Министерство науки и высшего образования Российской Федерации
Лысьвенский филиал
федерального государственного автономного образовательного учреждения
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
**для проведения промежуточной аттестации обучающихся по дисциплине
«Методы и средства обеспечения информационной безопасности
компьютерных и программных систем»**
Приложение к рабочей программе дисциплины

Направление подготовки:	09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы:	Компьютерные системы
Квалификация выпускника:	«Бакалавр»
Выпускающая кафедра:	Технических дисциплин
Форма обучения:	Очная, очно-заочная,

Курс: 4 (5) **Семестр**: 7 (9)

Трудоёмкость:
Кредитов по рабочему учебному плану: 3 ЗЕ
Часов по рабочему учебному плану: 108 ч.

Форма промежуточной аттестации:
Зачёт: 7 (9) семестр

Лысьва 2024

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД освоение учебного материала дисциплины запланировано в течение одного семестра (7-го семестра учебного плана очной формы обучения; 9-го семестра учебного плана очно-заочной и заочной форм обучения) и разбито на 3 учебных раздела. В каждом разделе предусмотрены аудиторные лекционные, лабораторные работы, а также самостоятельная работа студентов.

В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и зачета. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**				
	Текущий		**Рубежный**		**Итоговый**
	С	**ТО**	**ОЛР**	**Т/КР**	**Зачёт**
Усвоенные знания					
З.1 Знать основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства крипто-графической защиты информации;		ТО	ОЛР		ТВ
З.2 Знать современную классификацию средств защиты информации от несанкционированного доступа операционных систем и систем управления базами данных; технологию проектирования и создания безопасных информационных систем;		ТО	ОЛР		ТВ
З.3 Знать современную нормативно-правовую базу создания защищенных распределенных информационных систем;		ТО	ОЛР		ТВ
З.4 Знать инструментальные программные и аппаратные средства анализа защищенности компьютерных и программных систем.		ТО	ОЛР		ТВ
Освоенные умения					
У.1 Уметь применять современные программные средства защиты информации;			ОЛР		ПЗ
У.2 Уметь конфигурировать и настраивать современные аппаратные средства защиты информационных процессов в			ОЛР		ПЗ

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля				
	Текущий		Рубежный		Итоговый
	С	ТО	ОЛР	Т/КР	Зачёт
компьютерных системах;					
У.3 Уметь применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных и программных систем.			ОЛР		ПЗ
Приобретенные владения					
В.1 Владеть навыками разработки защищенной информационной системы;			ОЛР		ПЗ
В.2 Владеть навыками настройки и конфигурирования программных и аппаратных средств защиты информации.			ОЛР		ПЗ

С – собеседование по теме; ТО – теоретический опрос; КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; ПЗ – практическое задание.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в форме зачета, проводимая с учётом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;

- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ и рубежных контрольных работ (после изучения каждого модуля учебной дисциплины).

2.2.1. Защита лабораторных работ

Всего запланировано 2 лабораторные работы. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом или группой студентов. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.2.2. Рубежная контрольная работа

Согласно РПД запланировано 3 рубежные контрольные работы (КР).

Типовые задания первой КР:

1.Методы поиска и сбора информации:

- Использование поисковых систем.
- Использование электронных баз данных.
- Анализ информации в открытых источниках.

2.Методика устранения компьютерной информации:

- Физическое уничтожение.
- Использование шифрования.

Типовые задания второй КР:

1.Уязвимости Windows.

- Недостаточная защита аккаунтов.
- Уязвимости в программном обеспечении.
- Незапланированные обновления.

2.Защита от копирования переносных носителей.

- Использование цифровых прав управления доступом.
- Физические меры защиты.
- Контроль доступа к данным.

Типовые задания третьей КР:

Записать определения, описать: Информационное противоборство, Информационная преступность, Информационное воздействие, Информационное оружие, защита информации, утечка, разглашение, несанкционированный доступ, несанкционированное воздействие, цель и эффективность защиты информации, Конфиденциальность информации, Шифрованием информации, Целостностью информации, хеширование, доступность информации, Политика безопасности, аутентичность, контроль доступа, атака на информацию, Вредоносные программы, вирус, «троянский конь», атака «салями», загрузочные вирусы, макровирусы,

«черви», «маскарад», «люки», «взлом» системы; описать алгоритм.

Ответы на типовые вопросы контрольных работ приведены в Приложении А.

Типовые шкала и критерии оценки результатов рубежной контрольной работы приведены в общей части ФОС образовательной программы.

