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 2021

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 формы 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					
3.1 Знать: - основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства крипто-графической защиты информации; - современную классификацию средств защиты информации от несанкционированного доступа операционных систем и систем управления базами данных; технологию проектирования и создания безопасных информационных систем; - современную нормативно-правовую базу создания защищенных распределенных информационных систем; - 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; - конфигурировать и настраивать современные аппаратные средства защиты информационных процессов в компьютерных системах; - 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; - 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.

2.Методика устранения компьютерной информации.

Типовые задания второй КР:

1.Уязвимости Windows.

2.Защита от копирования переносных носителей.

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.

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».

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.

18. Приведите основные характеристики IP протоколов управления мобильностью.

19. Приведите основные характеристики протокола безопасности WEP.

20. Как осуществляется шифрование в протоколе WEP?

21. Существуют ли проблемы аутентификации при шифровании в протоколе WEP?

22. 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.

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

27. Алгоритм асимметричного шифрования Рабина

28. Криптосистема ЭльГемаля: структура, криптостойкость

29. Метод ключевого обмена Диффи-Хелмана

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

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

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

33. Генерация криптостойких случайных чисел.

34. Вероятностная генерация простых чисел для криптоалгоритмов.

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

36. Биометрические методы аутентификации пользователей

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

38. Система аутентификации по схеме «запрос-ответ»

39. Протокол аутентификации пользователей Kerberos

40. Угрозы безопасности в глобальных сетях

41. Межсетевые экраны: назначение, основные функции, состав

42. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки

43. Proxy-сервера: назначение, основные функции, достоинства и недостатки

44. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона

45. Обзор криптографических протоколов: SSL, TLS, IPSecurity, SSH, PPTP, L2TP

46. Средства аудита ОС семейства Windows

47. Модель безопасности ОС семейства Windows

48. Модель безопасности ОС Unix. Подсистема аудита ОС семейства Unix.

49. Вредоносные программы: определение, классификация

50. 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 2003.

14.Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа

ОС Windows Server 2003. 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 2003.

16.Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows XP. 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, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС Windows Server 2003 и Windows 2000.

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.

26. С помощью программы NetCrunch, постройте карту сети компьютерного класса.

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 виде зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.