

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
(НХТИ ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ



Заместитель директора по УР

Н.И. Никифорова

« 12 » 04 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине (модулю)

Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности

(код и наименование дисциплины (модуля))

09.03.02 «Информационные системы и технологии»

(код и наименование направления подготовки/специальности)

Системы информационной безопасности

(наименование профиля/специализации)

бакалавр

квалификация

форма обучения очная

(очная, очно-заочная, заочная)

Составитель ФОС:

Ст. преподаватель
(должность)


(подпись)

Захарова И.Н.
(Ф.И.О)

ФОС рассмотрен и одобрен на заседании кафедры ИСТ,
протокол от 15.03.2021 г. № 7

Зав. кафедрой


(подпись)

О.В. Матухина
(Ф.И.О.)

Эксперт:

Руководитель ООП



Л.Р. Вотякова

Ф.И.О., должность, организация, подпись

Перечень компетенций и индикаторов достижения компетенций с указанием этапов формирования в процессе освоения дисциплины

Компетенция:

ПК-2 Способен обеспечить информационную безопасность на уровне баз данных

ПК-2.1 Знает угрозы безопасности баз данных, способы предотвращения

ПК-2.2 Умеет выявлять угрозы безопасности на уровне баз данных

ПК-2.3 Владеет навыками применения способов предотвращения угроз безопасности на уровне баз данных

ПК-3 Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-3.1 Знает инструменты и методы проектирования архитектуры ИС, устройство, функционирование вычислительных систем и современных ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-3.2 Умеет проектировать архитектуру ИС, анализировать входную информацию, разрабатывать структуру баз данных, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-3.3 Владеет навыками проектирования архитектуры ИС, структуры баз данных, работы современных ИС, автоматизирующих задачи организационного управления и бизнес-процессы

<i>Индекс Компетенции</i>	<i>Этапы формирования компетенции (указать все темы из РПД)</i>				<i>Наименование оценочного средства</i>
	<i>Лекции</i>	<i>Практические Занятия, лабора- торный практи- кум</i>	<i>Лабораторные занятия</i>	<i>Курсовой проект (работа)</i>	
ПК-2.1	Тема 1--16	Не предусмотрены	Лаб.зан. 1-19	Тема 1--16	Реферат, Экзамен
ПК-2.2	-	Не предусмотрены	Лаб.зан. 1-19	Тема 1--16	Реферат, Экзамен
ПК-2.3	-	Не предусмотрены	Лаб.зан. 1-19	Тема 1--16	Реферат, Экзамен
ПК-3.1	Тема 1--16	Не предусмотрены	Лаб.зан. 1-19	Тема 1--16	Реферат, Экзамен
ПК-3.2	-	Не предусмотрены	Лаб.зан. 1-19	Тема 1--16	Реферат, Экзамен
ПК-3.3	-	Не предусмотрены	Лаб.зан. 1-19	Тема 1--16	Реферат, Экзамен

Перечень оценочных средств по дисциплине (модулю)

При оценке результатов деятельности обучающихся в рамках дисциплины Б1.В.06 Программно-аппаратные средства обеспечения информационной безопасности используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО «КНИТУ».

При изучении дисциплины предусматривается реферат, тестирование. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

За экзамен студент может получить минимум 24 балла и максимум – 40 баллов.

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Реферат	1	20	40
Тестирование	1	40	60
Итого:		60	100

При изучении дисциплины предусматривается выполнение курсовой работы. Студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Курсовая работа	1	60	100

Шкала оценивания

Цифровое выражение	Выражение в баллах:	Словесное выражение	Критерии оценки индикаторов достижения при форме контроля:
			экзамен
5	87 - 100	Отлично (зачтено)	Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий
4	74 - 86	Хорошо (зачтено)	Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

3	60 - 73	Удовлетворительно (зачтено)	Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.
2	Ниже 60	Неудовлетворительно (не зачтено)	Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Информационные технологии

Кафедра Информационных систем и технологий

Направление подготовки: 09.03.02 «Информационные системы и технологии»

Профиль: Системы информационной безопасности

Темы рефератов

Примерные темы:

1. Модель Кларка Вилсона
2. Модель «Китайская стена»
3. Модель Белла и Ла Падуллы
4. Модель Гогена-Мезигера
5. Сазерлендская модель
6. Дискреционная (матричная) модель
7. Модель Take-Grant
8. Модель типизированной матрицы доступа (Модель Харрисона-Руззо-Ульмана)
9. Модель Диона
10. Модель Биба
11. Ролевая политика

Критерии оценки реферата:

Структура реферата:

- 1) титульный лист;
- 2) план работы с указанием страниц каждого вопроса, подвопроса (пункта);
- 3) введение;
- 4) текстовое изложение материала, разбитое на вопросы и подвопросы (пункты, подпункты) с необходимыми ссылками на источники, использованные автором;
- 5) заключение;
- 6) список использованной литературы;

7) приложения, которые состоят из таблиц, диаграмм, графиков, рисунков, схем (необязательная часть реферата).

