d) Демаскирующие признаки

10. По расположению источника угроз могут быть.

a) Внутренние. Источники этих угроз располагаются внутри системы.

b) Внешние. Источники данных угроз находятся вне системы.

c) Угрозы, реализация которых не зависит от активности информационной системы.

d) Угрозы, осуществление которых возможно только при автоматизированной обработке данных.

11. По степени воздействия на информационную систему угрозы могут быть:

a) Пассивные. При реализации данных угроз структура и содержание системы не изменяются.

b) Преднамеренные. Они, как правило, связаны с действиями какого-либо человека,

c) Активные. При их осуществлении структура и содержание системы подвергается изменениям.

d)Случайные. Эти угрозы не связаны с умышленными действиями правонарушителей;

12. Что не входит к угрозам по размерам наносимого ущерба:

a) Общие. Эти угрозы наносят ущерб объекту безопасности в целом, причиняя значительное отрицательное влияние на условия его деятельности.

b) Локальные. Угрозы этого типа воздействуют на условия существования отдельных частей объекта безопасности.

c) Частные. Они причиняют вред отдельным свойствам элементов объекта или отдельным направлениям его деятельности.

d) Пассивные. При реализации данных угроз структура и содержание системы не изменяются.

13.Кто может быть владельцем защищаемой информации?

a) Только государство и его структуры;

b) Предприятия акционерные общества, фирмы;

c) Юридическое или физическое лицо;

d) Кто угодно.

14. 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.

15.Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

a) Пароли

b) Анкеты

c) Коды

d) Ярлыки

16.От несанкционированного доступа может быть защищён:

a) каждый диск

b) папка

c) файл

d) ярлык

17.К биометрическим системам защиты информации относятся системы идентификации по:

a) Отпечаткам пальцев;

b) Характеристикам речи;

c) Радужной оболочке глаза;

d) Изображению лица;

e) Геометрии ладони руки;

f) Все выше перечисленные;

18. Выберите типы вредоносных программ:

a) Вирусы, черви, троянские и хакерские программы

b) Шпионское, рекламное программное обеспечение

c) Операционная система Linux

d) Операционная система Windows

e) MicrosoftOffice

19. Компьютерные вирусы -

a) Являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

b) Вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

c) Это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

20. По "среде обитания" вирусы можно разделить на:

a) Загрузочные

b) файловые

c) макровирусы

d) очень опасные

e) не опасные

f) опасные

21. Попытка реализации угрозы – это …

А. уязвимость;

Б. атака;

В. конфиденциальность;

Г. взлом.

22.Найди соответствие.

a) заражают загрузочный сектор гибкого или жёсткого диска.

b) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске.

c) существуют для интегрированного офисного приложения MicrosoftOffice.

1. загрузочные вирусы

2. файловые вирусы

3. макровирусы

23.Сетевые черви -

a) Являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

b) Это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

c) Программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

24. Время жизни информации – это …

a. Время, пока информация хранится в информационной системе;

b. Время, пока информация актуальна;

c. Время, пока информация интересна для злоумышленников;

d. Время, пока стоимость создания информации выше стоимость потери

25. К субъектам информационной системы не относится …

a. Владелец;

b. Пользователь;

c. Регулятор;

d. Собственник;

1. К субъектам информационной системы не относится …

a. Владелец;

b. Пользователь;

c. Регулятор;

d. Собственник;

2. Что не относится к непреднамеренным воздействиям?

a. воздействия из-за ошибок пользователя;

b. сбой технических средств;

c. сбой программных средств;

d. внедрение вируса в автоматическом режиме.

3. Время жизни информации – это …

a. время, пока информация хранится в информационной системе;

b. время, пока информация актуальна;

c. время, пока информация интересна для злоумышленников;

d. время, пока стоимость создания информации выше стоимость потери.

4. Какие методы реализуют контроль соблюдения установленного порядка к защищаемой информации?

a. правовые;

b. административные;

c. технические;

d. все перечисленные.

