МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Чистопольский филиал «Восток»

(наименование института (факультета, филиала)

Кафедра компьютерных и телекоммуникационных систем

(наименование кафедры разработчика)

УТВЕРЖДЕНО:
Ученым советом КНИТУ-КАИ (в составе ОП ВО)

КОМПЛЕКТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

по дисциплине (модулю)

Б1.О.16 Защита информации

(индекс дисциплины по учебному плану, наименование дисциплины)

Чистополь 2023

Комплект оценочных материалов по дисциплине (модулю) разработан для обучающихся всех форм обучения по направлению подготовки (специальности):

Код и наименование направления подготовки (специальности)	Направленность (профиль, специализация, магистерская программа)
09.03.01 Информатика и вычислительная техника	Вычислительные машины, комплексы, системы и сети
	Автоматизированные системы обработки информации и управления

Разработчик(и):

Ефимова Юлия Викторовна, доцент, к.п.н.

Комплект оценочных материалов по дисциплине (модулю) рассмотрен на заседании кафедры КиТС, протокол № 8 от 26.05.2023г.

Заведующий кафедрой

Классен Виктор Иванович, д.т.н.

1 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля).

Промежуточная аттестация предназначена для оценки достижения запланированных результатов обучения по завершению изучения дисциплины (модуля) и позволяет оценить уровень и качество ее освоения обучающимися.

Комплект оценочных материалов представляет собой совокупность оценочных средств (комплекс заданий различного типа с ключами правильных ответов, включая критерии оценки), используемых при проведении оценочных процедур (текущего контроля, промежуточной аттестации) с целью оценивания достижения обучающимися результатов обучения по дисциплине (модулю).

1.1 Оценочные средства и балльные оценки для контрольных мероприятий

Таблица 1.1 – Объем дисциплины (модуля) для очной формы обучения

Семестр	Общая трудоемкость дисциплины (модуля), в з.е./час	*Виды учебной работы, в т.ч. проводимые с использованием ЭО и ДОТ*											
		Контактная работа обучающихся с преподавателем по видам учебной работы (аудиторная работа)							***Самостоятельная работа обучающегося (внеаудиторная работа)***				
		Лекции	Лабораторные работы	Практические занятия	Курсовая работа (консультация, защита)	Курсовой проект (консультации, защита)	Консультации перед экзаменом	Контактная работа на промежуточной аттестации	Курсовая работа (подготовка)	Курсовой проект (подготовка)	Проработка учебного материала (самоподготовка)	Подготовка к промежуточной аттестации	Форма промежуточной аттестации
8	2 ЗЕ/72	32	16	-	-	-	-	0,35	-	-	23,65	-	зачет
Итого	**2 ЗЕ/72**	**32**	**16**	**-**	**-**	**-**	**-**	**0,35**	**-**	**-**	**23,65**	**-**	

Текущий контроль успеваемости и промежуточная аттестация по дисциплине (модулю) осуществляется в соответствии с балльно-рейтинговой системой по 100-балльной шкале. Балльные оценки для контрольных мероприятий представлены в таблице 1.2. Пересчет суммы баллов в

традиционную оценку представлен в таблице 1.3.

Таблица 1.2 Балльные оценки для контрольных мероприятий

Наименование контрольного мероприятия	Максимальный балл на первую аттестацию	Максимальный балл за вторую аттестацию	Максимальный балл за третью аттестацию	Всего за семестр
8 семестр				
Тестирование	6	7	7	20
Выполнение лабораторной работы		15	15	30
Итого (максимум за период)	**6**	**22**	**22**	**50**
Зачет				**50**
Итого				**100**

Таблица 1.3 Шкала оценки на промежуточной аттестации

Выражение в баллах	Словесное выражение при форме промежуточной аттестации - зачет	Словесное выражение при форме промежуточной аттестации – экзамен, зачет с оценкой
от 86 до 100	Зачтено	Отлично
от 71 до 85	Зачтено	Хорошо
от 51 до 70	Зачтено	Удовлетворительно
до 51	Не зачтено	Неудовлетворительно

Форма и организация промежуточной аттестации по итогам освоения дисциплины – зачет, проводится два этапа: тестирование и устные ответы на экзаменационные вопросы.