Приложения располагаются последовательно, согласно заголовкам, отражающим их содержание.

Реферат оценивается научным руководителем исходя из установленных кафедрой показателей и критериев оценки реферата.

Критерии и показатели, используемые при оценивании учебного реферата

Критерии	Показатели
1. Новизна реферированного текста Макс. - 3 балла	<ul style="list-style-type: none"> - актуальность проблемы и темы; - новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; - наличие авторской позиции, самостоятельность суждений.
2. Степень раскрытия сущности проблемы Макс. - 2 балла	<ul style="list-style-type: none"> - соответствие плана теме реферата; - соответствие содержания теме и плану реферата; - полнота и глубина раскрытия основных понятий проблемы; - обоснованность способов и методов работы с материалом; - умение работать с литературой, систематизировать и структурировать материал; - умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
3. Обоснованность выбора источников Макс. - 2 балла	<ul style="list-style-type: none"> - круг, полнота использования литературных источников по проблеме; - привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).
4. Соблюдение требований к оформлению Макс. - 1 балла	<ul style="list-style-type: none"> - правильное оформление ссылок на используемую литературу; - грамотность и культура изложения; - владение терминологией и понятийным аппаратом проблемы; - соблюдение требований к объему реферата; - культура оформления: выделение абзацев.
5. Грамотность Макс. - 1 балла	<ul style="list-style-type: none"> - отсутствие орфографических и синтаксических ошибок, стилистических погрешностей;

	<ul style="list-style-type: none"> - отсутствие опечаток, сокращений слов, кроме общепринятых; - литературный стиль.
6. Проверка на антиплагиат Макс.1 баллов	<ul style="list-style-type: none"> - проверка реферата в система антиплагиат. - должно быть не менее 70% оригинальности текста

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Информационные технологии

Кафедра Информационных систем и технологий

Направление подготовки: 09.03.02 «Информационные системы и технологии»

Профиль: Системы информационной безопасности

Примерные вопросы теста
по дисциплине Б1.В.06 Программно-аппаратные средства информационной безопасности

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Виды угроз информационной безопасности Российской Федерации.
8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации
10. Источники понятий в области информационной безопасности.
11. Основные понятия информационной безопасности.
12. Общеметодологические принципы теории информационной безопасности.
13. Понятие и сущность защищаемой информации.
14. Права и обязанности обладателя информации.
15. Виды защищаемой информации.
16. Перечень сведений конфиденциального характера.
17. Понятие интеллектуальной собственности и особенности ее защиты.
18. Понятие угрозы информационной безопасности.
19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
20. Классификация и виды угроз информационной безопасности.
21. Внутренние и внешние источники угроз информационной безопасности.
22. Угрозы утечки информации и угрозы несанкционированного доступа.

23. Основные элементы канала реализации угрозы безопасности информации.
24. Субъекты и цели информационного противоборства.
25. Составные части и методы информационного противоборства.
26. Информационное оружие, его классификация и возможности.
27. Методы нарушения конфиденциальности, целостности и доступности информации.
28. Информационное противоборство как способ воздействия на информационные системы.
29. Информационная безопасность критически важных объектов.
30. Обеспечение безопасности объектов информационной сферы государства в информационном противоборстве.
31. Компьютерная система как объект информационной безопасности.
32. Основные способы защиты информации.
33. Понятие и классификация средств защиты информации.
34. Характеристика средств защиты информации.
35. Уровни информационной безопасности и их характеристика.
36. Сервисы безопасности программно-технического уровня.
46. Назначение формальных моделей безопасности. Политика безопасности.
47. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.
48. Мандатная модель безопасности. Модель Белла-ЛаПадулы.
49. Формальные модели целостности.
50. Понятие ролевого управления доступом.

Примерный тест:

1) Возможность за приемлемое время получить требуемую информационную услугу называется:

1. Конфиденциальность
2. Доступность
3. Целостность
4. Непрерывность

Эталон ответа: b

2) К аспектам информационной безопасности не относится:

1. Доступность
2. Целостность
3. Конфиденциальность
4. Защищенность

Эталон ответа: d

3) По каким критериям нельзя классифицировать угрозы:

1. по расположению источника угроз
2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
3. по способу предотвращения
4. по компонентам информационных систем, на которые угрозы нацелены

Эталон ответа: с

4) Главное достоинство парольной аутентификации – ...

1. простота
2. надежность
3. секретность
4. запоминаемость

Эталон ответа: а

5) Сколько уровней включает в себя сетевая модель OSI?

1. 5
2. 7
3. 6
4. 8

Эталон ответа: b

6) Межсетевой экран (Брандмауэр, firewall) – это...