5. Что не является примером нарушения статической целостности информации?

a. ввод неверных данных;

b. несанкционированное изменение данных;

c. изменение программного модуля вирусом;

d. внесение дополнительных пакетов в сетевой трафик.

6. Что не относится к косвенным каналам утечки информации?

a. перехват побочного электромагнитного излучения;

b. использование подслушивающих средств;

c. сбор производственных отходов с информацией;

d. дистанционное видеонаблюдение.

7. Наиболее защищенным элементом информационной системы обычно является …

a. Операционная система;

b. Персонал;

c. Система управления базами данных;

d. Сетевые подключения.

8. Как по-другому называется монитор безопасности?

a. системный монитор;

b. администраторский монитор;

c. диспетчер доступа;

d. диспетчерский монитор.

9. Выберите лишний шаг в процедуре разработки политики информационной безопасности.

a. разработка желаемой политики безопасности;

b. выбор системы защиты;

c. стандартизация системы защиты;

d. определение требований, не реализованных системой защиты.

10.Что не относится к основным принципам обеспечения национальной безопасности?

a. взаимная ответственность личности, общества и государства по обеспечению безопасности;

b. законность;

c. соблюдение баланса между сферами ответственности личности, общества и государства;

d. соблюдение баланса жизненно важных интересов личности, общества и государства.

11.Основной задачей криптоанализа является …

a. компрометация ключа;

b. получение открытого текста без знания ключа;

c. получение шифр текста без знания ключа;

d. получение ключа из шифр текста.

12.Класс односторонних функций, применяемых в криптографии, называется

a. генераторы случайных чисел или рнд-функция;

b. функции Керкхоффса или крфс-функция;

c. сингл-функция;

d. хэш-функция.

13. С помощью какого типа криптографических алгоритмов реализуется электронная цифровая подпись?

a. блочных;

b. поточных;

c. симметричных;

d. ассиметричных.

14. Что не является методом идентификации?

a. использование парольной фразы;

b. метод "рукопожатия";

c. метод "встречного приветствия";

d. использование смарт-карт.

15. К какому виду ошибок относится пропуск атак на информационные системы?

a. ошибки первого рода;

b. ошибки второго рода;

c. ошибки третьего рода;

d. ошибки четвертого рода.

16. Угрозы, приводящие к несанкционированному распространению носителя к злоумышленнику-

a. Угрозами утечки информации

b. Угрозами воздействия на источник информации

17.Сетевые черви это

a. Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты

b. Вирусы, которые проникнув на компьютер, блокируют работу сети

c. Вирусы, которые внедряются в документы под видом макросов

d. Хакерские утилиты управляющие удаленным доступом компьютера

e. Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

18. К вредоносным программам относятся:

a. Потенциально опасные программы

b. Вирусы, черви, трояны

c. Шпионские и рекламные программы

d. Вирусы, программы-шутки, антивирусное программное обеспечение

e. Межсетевой экран, брандмауэр

19.Отметьте составные части современного антивируса

a. Модем

b. Принтер

c. Сканер

d. Межсетевой экран

e. Монитор

20.Вредоносные программы - это

a. шпионские программы

b. программы, наносящие вред данным и программам, находящимся на компьютере

c. антивирусные программы

d. программы, наносящие вред пользователю, работающему на зараженном компьютере

e. троянские утилиты и сетевые черви

21.Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию?

22.Компьютерные вирусы это

a. Вредоносные программы, наносящие вред данным.

b. Программы, уничтожающие данные на жестком диске

c. Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.

d. Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера

e. Это скрипты, помещенные на зараженных интернет-страничках

23.Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

a. Загрузочный вирус

b. Макровирус

c. Файловый вирус

d. Сетевой червь

e. Троян

24.Укажите порядок действий при наличии признаков заражения компьютера

a. Сохранить результаты работы на внешнем носителе

b. Запустить антивирусную программу

c. Отключиться от глобальной или локальной сети

25.Вирус поражающий документы называется

a. Троян

b. Файловый вирус

c. Макровирус

d. Загрузочный вирус

e. Сетевой червь

1. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

a. активный перехват;

b. пассивный перехват;

c. аудиоперехват;

d. видеоперехват;

e. просмотр мусора.