1.2 Оценочные средства для проведения текущего контроля

1.2.1 Тестовые вопросы

Тестовые вопросы содержат следующие типы вопросов с соответствующим количеством баллов за правильный ответ:

Тип вопроса	Количество баллов за правильный ответ
запрос выбора вариантов ответа	1
запрос нескольких ответов	1 -при выборе всех правильных 0,5 – за 2 правильных из 3 0,25 – за 1 правильный из 3 0,5 – за 1 правильный из 2
запрос ввода пропущенного текста	1

1. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?

a. конфиденциальность +

b. доступность

c. целостность

d. аутентичность

2. Как называется состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?

a. конфиденциальность

b. доступность

c. целостность +

d. аутентичность

3. Как называется состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно?

a. конфиденциальность

b. доступность +

c. целостность

d. аутентичность

4. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?

a. атака

b. угроза +

c. уязвимость

d. слабое место системы

5. Как называется попытка реализации угрозы?

a. атака +

b. нападение

c. уязвимость

d. слабое место системы

6. Следствием наличия уязвимостей в информационной системе является:

a. угроза +

b. атака

c. нападение

d. необходимость замены компонентов системы

7. Какой уровень защиты информации представляет собой комплекс мер, применяемых руководством организации?

a. законодательный

b. процедурный

c. программно-технический

d. административный +

9. На каком уровне защиты информации находятся непосредственно средства защиты?

a. законодательный

b. процедурный

c. программно-технический +

d. административный

10. Совокупность содержащейся в базах данных информации, информационных технологий и технических средств, обеспечивающих ее обработку, называется:

a. система защиты информации

b. автоматизированная система идентификации

c. информационная система +

d. система обработки персональных данных

11. Персональные данные это:

a. любая информация, относящаяся к определенному, или определяемому на основании такой информации физическому лицу +

b. сведения (сообщения, данные) независимо от формы их представления

c. любая информация, касающаяся физиологических особенностей человека

d. информация, позволяющая связаться с человеком любым доступным способом

12. К какой категории персональных данных можно отнести адресную книгу?

a. биометрические

b. специальные

c. дополнительные

d. общедоступные +

13. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?

a. биометрические

b. специальные +

c. дополнительные

d. общедоступные

14. До начала обработки персональных данных оператор обязан:

a. получить письменное согласие субъекта персональных данных +

b. получить устное согласие субъекта персональных данных

c. уведомить регулятора о своем намерении в электронной форме

d. уведомить регулятора о своем намерении в устной форме

15. Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на:

a. субъекта персональных данных

b. оператора персональных данных +

c. доверенное лицо

d. администратора безопасности информационной системы персональных данных

16. Если в результате несанкционированного доступа персональные данные были уничтожены, оператор обязан:

a. уведомить об этом регулятора

b. уведомить об этом субъекта персональных данных

c. немедленно восстановить персональные данные +

d. произвести перенастройку средств защиты информации

17. Кто должен своевременно обнаруживать факты несанкционироанного доступа к персональным данным?

a. оператор персональных данных +

b. субъект персональных данных

c. регулятор

d. контролер

18. Кто такой инсайдер?

a. сотрудник являющийся источником утечки информации +

b. любой источник утечки информации

c. программа-вирус являющаяся источником утечки информации

d. сканер безопасности

19. Для чего создается реестр конфиденциальных документов?

a. для определения, какие документы являются конфиденциальными, какие сотрудники имеют доступ какого уровня к каким документам +

b. для классификации документов

c. для выполнения требований законов

d. для выполнения требований компании

20. Анализ защищенности информационных систем проводится с помощью:

a. межсетевых экранов

b. сканеров безопасности +

c. браузеров

d. команды ping

21. Электронные замки предназначены для:

a. хранения большого объема конфиденциальной информации

b. защиты периметра корпоративной сети

c. надежной аутентификации и идентификации пользователей +

d. блокирования компьютера во время отсутствия пользователя на рабочем месте

22. Наличие межсетевого экрана необходимо при:

a. использовании автономного автоматизированного рабочего места

b. использовании изолированной локальной сети

c. использовании сетей общего пользования +

d. использовании почтового ящика в сети Интернет

23. Свойства информации с точки зрения информационной безопасности

a. интерпретируемость, связность, активность

b. уязвимость, угроза, атака

c. полнота и непротиворечивость

d. целостность, конфиденциальность, доступность+

24. Расставьте в порядке логического следования событий в АСОИ

a. возникновение угрозы, наличие уязвимости, реализация атаки

b. наличие уязвимости, возникновение угрозы, реализация атаки+

c. реализация атаки, наличие уязвимости, возникновение угрозы

d. наличие уязвимости, реализация атаки, возникновение угрозы

25. К какой мере обеспечения информационной безопасности относится использование криптографических средств преобразования информации?

a. правовая

b. программно-аппаратная+

c. морально-этическая

d. организационно-административная

26. Что из перечисленного является верным?

a. субъект доступа – это пассивный компонент, который может стать причиной потока информации от субъекта к объекту или изменения состояния системы

b. субъект доступа – это активный компонент, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы+

c. объект доступа – это пассивный компонент системы, не хранящий, не принимающий и не передающий информацию

d. объект доступа – это активный компонент системы, хранящий, принимающий или передающий информацию

27. Какая угроза реализуется при атаке на чтение закрытой информации?

a. нарушение конфиденциальности информации+

b. нарушение доступности информации

c. нарушение целостности информации

d. нарушение работоспособности системы обработки информации

28. Что из перечисленного не является каналом утечки информации?

a. виброакустический канал

b. электромагнитный канал

c. визуальный канал

d. телевизионный канал

29. Нарушение какого принципа обеспечения ИБ может дать возможность злоумышленнику внедрить в АСОИ программную закладку?

a. принцип простоты применения защитных мер и средств

b. принцип открытости алгоритмов и механизмов защиты

c. принцип разумной достаточности

d. принцип непрерывности защиты+

30. Основная цель создания политики безопасности информационной системы

a. определить множество субъектов и объектов компьютерной системы

b. наделить полномочиями пользователей информационной системы

c. определить условия, которым подчиняется поведение подсистемы безопасности+

d. обеспечить целостность, конфиденциальность и доступность информации

9. Какая политика безопасности не обеспечивает конфиденциальность?

a. политика безопасности Хариссона-Руззо-Ульмана

b. политика безопасности Биба +

c. политика безопасности Белла-ЛаПадулы

d. мандатная политика безопасности

10. Какая политика безопасности контролирует целостность информации?

a. политика безопасности Белла-ЛаПадулы

b. политика безопасности Хариссона-Руззо-Ульмана

c. политика безопасности Биба+

d. дискреционная политика безопасности

11. Какая политика безопасности разрешает проблему программных закладок?

a. мандатная политика безопасности

b. дискреционная политика безопасности

c. политика безопасности Хариссона-Руззо-Ульмана

d. политика безопасности Белла-ЛаПадулы+

12. Какое из перечисленных определений является верным?

a. аутентификация – подтверждение принадлежности идентификатора пользователю+

b. авторизация – предъявление пользователем идентификатора для идентификации

c. верификация – наделение полномочиями субъекта системы

d. идентификация – подтверждение принадлежности аутентификатора пользователю

15. Для обеспечения конфиденциальности информации используется

a. декодирование

b. электронная цифровая подпись

c. шифрование+

d. цифровой сертификат

16. Что из перечисленного не может использоваться в системах биометрической идентификации/аутентификации пользователей?

a. рукописный почерк

b. клавиатурный почерк

c. мышиный почерк

d. мышиная задержка+

17. Какая из криптоаналитических атак требует привлечения предельных вычислительных ресурсов?

a. атака методом анализа частотности закрытого текста

b. атака по словарю

c. атака по открытому тексту

d. атака методом полного перебора всех возможных ключей+

18. Основной недостаток симметричной криптосистемы

a. проблема генерации ключевой информации

b. низкая скорость работы симметричных криптоалгоритмов

c. отсутствие эффективных алгоритмов симметричного шифрования

d. проблема хранения и распространения ключей шифрования+

19. На каком ключе происходит шифрование сообщения в асимметричной криптосистеме?