2.3. Выполнение комплексного индивидуального задания на самостоятельную работу

Для оценивания навыков и опыта деятельности (владения), как результата обучения по дисциплине, не имеющей курсового проекта или работы, используется индивидуальное комплексное задание студенту.

Примерные задания индивидуальных работ

1. Выполнение индивидуального задания по теме: «Вирусы, черви, распространенные вирусы современности, их последствия».
2. Выполнение индивидуального задания по теме: «Методы обеспечения защиты компьютерных и программных систем»

Типовые шкала и критерии оценки результатов защиты индивидуального комплексного задания приведены в общей части ФОС образовательной программы.

2.4. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

2.4.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания

Промежуточная аттестация проводится в форме зачета. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде зачета приведены в общей части ФОС образовательной программы.

2.4.2. Процедура промежуточной аттестации с проведением аттестационного испытания

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций.

2.4.2.1. Типовые вопросы и задания для зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Структура понятия «Информационная безопасность», что в нее входит, особенности.
2. Атаки (источники, формы, риски) на информацию.
3. Вредоносные программы.
4. Назовите основные характеристики стандарта широкополосной БПС IEEE.802.16.
5. Криптографические модели, методы криптографии, алгоритм RSA.
6. Электронная цифровая подпись, описать, особенности, требования.
7. Криптографический интерфейс приложений ОС Windows (CryptoAPI). Опишите принципы использования CryptoAPI.
8. Опишите основные алгоритмы шифрования. Понятия симметричных и ассиметричных алгоритмов. Применение.
9. Опишите многоуровневую защиту корпоративных сетей.
10. Какие существуют способы несанкционированного доступа к информации и способы противодействия данному доступу.
11. Описать что такое межсетевой экран, для чего, основные понятия.
12. Что такое виртуальные сети, объяснить понятие туннелирование, управление, возможности типичных систем.
13. Опишите основную защиту информации в сетях, понятие открытый и закрытый ключ.
14. Применение инфраструктуры на основе криптографии.
15. Описать стандарты: X.509, PKCS, PKIX, SSL, TLS, SET.
16. Опишите безопасность в открытых сетях, принцип действия криптографии с открытым и закрытым ключом.
17. Приведите основные характеристики IP протоколов управления мобильностью.
18. Приведите основные характеристики протокола безопасности WEP.
19. Как осуществляется шифрование в протоколе WEP?
20. Существуют ли проблемы аутентификации при шифровании в протоколе WEP?
21. Приведите примеры основных приложений, используемых в компании и настроенные как сетевые, методы обеспечения безопасности в них.

Типовые вопросы и практические задания для контроля освоенных умений:

1.Компьютерная информация: определение, основные категории с точки зрения безопасности

2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.

3. Политика безопасности информационных систем и ее основные элементы.

4. Классификация угроз информационным системам.

5. Обзор нормативных правовых актов РФ в области информационной защиты.

6. Дискреционный и мандатный доступ к ресурсам информационных систем.

7. Основные методы обеспечения безопасности информационных систем

8. Основные услуги безопасности, предоставляемые информационными системами

9. Механизмы реализации услуг безопасности в информационных системах

10. Классификация криптографических алгоритмов

11. Структурная схема симметричной криптосистемы

12. Структурная схема асимметричной криптосистемы

13. Математические определения шифра, процедур шифрования и дешифрации

14. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы.

15. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля

16. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования, шифры ECB, CBC, CFB, OFB.

17. Алгоритмы шифрования DES и TEA: структура, достоинства и недостатки

18. Линейный криптоанализ блочных шифров

19. Дифференциальный криптоанализ блочных шифров

20 Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов.

21. RSA: возможные криптоатаки и криптостойкость алгоритма, структура криптоалгоритма

22. Алгоритм асимметричного шифрования Рабина

23. Криптосистема ЭльГемаля: структура, криптостойкость

24. Метод ключевого обмена Диффи-Хелмана

25. Системы управления ключами: разновидности ключей, схемы обмена ключами

26. Сертификация открытых ключей асимметричных алгоритмов. Инфраструктура PKI. Хэш-функции: назначение и основные свойства

27. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA.

28. Генерация криптостойких случайных чисел.

29. Вероятностная генерация простых чисел для криптоалгоритмов.