2. Перехват, который осуществляется путем использования оптической техники, называется:

a. активный перехват;
b. пассивный перехват;
c. аудиоперехват;
d. видеоперехват;
e. просмотр мусора.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

a. активный перехват;
b. пассивный перехват;
c. аудиоперехват;
d. видеоперехват;
e. просмотр мусора.

4. Перехват, который осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера называется:

a. активный перехват;
b. пассивный перехват;
c. аудиоперехват;
d. видеоперехват;
e. просмотр мусора.

5. Перехват, который неправомерно использует технологические отходы информационного процесса называется:

a. активный перехват;
b. пассивный перехват;
c. аудиоперехват;
d. видеоперехват;
e. просмотр мусора.

6. Как называется последовательность шагов, которые предпринимают стороны для совместного решения задачи, требующей применение криптографических методов:

a.криптографические алгоритмы;
b.криптографические протоколы;
c.криптографические функции;
d.криптографические обмены.

7. Уберите несуществующий криптографический протокол.

a. Протокол с наблюдением;
b. Протокол с арбитражем;
c. Протокол с судейством;
d. Самоутверждающийся протокол.

8. Что не относится к основным криптографическим протоколам?

a. обмен ключами;
b. депонирование ключей;
c. цифровая подпись;
d. распределение ответственности.

9. С помощью какого типа криптографических алгоритмов реализуется электронная цифровая подпись?

a. блочных;
b. поточных;
c. симметричных;
d. ассиметричных.

10. Что не является видом криптоаналитической атаки?

a. словарная атака;
b. брутфорсе-атака;
c. блицкриг-атака;
d. метод сведения к середине.

11.Что не относится к основным преимуществам программных средств защиты?

a. простота тиражирования;

b. простота доступа к ресурсам;

c. простота применения;

d. гибкость настройки.

12.Что не является видом сервисов безопасности?

a. превентивные меры;

b. проективные меры;

c. меры по выявлению нарушений;

d. меры восстановления режимы безопасности.

13.Что не является методом идентификации?

a. использование парольной фразы;

b. метод "рукопожатия";

c. метод "встречного приветствия";

d. использование смарт-карт.

14. Какая система идентификации по биометрическим показателям является наиболее распространённой?

a. по отпечаткам пальцев;

b. по сетчатке глаза;

c. по голосу;

d. по клавиатурному почерку.

15.Какой сервис позволяет контролировать действия субъектов над информационными объектами?

a. сервис контроля пользователей;

b. сервис управления доступом;

c. системный сервис;

d. пользовательский сервис.

16. Как называется анализ накопленной системной информации, проводимый оперативно или периодически?

a.аудит;

b.протоколирование;

c.идентификация;

d.систематизация.

17.К какому виду ошибок относится пропуск атак на информационные системы?

a. ошибки первого рода;

b. ошибки второго рода;

c. ошибки третьего рода;

d. ошибки четвертого рода.

18.Что не относится к потенциальным угрозам безопасности информации в локальных вычислительных сетях?

a. несанкционированный доступ в локальную вычислительную систему со стороны штатных компьютеров;

b. несанкционированный доступ со стороны линий связи;

c. нештатные административно-правовые ситуации;

d. аварийные ситуации с оборудованием.

19.Как называются программные или аппаратные средства разграничения доступа между сегментами локальной вычислительной сети?

a. антивирусный экран;

b. межсетевые экраны;

c. транспортный узел;

d. сигнально-аппаратный узел.