a. секретном

b. ассиметричном

c. открытом+

d. сообщение шифруется как на открытом, так и на секретном ключе (зависит от используемого алгоритма)

20. Реализация асимметричных криптосистем основана на использовании

a. однонаправленных функций+

b. свойств электронной цифровой подписи

c. функций хэширования

d. процедур идентификации и аутентификации отправителей сообщений

21. Понятие, не относящееся к свойствам функций хэширования

a. рассеивание

b. чувствительность к изменениям

c. открытость+

d. необратимость

22. Основное назначение электронных ключей HASP

a. использование в качестве идентификатора пользователя

b. защита программ от несанкционированного использования+

c. ограничение работы программ по времени

d. шифрование данных

23. Сниффинг – это:

a. Прослушивание каналов связи +

b. Нарушение работоспособности программных компонентов удаленных систем с целью дезорганизации их

c. Сканирование компьютерных сетей от вирусов

d. Получение прав доступа к удаленной системе, использующей нестойкие алгоритмы аутентификации пользователя

24. Атаки вида отказа в обслуживании – это :

a. Прослушивание каналов связи

b. Нарушение работоспособности программных компонентов удаленных систем с целью дезорганизации их +

c. Сканирование компьютерных сетей

d. Получение прав доступа к удаленной системе, использующей нестойкие алгоритмы аутентификации пользователя

e. Внедрение в системы и сети организаций разрушающих программных воздействий

25. Spoofing – это :

a. Прослушивание каналов связи

b. Нарушение работоспособности программных компонентов удаленных систем с целью дезорганизации их

c. Внедрение в системы и сети организаций разрушающих программных воздействий

d. Несанкционированный доступ пользователей к функциям системы, предоставляемым легальным пользователям+

27. Конфиденциальность информации - это

a. её свойство, обеспечивающее возможность эффективного шифрования

b. уровень её секретности, используемый для разграничения доступа

c. её свойство быть известной только допущённым и прошедшим проверку субъектам системы.+

d. возможность работы с ней только законным пользователям

28. Целостность информации - это

a. невозможность внесения в неё каких-либо изменений

b. её свойство быть неизменной в синтаксическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий

c. её свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.+

29. Доступность информации - это

a. её свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов.+

b. когда информация опубликована на общедоступном ресурсе

c. её свойство быть доступной для любых субъектов системы

d. возможность реализации криптоаналитической атаки без знания ключа шифрования

30. Потенциальная возможность нанесения ущерба системе обработки информации называется

a. разрушительным воздействием на систему обработки информации

b. угрозой информационной безопасности.+

c. каналом несанкционированного доступа к информации

d. атакой на систему обработки информации

31. Неудачное свойство системы, делающее возможным возникновение и реализацию угрозы информационной безопасности, называется

a. слабым звеном системы

b. минимальным уровнем безопасности системы обработки информации

c. атакой

d. уязвимостью.+

32. Непосредственная реализация угрозы называется

a. несанкционированным доступом

b. атакой.+

c. принципом недостаточности средств защиты

d. нарушением безопасности информации

34. Совокупность норм, правил и практических рекомендаций, регламентирующих процесс обработки информации, выполнение которых обеспечивает за-щиту от заданного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности компьютерной системы называется

a. регламентом безопасности системы обработки информации

b. политикой безопасности.+

c. нулевым кольцом защиты информации

d. основополагающим принципом информационной безопасности

35. Примером какой модели является политика безопасности Харрисона-Руззо-Ульмана?

a. мандатной

b. дискреционной.

c. ролевой

d. смешанной

36. Примером какой модели является политика безопасности Белла-ЛаПадулы?