30. Аутентификация в информационных системах: назначение, разновидности, угрозы подсистемам аутентификации

31. Биометрические методы аутентификации пользователей

32. Системы аутентификации с защищенными паролями и с проверкой на стороне сервера

33. Система аутентификации по схеме «запрос-ответ»
34. Протокол аутентификации пользователей Kerberos
35. Угрозы безопасности в глобальных сетях
36. Межсетевые экраны: назначение, основные функции, состав
37. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки
38. Proxy-сервера: назначение, основные функции, достоинства и недостатки
38. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона
40. Обзор криптографических протоколов: SSL, TLS, IPSecurity, SSH, PPTP, L2TP
41. Средства аудита ОС семейства Windows
42. Модель безопасности ОС семейства Windows
43. Модель безопасности ОС Unix. Подсистема аудита ОС семейства Unix.
44. Вредоносные программы: определение, классификация
45. Компьютерные вирусы: определение, методы заражения и маскировки. Методы защиты от вирусов.

Типовые комплексные задания для контроля приобретенных владений:

1.Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.

2.Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.

3.Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.

4.Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.

5.Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых фильтров.

6.Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.

7.Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.

8.Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.

9.Разработайте политику для пакетного фильтра, разрешающего только

получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.

10.Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.

11.С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.

12.Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.

13.Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа ОС Windows Server.

14.Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа ОС Windows Server. Файл-сертификат открытого ключа прилагается.

15.Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа ОС Windows Server.

16.Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

17.Осуществите криптографическую защиту сетевого трафика средствами СКЗИ StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

18.Организовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89 и ГОСТ 34.12-2015, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС Windows Server и Windows.

19.Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.

20.Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMPпакетов большой длины.

21.Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.

22.Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users».

23.Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители.

24.Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping и широковещательной ICMP-посылки; утилиты

icmpush (тип ICMPпакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.

25. С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС и запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа и версии ОС, а также сетевых сервисов.

2.3.2.2. Шкалы оценивания результатов обучения на зачете

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь и владеть* заявленных дисциплинарных компетенций проводится в режиме «зачтено» и «не зачтено».

Типовые шкала и критерии оценки результатов обучения при сдаче зачёта для компонентов *знать, уметь и владеть* приведены в общей части ФОС бакалаврской программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при зачете считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в форме зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.

Приложение А

Ответы на типовые задания первой КР:

1.Методыпоискаисбора информации:

- Использование поисковых систем.

- Использование электронных баз данных.

- Анализ информации в открытых источниках.

2.Методикаустраниениякомпьютернойинформации:

- Физическое уничтожение.

- Использование шифрования.

Задание первой контрольной работы включает две части: методы поиска и сбора информации, а также методику устранения компьютерной информации.

1. Методы поиска и сбора информации:

- Использование поисковых систем. При поиске информации в сети Интернет наиболее распространенным методом является использование поисковых систем, таких как Google, Яндекс, Bing и др. Необходимо правильно формулировать запрос, чтобы получить максимально точные результаты и оценить достоверность и актуальность найденной информации.

- Использование электронных баз данных. Электронные базы данных представляют собой коллекции информации, организованные в удобной для поиска форме. Они содержат разнообразные источники данных, такие как научные статьи, книги, патенты и многое другое. Примеры электронных баз данных включают PubMed, IEEE Xplore, Scopus и множество других. При использовании электронных баз данных важно уметь правильно работать с интерфейсом и проводить эффективный поиск информации.

- Анализ информации в открытых источниках. Открытые источники информации представляют собой данные, доступные для свободного использования и публикации. Это могут быть государственные отчеты, статистические данные, научные статьи, открытые базы данных и т.д. Чтобы провести анализ информации из открытых источников, необходимо быть

внимательным к их достоверности и актуальности, а также уметь провести анализ и интерпретацию полученных данных.

2. Методика устранения компьютерной информации:

- Физическое уничтожение. При физическом уничтожении компьютерной информации используется метод полного стирания или разрушения носителя информации. Например, это может быть механическое разрушение жесткого диска или использование магнитных полей для стирания информации. Важно правильно выбрать метод, чтобы убедиться в надежности удаления информации.

- Использование шифрования. Для защиты компьютерной информации от несанкционированного доступа можно применять методы шифрования. Шифрование позволяет превратить информацию в непонятный для посторонних вид, а доступ к ней получат только те, у кого есть ключ. Существует множество алгоритмов шифрования, таких как AES, RSA и другие. Необходимо выбрать подходящий алгоритм и правильно настроить шифрование, чтобы достичь максимального уровня защиты данных.

Ответы на типовые задания второй КР:

1.Уязвимости Windows.

- Недостаточная защита аккаунтов.

- Уязвимости в программном обеспечении.

- Незапланированные обновления.

2.Защитаоткопированияпереносныхносителей.

- Использование цифровых прав управления доступом.

- Физические меры защиты.