20.Как называют вид компьютерных вирусов, которые действуют самостоятельно и не внедряются в тела других файлов?

a."трояны";

b. стелс-вирусы;
c. полиморфы;
d."черви".
21.Попытка реализации угрозы – это …
a. уязвимость;
b. атака;
c. конфиденциальность;
d. взлом.
22. Что не является примером нарушения статической целостности информации?
a. ввод неверных данных;
b. несанкционированное изменение данных;
c. изменение программного модуля вирусом;
d. внесение дополнительных пакетов в сетевой трафик.
23. Угроза утечки информации ограниченного доступа, хранящейся в информационной системе или передающейся по каналам связи – это …
a. угроза нарушения конфиденциальности;
b. угроза нарушения целостности;
c. угроза отказа служб;
d. все перечисленные.
24. 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.
25.Что не относится к косвенным каналам утечки информации?
a. перехват побочного электромагнитного излучения;
b. использование подслушивающих средств;
c. сбор производственных отходов с информацией;
d. дистанционное видеонаблюдение.

Блок 3 (Владеть):
1. С помощью какого типа криптографических алгоритмов реализуется электронная цифровая подпись?
b. блочных;
c. поточных;
d. симметричных;
e. ассиметричных.
2. Что не является методом идентификации?
a. использование парольной фразы;
b. метод "рукопожатия";
c. метод "встречного приветствия";
d. использование смарт-карт.
3. К какому виду ошибок относится пропуск атак на информационные системы?
a. ошибки первого рода;
b. ошибки второго рода;
c. ошибки третьего рода;
d. ошибки четвертого рода.
4. Угрозы, приводящие к несанкционированному распространению носителя к злоумышленнику-
c. Угрозами утечки информации
d. Угрозами воздействия на источник информации
5. Сетевые черви это
a. Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты

b. Вирусы, которые проникнув на компьютер, блокируют работу сети

c. Вирусы, которые внедряются в документы под видом макросов

d. Хакерские утилиты управляющие удаленным доступом компьютера

e. Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

6. К вредоносным программам относятся:

a. Потенциально опасные программы

b. Вирусы, черви, трояны

c. Шпионские и рекламные программы

d. Вирусы, программы-шутки, антивирусное программное обеспечение

e. Межсетевой экран, брандмауэр

7. Отметьте составные части современного антивируса

a. Модем

b. Принтер

c. Сканер

d. Межсетевой экран

e. Монитор

8. Вредоносные программы - это

a. шпионские программы

b. программы, наносящие вред данным и программам, находящимся на компьютере

c. антивирусные программы

d. программы, наносящие вред пользователю, работающему на зараженном компьютере

e. троянские утилиты и сетевые черви

9. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию?

10.Компьютерные вирусы это

a. Вредоносные программы, наносящие вред данным.

b. Программы, уничтожающие данные на жестком диске

c. Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.

d. Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера

e. Это скрипты, помещенные на зараженных интернет-страничках

11.Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

a. Загрузочный вирус

b. Макровирус

c. Файловый вирус

d. Сетевой червь

e. Троян

12.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.

13. Право на использование некоторого ресурса – это …

a. уполномочивание;

b. контроль доступа;

c. право собственности;

d. сертификация.

14. Какие методы реализуют контроль соблюдения установленного порядка к защищаемой информации?

a. правовые;

b. административные;

c. технические;

d. все перечисленные.

15. 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.

16. Методами защиты с "черным ящиком" называют …

a. методы, не имеющие математического обоснования стойкости;

b. "слепые" полуавтоматические методы;

c. криптографические методы;

d. методы, реализованные на аппаратном уровне.

17.Что является основной целью административного уровня безопасности?

a. отладка монитора безопасности;

b. формирование политики безопасности;

c. реализация дискреционной модели;

d. реализация мандатной модели.

18. К какому уровню политике безопасности относятся вопросы, касающиеся отдельных аспектов организации?

a. верхнего уровня;

b. административного уровня;

c. среднего уровня;

d. нижнего уровня.

19. Выберите лишний шаг в процедуре разработки политики информационной безопасности.

a. разработка желаемой политики безопасности;

b. выбор системы защиты;

c. стандартизация системы защиты;

d. определение требований, не реализованных системой защиты.

