

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.17 Методы и средства защиты информационных систем критичных
отраслей

(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 очно

(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

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

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-4 Способен администрировать сетевую подсистему инфокоммуникационной системы организации

ПК-4.1 Знает общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

ПК-4.2 Умеет использовать современные средства администрирования баз данных

ПК-4.3 Владеет навыками администрирования сетевой системы и программного обеспечения инфокоммуникационной системы

<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--8	Не предусмотрены	Лаб.зан. 1-7	Не предусмотрены	Экзамен, реферат
ПК-2.2	-	Не предусмотрены	Лаб.зан. 1-7	Не предусмотрены	Экзамен, реферат
ПК-2.3	-	Не предусмотрены	Лаб.зан. 1-7	Не предусмотрены	Экзамен, реферат
ПК-4.1	Тема 1--8	Не предусмотрены	Лаб.зан. 1-7	Не предусмотрены	Экзамен, реферат
ПК-4.2	-	Не предусмотрены	Лаб.зан. 1-7	Не предусмотрены	Экзамен, реферат
ПК-4.3	-	Не предусмотрены	Лаб.зан. 1-7	Не предусмотрены	Экзамен, реферат

Перечень оценочных средств по дисциплине (модулю)

При оценке результатов деятельности обучающихся в рамках дисциплины Б1.В.17 Методы и средства защиты информационных систем критичных отраслей 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 экзамен, реферат, выполнение двух расчётно-графических работ. 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	8	10
Промежуточное тестирование	1	28	50
Экзамен	1	24	40
Итого:		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

Варианты тем:

1. средства ИнфоТеКС для защиты АСУ КИИ
2. Средства VipNet Coordinator IG
3. Классификация АСУТП: требования, параметры, сроки. Категорирование объектов критической информационной инфраструктуры
4. Разработка модели угроз
5. Выбор мер защиты объектов информатизации
6. Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
7. Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры
8. Технические и организационные меры безопасности значимых объектов
9. Категории объектов критической информационной инфраструктуры

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; - 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

Примерные вопросы теста
по дисциплине Б1.В.07 Основы информационной безопасности

1. Какое из определений информационных технологий верно
 - а) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
 - б) приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных;
 - в) ресурсы, необходимые для сбора, обработки, хранения и распространения информации;
 - г) все перечисленное.
2. Безопасность информации
 - а) состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;
 - б) состояние при котором невозможно изменить информацию;
 - в) состояние обеспечивающее целостность и защищенность информации;
 - г) состояние при котором злоумышленник не может получить информацию.
3. Безопасность критической информационной инфраструктуры
 - а) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;
 - б) состояние защищенности, при котором обеспечены конфиденциальность, доступность и целостность информации;
 - в) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование
 - г) состояние обеспечивающее целостность и защищенность информации.
4. Доступ к информации
 - а) возможность получения информации и ее использования;
 - б) состояние доступности;
 - в) возможность проводить сбор, обработку и передачу информации
 - г) Возможность изменения информации
5. Значимый объект критической информационной инфраструктуры
 - а) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;
 - б) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;
 - в) информационно-телекоммуникационная сеть;

- г) автоматизированная система управления субъекта критической информационной инфраструктуры.
- 6. Объект критической информационной инфраструктуры
 - а) информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационной инфраструктуры;
 - б) автоматизированная система управления субъекта критической информационной инфраструктуры;
 - в) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;
 - г) который включен в реестр значимых объектов критической информационной инфраструктуры.
- 7. Субъекты критической информационной инфраструктуры
 - а) государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы;
 - б) информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности,
 - в) российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей; - все выше перечисленное.
- 8. Какой закон регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.
 - а) Федеральный закон от 26.07.2017 № 187ФЗ;
 - б) Приказ ФСБ России от 19.06.2019 № 281;
 - в) Приказ ФСТЭК России от 25 декабря 2017 г. № 239;
 - г) Постановление Правительства РФ от 8 февраля 2018 г. № 127.
- 9. Компьютерный инцидент
 - а) любое реальное или предполагаемое событие имеющее отношение к безопасности компьютерной системы или компьютерной сети;
 - б) атака на компьютерную систему;
 - в) изменение системы безопасности компьютерной сети;
 - г) событие изменяющее компьютерную систему.
- 10. Под ? понимается установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.
 - а) категоризацией;
 - б) идентификацией;

- в) установлением значимости;
- г) обеспечением безопасности.

Примерный перечень экзаменационных вопросов:

1. Состав технических мер по защите КИИ согласно приказу №239 ФСТЭК
2. Состав организационных мер по защите КИИ согласно приказу №239 ФСТЭК
3. Основные законы в сфере безопасности КИИ
4. Перечислите потенциальные сферы объектов КИИ, кратко охарактеризуйте их
5. Как определяются категории значимости объектов КИИ
6. Основные регуляторы объектов КИИ, их функции
7. Какая информация включается в реестр КИИ
8. Основные требования и последовательность реализаций требований к ИБ объекта КИИ
9. Классификация угроз безопасности объектов КИИ
10. Состав системы безопасности значимых объектов
11. Требования к средствам системы безопасности объектов КИИ
12. Виды угроз информационной безопасности Российской Федерации.
13. Источники угроз информационной безопасности Российской Федерации.
14. Внешние источники угроз.
15. Внутренние источники угроз.
16. Направления обеспечения информационной безопасности государства.
17. Проблемы региональной информационной безопасности
18. СЗИ от угроз нарушения конфиденциальности
19. СЗИ от угроз нарушения целостности
20. СЗИ от угроз нарушения доступности
21. Безопасность периметра сети
22. Защита рабочих станций