- Контроль доступа к данным.

Задание второй контрольной работы кратко:

1. Уязвимости Windows:

- Недостаточная защита аккаунтов: Возможность взлома аккаунтов на компьютерах под управлением Windows является одной из основных уязвимостей. Для защиты от этой уязвимости необходимо использовать сложные пароли, двухфакторную аутентификацию и ограничение прав доступа для пользователей.

- Уязвимости в программном обеспечении: Windows является популярной операционной системой, и множество программных продуктов сторонних разработчиков работает на ней. Некачественное программное обеспечение может содержать уязвимости, через которые злоумышленники могут получить несанкционированный доступ к компьютеру. Для устранения этой уязвимости рекомендуется использование только официального программного обеспечения и регулярное обновление всех установленных приложений.

- Незапланированные обновления: Некоторые уязвимости в Windows могут быть предотвращены путем применения обновлений операционной системы и установки последних патчей безопасности. Однако некоторые пользователи отключают автоматические обновления, что оставляет их компьютеры уязвимыми. Для защиты от этой уязвимости следует включить автоматические обновления и регулярно проверять наличие новых обновлений.

2. Защита от копирования переносных носителей:

- Использование цифровых прав управления доступом: Цифровые права управления доступом (DRM) предоставляют возможность ограничить копирование и распространение данных на переносных носителях. Это может быть реализовано через шифрование данных или применение специальных механизмов защиты, которые ограничивают доступ к данным только авторизованным пользователям.

- Физические меры защиты: Для защиты от копирования переносных носителей можно использовать физические меры, такие как использование прочных упаковок, специальных замков или маркировку, предупреждающую о запрете копирования. Это усложняет несанкционированное копирование данных и повышает уровень безопасности информации.

- Контроль доступа к данным: Для защиты от копирования переносных носителей рекомендуется ограничить доступ к данным только авторизованным пользователям. Это может быть достигнуто через применение паролей, шифрование данных или установку специальных программ и механизмов, которые контролируют доступ к информации. Кроме того, можно использовать системы управления правами доступа (Access Control Systems), чтобы определить, кто имеет

доступ к данным и каким образом они могут быть использованы.

Эти методы помогут защитить данные от уязвимостей Windows и от копирования на переносных носителях. Однако важно помнить, что безопасность - это постоянный и динамический процесс, и регулярное обновление и анализ уровня защиты являются неотъемлемой частью обеспечения безопасности компьютерных систем.

Ответы на типовые задания третьей КР:

Записать определения, описать: Информационное противоборство, Информационная преступность, Информационное воздействие, Информационное оружие, защита информации, утечка, разглашение, несанкционированный доступ, несанкционированное воздействие, цель и эффективность защиты информации, Конфиденциальность информации, Шифрованием информации, Целостностью информации, хеширование, доступность информации, Политика безопасности, аутентичность, контроль доступа, атака на информацию, Вредоносные программы, вирус, «троянский конь», атака «салями», загрузочные вирусы, макровирусы, «черви», «маскарад», «люки», «взлом» системы; описать алгоритм.

Информационное противоборство - это процесс, в рамках которого стороны стремятся получить преимущество в области информации и использовать ее в своих интересах. В рамках информационного противоборства могут проводиться различные операции, включая сбор, обработку, передачу и защиту информации.

Информационная преступность - это вид преступности, связанный с использованием информационных технологий и сетей. Включает в себя такие действия, как несанкционированный доступ к информации, уничтожение данных, мошенничество, киберскампания и другие формы преступной деятельности, связанные с использованием информационных технологий.

Информационное воздействие - это процесс воздействия на информацию с целью изменения ее восприятия, распространения определенных сообщений или манипуляции убеждениями и поведением людей. Информационное воздействие может использоваться в различных сферах, включая политику, рекламу, психологическую войну и киберспорт.

Информационное оружие - это инструмент или технология, используемая для атаки или защиты информации. Это может включать в себя программные и аппаратные средства, алгоритмы, методы шифрования и другие технические средства для манипулирования или защиты информации.

Защита информации - это комплекс мер, принимаемых для обеспечения конфиденциальности, целостности и доступности информации. Включает в себя такие меры, как шифрование данных, контроль доступа, мониторинг и обновление систем безопасности, обучение пользователей и другие процедуры и технические средства для защиты информации от несанкционированного доступа и использования.

Утечка - это непреднамеренное или преднамеренное раскрытие информации, которая должна быть конфиденциальной. Это может произойти из-за ошибок или уязвимостей в системе, ошибки пользователя или злонамеренных действий.