20. Что не относится к недостаткам операционных систем семейств Windows?

a. невозможно встроенными средствами гарантированно удалять остаточную информацию;

b. невозможно встроенными средствами обеспечить полноту системы;

c. не обеспечивается регистрация выдачи документов на "твёрдую копию", а также некоторые другие требования к регистрации событий;

d. невозможно в общем случае обеспечить замкнутость (или целостность) программной среды.

21. Какие методы несанкционированного доступа является наиболее распространёнными в операционной системе Windows?

a. Позволяющие несанкционированно запустить исполняемый код;

b. Позволяющие обойти установленные разграничения прав доступа;

c. Троянские программы;

d. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

22.Уберите несуществующий криптографический протокол.

a. Протокол с наблюдением;

b. Протокол с арбитражем;

c. Протокол с судейством;

d. Самоутверждающийся протокол.

23. Что не относится к основным криптографическим протоколам?

a. обмен ключами;

b. депонирование ключей;

c. цифровая подпись;

d. распределение ответственности.

24. С помощью какого типа криптографических алгоритмов реализуется электронная цифровая подпись?

a. блочных;

b. поточных;

c. симметричных;

d. ассиметричных.

25. Что не является видом криптоаналитической атаки?

a. словарная атака;

b. брутфорсе-атака;

c. блицкриг-атака;

d. метод сведения к середине.

1. Информация является первичной и описывает конкретный материальный объект на языке его признаков.

a) Информация признаковая.

b) Источники информации

c) Системы информации.

d) Семантическая информация

2. Источниками признаковой информации являются

a) Источники информации.

b) Объекты.

c) Конфиденциальная информация.

d) Семантическая информация.

3. Продукт абстрактного мышления человека и обработки данных рецепторов других живых существ.

a) Демаскирующие признаки

b) Объект защиты.

c) Семантическая информация

d) Признаковая информация

4. Что не является примером нарушения статической целостности информации?

e. Ввод неверных данных;

f. Несанкционированное изменение данных;

g. Изменение программного модуля вирусом;

h. Внесение дополнительных пакетов в сетевой трафик.

5.Что не относится к косвенным каналам утечки информации?

a. Перехват побочного электромагнитного излучения;

b. Использование подслушивающих средств;

c. Сбор производственных отходов с информацией;

d. Дистанционное видеонаблюдение.

6. Наиболее защищенным элементом информационной системы обычно является …

a. Операционная система;

b. Персонал;

c. Система управления базами данных;

d. Сетевые подключения.

7. К субъектам информационной системы не относится …

a. Владелец;

b. Пользователь;

c. Регулятор;

d. Собственник;

8. Информационная система – это …

a. Набор программных и технических средств;

b. Упорядоченную совокупность документов и информационных технологий, реализующих информационные процессы;

c. Упорядоченная совокупность документов, относящихся к определенной области;

d. Набор программных средств, относящихся к одной задаче.

9. Несанкционированный доступ – это …

a. Доступ или воздействие с нарушением правил доступа;

b. Изменение пароля с правами администратора;

c. Доступ в незащищенную систему пользователя;

d. Изменение пароля доступа в систему пользователем.

10.К конфиденциальной информации не относится …

a. Служебная тайна;

b. Персональные данные;

c. Государственная тайна;

d. Коммерческая тайна.

11.Что не относится к непреднамеренным воздействиям?

a. Воздействия из-за ошибок пользователя;

b. Сбой технических средств;

c. Сбой программных средств;

d. Внедрение вируса в автоматическом режиме.

12.Целью защиты информации является …

a. Предотвращение экономического ущерба собственнику, владельцу или пользователю информации;

b. Предотвращения доступа в информационную систему нелегитимным пользователям;

c. Недопущение распространения конфиденциальной информации;

d. Соблюдение политики безопасности и выполнение правил хранения информации.

13.Что не является характеристикой информации?

a. Статичность;

b. Тип доступа;

c. Время отклика;

d. Стоимость создания.