1. Комплекс аппаратных средств
2. Комплекс программных средств
3. Комплекс аппаратных или программных средств
4. Комплекс аппаратных и программных средств

Эталон ответа: с

7) На каком уровне сетевой модели OSI не работает межсетевой экран:

1. Физический
2. Сеансовый
3. Сетевой
4. Транспортный

Эталон ответа: а

8) Межсетевого экрана какого класса не существует:

1. экранирующий маршрутизатор
2. экранирующий коммутатор
3. экранирующий транспорт

4. экранирующий шлюз

Эталон ответа: b

9) Что из перечисленного не входит в состав программного комплекса антивирусной защиты:

1. Подсистема сканирования
2. Подсистема управления
3. Подсистема обнаружения вирусной активности
4. Подсистема устранения вирусной активности

Эталон ответа: d

10) На каком этапе заканчивается жизненный цикл автоматизированной системы?

1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

Эталон ответа: c

11) Какие задачи выполняет теория защиты информации:

1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
4. выполняет все вышеперечисленные

Эталон ответа: d

12) Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:

1. SSL
2. SET
3. HTTP
4. IPSec

Эталон ответа: c

13) Какого метода разграничения доступа не существует:

1. разграничение доступа по спискам
2. разграничение доступа по уровням секретности и категориям
3. локальное разграничение доступа
4. парольное разграничение доступа

Эталон ответа: с

14) К основным функциям подсистемы защиты операционной системы относятся:

1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

Эталон ответа: d

15) Риск – это...

1. вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки
2. фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки
3. действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
4. реализованная угроза

Эталон ответа: а

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Информационные технологии

Кафедра Информационных систем и технологий

Направление подготовки: 09.03.02 «Информационные системы и технологии»

Профиль: Системы информационной безопасности

Комплект заданий для курсовых работ
по дисциплине «Программно-аппаратные средства информационной безопасности»

Рекомендуемая тематика проекта

1. Дискреционная модель доступа к файлам
2. Мандатное управление доступом
3. Проверка целостности файлов
4. Программа для аутентификации с помощью usb-устройства
5. Аутентификация с использованием ключа eToken
6. Запрет запуска программ через приложение «Windows forms»
7. Разграничение доступа к принтерам
8. Разграничение доступа к устройствам. Флеш-накопители
9. Реализация асимметричного шифрования
10. Реализация симметричного шифрования
11. Расширение базовой системы аутентификации Windows
12. Программа для учета установленного ПО
13. Программа для учета установленного АО
14. Лабораторная работа «Защита конфиденциальной информации с помощью УКЗД “Криптон”»
15. Конфиденциальная работа с электронной почтой с использованием ruToken
16. Антифишинговый фильтр
17. Программный межсетевой экран (windows)
18. Программный межсетевой экран (linux)
19. Программное средство создания электронной подписи и цифровых сертификатов
20. Разработка защиты от программ слежения за набором на клавиатуре
21. Разработка ПО, защищенного от исследования
22. Разработка программной системы защиты от кражи ПК
23. Реализация системы аутентификации мобильного устройства
24. Разработка системы защиты от криптомайнеров
25. Разработка системы защиты от несанкционированного сканирования портов
26. Система для проведения аудита безопасности MySQL
27. Система для проведения аудита безопасности PostgreSQL
28. Аудит файлов в операционной системе Android
29. Аудит файлов в операционной системе iOS
30. Система DRM-защиты
31. Ограничение доступа к USB накопителям с применением шифрования
32. Защита от несанкционированного копирования программ
33. Антивирус на основе сигнатурного поиска

План проведения исследовательской работы

1. Выбор темы исследования.
2. Определение объекта и предмета исследования.
3. Определение цели и задач.
4. Формулировка названия работы.
5. Разработка гипотезы.
6. Составление плана исследования.
7. Литературный обзор и патентное исследование.
8. Выбор методов исследования.
9. Проведение исследования (сбор материала, исходного набора данных, определение условий и т.д.).
10. Обработка результатов исследования.
11. Формулирование выводов.
12. Оформление работы.

План проектирования и разработки ИТ, ИС, АС

1. Формирование требований.
2. Разработка концепции.
3. [Техническое задание](#).
4. [Эскизный проект](#).
5. [Технический проект](#).
6. Рабочее проектирование.
7. Оформление документации.
8. Ввод в действие.

Критерии оценки

	Тема контрольной точки	Вид контроля	Минимальное количество баллов	Максимальное количество баллов
	Управление проектом	Защита раздела курсовой работы	12	20
	Информационная модель	Защита раздела курсовой работы	12	20
	Математическое моделирование	Защита раздела курсовой работы	12	20
	Хранение, обработка и накопление данных	Защита раздела курсовой работы	12	20
	Обеспечение ИБ	Защита раздела курсовой работы	12	20
	Итого		60	100