a. мандатной.+

b. избирательного разграничения доступа

c. ролевой

d. дискреционной

37. Наиболее распространённые системы идентификации/аутентификации

a. на основе индивидуальных биометрических характеристик пользователя

b. парольные+

c. с использованием технических устройств

d. на основе HASP

38. Реализация асимметричных криптосистем основана на использовании

a. однонаправленных функций+

b. свойств электронной цифровой подписи

c. функций хэширования

d. процедур идентификации и аутентификации отправителей секретных сообщений

39. Что из перечисленного не является примером однонаправленной функции

a. целочисленное умножение

b. дискретное логорифмирование

c. сложение по модулю+

d. модульная экспонента

e. факторизация больших чисел

40. Понятие, не относящееся к свойствам функций хэширования

a. рассеивание

b. чувствительность к изменениям

c. открытость+

d. необратимость

41. Электронная цифровая подпись предназначена для

a. обеспечения целостности и конфиденциальности передаваемого сообщения

b. обеспечения целостности передаваемого сообщения и подтверждения его авторства+

c. реализации асимметричного криптографического обмена сообщениями

d. идентификации текстов, передаваемых по открытым каналам связи

42. Дайджест сообщения - это

a. зашифрованный хэш-образ документа

b. часть рассеянного значения хэш-функции

c. результат хэширования данного сообщения+

d. краткое изложение сообщения

43. Основной и наиболее простой способ защиты ПО с помощью ключей HASP

a. использование пароля доступа к ключу HASP

b. использование пристыковочного мехонизма+

c. анализ значений, возвращаемых функцией отклика

d. использование API-функций HASP

44. Принцип разделения обязанностей требует:

a. контроль каналов передачи информации и средств защиты

b. передавать критически важные функции людям с различными ролями в организации+

c. установки исправлений системы безопасности по мере их выхода и подержания параметров настройки системы безопасности в актуальном состоянии

d. защита должна быть ненавязчивой и необременительной для пользователей, чтобы не вызвать их противодействие

45. Принцип минимальной уязвимости гласит:

a. сведя к минимуму возможность для атаки, удастся обойтись минимальной защитой, а значит, и свести к минимуму вероятность взлома защиты сети

b. защита должна быть ненавязчивой и необременительной для пользовате-лей, чтобы не вызвать их противодействие

c. установки исправлений системы безопасности по мере их выхода и подержания параметров настройки системы безопасности в актуальном состоянии

в. минимизации прав и привилегий пользователей и доступ только к абсолютно необходимым данным+

46. Принцип актуальности требует:

a. установки исправлений системы безопасности по мере их выхода и подержания параметров настройки системы безопасности в актуальном состоянии+

b. передавать критически важные функции людям с различными ролями в организации

c. минимизации прав и привилегий пользователей и доступ только к абсолютно необходимым данным

d. защита должна быть ненавязчивой и необременительной для пользователей, чтобы не вызвать их противодействие

47. Инсайдеры – это:

a. легитимные сотрудники организации, имеющие определенный доступ к КИС+

b. нарушители из внешних сетей по отношению к рассматриваемой, которые атакуют внутренние ресурсы корпоративной сети

c. легитимные сотрудники организации, пытающиеся получить определенный доступ к КИС

d. нарушители из внешних сетей по отношению к рассматриваемой, которые атакуют внешние ресурсы корпоративной сети

48. Аутсайдеры – это:

a. легитимные сотрудники организации, имеющие определенный доступ к КИС

b. нарушители из внешних сетей по отношению к рассматриваемой, которые атакуют внутренние ресурсы корпоративной сети+

c. легитимные сотрудники организации, пытающиеся получить определенный доступ к КИС

d. нарушители из внешних сетей по отношению к рассматриваемой, которые атакуют внешние ресурсы корпоративной сети

49. Атаки вида отказа в обслуживании – это :

a. Нарушение работоспособности программных компонентов удаленных систем с целью дезорганизации их +

b. Прослушивание каналов связи

c. Сканирование компьютерных сетей

d. Внедрение в системы и сети организаций разрушающих программных воздействий

50. Информационная система – это:

a. программа, которая использует информационные ресурсы

b. взаимосвязанная совокупность сетей, служб передачи данных и теле-служб, предназначенная для предоставления единого защищенного сетевого пространства ограниченному рамками организации кругу пользователей+

c. любая система или программа, которая использует информационные ресурсы для удовлетворения нужд собственника или пользователя системы

d. взаимосвязанная совокупность сетей, служб передачи данных и теле-служб, предназначенная для предоставления единого защищенного сетевого пространства неограниченному кругу пользователей