14.Какая стоимостная характеристика информации совпадает с себестоимостью информации?

a. Стоимость создания;

b. Стоимость потери конфиденциальности;

c. Стоимость скрытого нарушения целостности;

d. Стоимость утраты.

15.Время жизни информации – это …

a. Время, пока информация хранится в информационной системе;

b. Время, пока информация актуальна;

c. Время, пока информация интересна для злоумышленников;

d. Время, пока стоимость создания информации выше стоимость потери.

16. Каков максимальный срок хранения документов с грифом "секретно"?

a. 5 лет;

b. 10 лет;

c. Неограничен;

d. До тех пор, пока информация не будет скомпрометирована.

17.Отличительные особенности объектов наблюдения, позволяющие отличить объект конфиденциальных интересов от других, подобных ему –

a) Демаскирующие признаки

b) Конфиденциальная информация.

c) Семантическая информация.

18.Средства регистрации, хранения, передачи информации, или, иначе, материал, на который можно записывать информацию.

a) Источник информации

b) Носители информации

c) Информационные ресурсы

d) Источники информации

19.Документы и массивы документов в информационных системах: библиотеках, архивах, фондах, банках данных, других видах информационных систем.

a) Источник информации

b) Носители информации

c) Информационные ресурсы

d) Источники информации

20.Информация, составляющая государственную тайну не может иметь гриф…

a) «для служебного пользования»

b) «секретно»

c) «совершенно секретно»

d) «особой важности»

21.Утечка информации – это …

a) Процесс раскрытия секретной информации

b)Процесс уничтожения информации

c) Непреднамеренная утрата носителя информации

d)Несанкционированный процесс переноса информации от источника к злоумышленнику

22.Защита информации обеспечивается применением антивирусных средств

a) Да

b) Нет

c) Не всегда

23. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроз

a) Активная

b) Пассивная

24. 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.

25. Право на использование некоторого ресурса – это …

a) контроль доступа;

b) право собственности;

c) сертификация.

d) уполномочивание;

1. 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.

2. Право на использование некоторого ресурса – это …

a. уполномочивание;

b. контроль доступа;

c. право собственности;

d. сертификация.

3. Какие методы реализуют контроль соблюдения установленного порядка к защищаемой информации?

a. правовые;

b. административные;

c. технические;

d. все перечисленные.

4. 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.

5. Методами защиты с "черным ящиком" называют …

a. методы, не имеющие математического обоснования стойкости;

b. "слепые" полуавтоматические методы;

c. криптографические методы;

d. методы, реализованные на аппаратном уровне.

6. Что является основной целью административного уровня безопасности?

a. отладка монитора безопасности;

b. формирование политики безопасности;

c. реализация дискреционной модели;

d. реализация мандатной модели.

7. К какому уровню политике безопасности относятся вопросы, касающиеся отдельных аспектов организации?

a. верхнего уровня;

b. административного уровня;

c. среднего уровня;

d. нижнего уровня.

8. Выберите лишний шаг в процедуре разработки политики информационной безопасности.

a. разработка желаемой политики безопасности;

b. выбор системы защиты;

c. стандартизация системы защиты;

d. определение требований, не реализованных системой защиты.

9. Что не относится к недостаткам операционных систем семейств Windows?

a. невозможно встроенными средствами гарантированно удалять остаточную информацию;

b. невозможно встроенными средствами обеспечить полноту системы;

c. не обеспечивается регистрация выдачи документов на "твёрдую копию", а также некоторые другие требования к регистрации событий;

d. невозможно в общем случае обеспечить замкнутость (или целостность) программной среды.

10. Какие методы несанкционированного доступа является наиболее распространёнными в операционной системе Windows?

a. Позволяющие несанкционированно запустить исполняемый код;

b. Позволяющие обойти установленные разграничения прав доступа;

c. Троянские программы;

d. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

11. Наиболее распространёнными методами несанкционированного доступа в операционной системе Unix является …

a. Позволяющие несанкционированно запустить исполняемый код;

b. Позволяющие обойти установленные разграничения прав доступа;

c. Троянские программы;

d. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

12. Что не относится к основным принципам обеспечения национальной безопасности?

a. взаимная ответственность личности, общества и государства по обеспечению безопасности;

b. законность;

c. соблюдение баланса между сферами ответственности личности, общества и государства;

d. соблюдение баланса жизненно важных интересов личности, общества и государства.