Разглашение - это осознанное раскрытие конфиденциальной информации без разрешения правообладателя. Может быть случайным или умышленным действием.

Несанкционированный доступ - это получение доступа к информации или ресурсам без соответствующих полномочий или разрешения. Может быть результатом хакерской атаки, использования украденных учетных данных или других методов нарушения безопасности.

Несанкционированное воздействие - это использование информационных технологий для нанесения вреда или манипуляции информацией или системами. Может включать в себя вредоносные программы, кибератаки, фишинг, социальную инженерию и другие методы.

Цель и эффективность защиты информации - основная цель защиты информации заключается в обеспечении конфиденциальности, целостности и доступности информации. Это достигается путем реализации соответствующих технических, организационных и процедурных мер. Если эти меры эффективны, то информация защищена от несанкционированного доступа, изменения или утраты.

Конфиденциальность информации - это свойство информации, которое

гарантирует ее ограниченный доступ только для авторизованных лиц или организаций. Она обеспечивается с использованием методов шифрования, контроля доступа и политик безопасности.

Шифрование информации - это процесс преобразования информации в зашифрованную форму, чтобы она стала непонятной и недоступной для неавторизованных пользователей. Шифрование обеспечивает конфиденциальность информации при передаче или хранении.

Целостность информации - это свойство информации, которое гарантирует ее неприкосновенность и неизменность. Оно обеспечивается защитой от несанкционированного изменения или модификации данных.

Хеширование - это процесс преобразования данных фиксированного размера (хеша) из произвольно большого объема информации. Хеш служит для проверки целостности данных, поскольку любое изменение входных данных приведет к изменению хеша.

Доступность информации - это свойство информации, которое гарантирует ее доступность для авторизованных пользователей в нужное время и месте. Для обеспечения доступности информации необходимо иметь надежные системы хранения, резервное копирование данных и мониторинг состояния систем.

Политика безопасности - это набор правил, процедур и механизмов, которые определяют правила доступа к информации, контроль мер безопасности и ответственность за нарушения. Политика безопасности включает в себя правила шифрования, уровни доступа, аутентификацию пользователей и другие меры безопасности.

Аутентичность - это свойство информации или объекта, которое гарантирует его истинность и подлинность. В контексте информационной безопасности аутентичность может быть обеспечена с помощью аутентификации пользователей, проверки цифровых подписей или других методов идентификации.

Контроль доступа - это процесс управления доступом к информации или системе. Включает в себя аутентификацию пользователей, авторизацию, установление прав доступа и механизмы контроля использования ресурсов.

Атака на информацию - это действие или серия действий, направленных на получение, изменение или уничтожение информации. Может быть различными формами атаки, такими как хакерские атаки, внедрение вредоносных программ, социальная инженерия и другие методы.

Вредоносные программы - это программы, разработанные с целью причинения вреда компьютерным системам или пользователем. Включает в себя вирусы, троянские кони, черви, маскарадные программы и другие формы вредоносного программного обеспечения.

Вирус - это тип вредоносной программы, которая способна размножаться и распространяться, заражая файлы или программы.

"Троянский конь" - это тип вредоносной программы, которая скрывается внутри полезной программы или файлового объекта и выполняет свои вредоносные действия без ведома пользователя.

Атака "салями" - это метод мошенничества, при котором атакующий, постепенно и незаметно, похищает или украшает небольшие кусочки информации или денежных средств с целью незаметного обогащения.

Загрузочные вирусы - это тип вредоносной программы, которая инфицирует секторы загрузочного раздела жесткого диска или мастер загрузочной записи (MBR) и запускается во время загрузки компьютера.

Макровирусы - это тип вредоносной программы, которая использует макрофункции в приложениях, чтобы выполнить свои вредоносные действия.

"Черви" - это тип вредоносной программы, которая распространяется по сетям и автоматически внедряется и выполняется на компьютерах без ведома пользователя.

"Маскарад" - это метод атаки, при котором злоумышленник представляется другим пользователем или системой с целью получения несанкционированного доступа к информации или ресурсам.

"Люки" - это слабые места в системе или программном обеспечении, через которые злоумышленник может получить несанкционированный доступ или выполнить атаку.

"Взлом" системы - это процесс незаконного проникновения в компьютерную систему с целью получения доступа к информации или использования ресурсов.

Алгоритм - это последовательность шагов или инструкций, определяющих порядок выполнения определенной операции или решения конкретной задачи. В контексте информационной безопасности алгоритмы используются для шифрования данных, аутентификации пользователей, контроля доступа и других операций, связанных с защитой информации.