13. К правовым методам обеспечения информационной безопасности не относят …

a. определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

b. определение ответственности физических и юридических лиц за несанкционированный доступ к информации;

c. определение уровней безопасностей в информационных системах;

d. определение ответственности физических и юридических лиц за противоправное раскрытие конфиденциальной информации.

14. Какой документ представляет собой совокупность взглядов на цели, задачи и принципы и основные направления обеспечения информационной безопасности Российской Федерации:

a. Конституция Российской Федерации;

b. Концепция национальной безопасности Российской Федерации;

c. Доктрина информационной безопасности Российской Федерации;

d. Федеральный закон "Об информации, информатизации и защите информации".

15. К какому уровню правового обеспечения информационной безопасности относятся Постановления Правительства Российской Федерации:

a. первому;

b. второму;

c. третьему;

d. четвертому.

16. Основной задачей криптоанализа является …

a. компрометация ключа;

b. получение открытого текста без знания ключа;

c. получение шифртекста без знания ключа;

d. получение ключа из шифртекста.

17. Что не относится к задачам криптографии?

a. аутентификация;

b. целостность;

c. системность;

d. неоспоримость.

18. Как называются криптографические алгоритмы, для которых ключ зашифрования не совпадает с ключом расшифрования?

a. блочные;

b. поточные;

c. симметричные;

d. ассиметричные.

19. В чем суть принципа Керкхоффса?

a. в криптосистеме должен использоваться сменный элемент, называемый ключом, и секретность шифра обеспечивается секретностью ключа шифрования;

b. устойчивость криптосистемы обратно пропорциональна интегральной мощности используемых для взлома компьютеров;

c. устойчивость криптосистемы полиномиально зависит от длины используемого ключа;

d. в криптосистеме шифрование должно осуществляться посимвольно, причем каждый следующий символ не должен зависеть от предыдущих.

20. Класс односторонних функций, применяемых в криптографии, называется …

a. генераторы случайных чисел или рнд-функция;

b. функции Керкхоффса или крфс-функция;

c. сингл-функция;

d. хэш-функция.

21.Какой сервис позволяет контролировать действия субъектов над информационными объектами?

a. сервис контроля пользователей;

b. сервис управления доступом;

c. системный сервис;

d. пользовательский сервис.

22. Как называется анализ накопленной системной информации, проводимый оперативно или периодически?

a. аудит;

b. протоколирование;

c. идентификация;

d. систематизация.

23. К какому виду ошибок относится пропуск атак на информационные системы?

a. ошибки первого рода;

b. ошибки второго рода;

c. ошибки третьего рода;

d. ошибки четвертого рода.

24. Что не относится к потенциальным угрозам безопасности информации в локальных вычислительных сетях?

a. несанкционированный доступ в локальную вычислительную систему со стороны штатных компьютеров;

b. несанкционированный доступ со стороны линий связи;

c. нештатные административно-правовые ситуации;

d. аварийные ситуации с оборудованием.

25. Как называются программные или аппаратные средства разграничения доступа между сегментами локальной вычислительной сети?

a. антивирусный экран;

b. межсетевые экраны;

c. транспортный узел;

d. сигнально-аппаратный узел.

Методические материалы, характеризующие процедуры оценивания

Перерчень вопросов для проведения устного собеседования.

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	***Продвинутый уровень***

		выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	
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) Аппаратно-программные средства криптографической защиты информации выполняют функции:

1. Аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.

2. Организовывают реализацию политики безопасности информации на этапе эксплуатации КС.

3. Проверяют на отсутствие закладок приборов, устройств.

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=404

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