1.2.2 Выполнение лабораторных работ

Перечень лабораторных работ и система оценивания:

Семестр	Наименование лабораторной работы	Кол-во баллов	Критерии оценивания
8	Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты	6-5	Проведены необходимые опыты и измерения; самостоятельно и рационально выбрано необходимое оборудование; все опыты проведены в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдены требования правил безопасности труда; в отчете правильно и аккуратно выполнены все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполнен анализ погрешностей.
		4	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы.
		3	Работа выполнена полностью. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы.
		2	Работа выполнена полностью. Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных

			суждений, допускает ошибки при ответе на дополнительные вопросы.
		0-1	Работа выполнена полностью. Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.
8	Реализация политик информационной безопасности. Дискреционная модель политики безопасности	6-5	Проведены необходимые опыты и измерения; самостоятельно и рационально выбрано необходимое оборудование; все опыты проведены в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдены требования правил безопасности труда; в отчете правильно и аккуратно выполнены все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполнен анализ погрешностей.
		4	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы.
		3	Работа выполнена полностью. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы.
		2	Работа выполнена полностью. Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы.
		0-1	Работа выполнена полностью. Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.
8	Мандатные политики безопасности. Политика безопасности Белла-	6-5	Проведены необходимые опыты и измерения; самостоятельно и рационально выбрано необходимое оборудование; все опыты проведены в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдены

	ЛаПадулы		требования правил безопасности труда; в отчете правильно и аккуратно выполнены все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполнен анализ погрешностей.
		4	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы.
		3	Работа выполнена полностью. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы.
		2	Работа выполнена полностью. Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы.
		0-1	Работа выполнена полностью. Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.
8	Методы криптографической защиты информации Простейшие алгоритмы шифрования	6-5	Проведены необходимые опыты и измерения; самостоятельно и рационально выбрано необходимое оборудование; все опыты проведены в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдены требования правил безопасности труда; в отчете правильно и аккуратно выполнены все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполнен анализ погрешностей.
		4	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы.
		3	Работа выполнена полностью.

			Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы.
		2	Работа выполнена полностью. Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы.
		0-1	Работа выполнена полностью. Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.
8	Защита сетей с применением межсетевых экранов Настройка брандмауэра в Windows	6-5	Проведены необходимые опыты и измерения; самостоятельно и рационально выбрано необходимое оборудование; все опыты проведены в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдены требования правил безопасности труда; в отчете правильно и аккуратно выполнены все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполнен анализ погрешностей.
		4	Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы.
		3	Работа выполнена полностью. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, отсутствуют ошибки при описании теории, испытывает затруднения в формулировке собственных обоснованных и аргументированных суждений, допуская незначительные ошибки на дополнительные вопросы.
		2	Работа выполнена полностью. Обучающийся практически не владеет теоретическим материалом, допуская ошибки по сущности рассматриваемых (обсуждаемых) вопросов, испытывает затруднения в формулировке собственных

			обоснованных и аргументированных суждений, допускает ошибки при ответе на дополнительные вопросы.
		0-1	Работа выполнена полностью. Обучающийся не владеет теоретическим материалом, допуская грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на дополнительные вопросы.

1.2.3 Курсовая работа

Не предусмотрено учебным планом.

1.3. Оценочные средства для проведения промежуточного контроля (промежуточной аттестации)

Семестр	Вид промежуточной аттестации	Вид контрольного мероприятия	Балльные оценки
8	зачет	Тестовые задания Экзаменационные вопросы	0-20 0-30

1.3.1. Тестовые задания

Тестовые задания промежуточной аттестации представляют собой совокупность тестовых вопросов текущего контроля.

1.3.2 Комплексное задание (экзаменационный билет)

Билеты зачета равноценны по трудности, одинаковы по структуре, параллельны по расположению заданий. Комплексное экзаменационное задание состоит из 2 вопросов теоретического характера. Теоретические вопросы направлены на проверку знаний.

1.3.2.1 Вопросы на зачете/экзамене (экзаменационные вопросы)

№ п/п	Тип вопроса	Вопрос
1	Теоретический	Принципы и меры обеспечения информационной безопасности в АСОИ
2		Шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию
3		Иерархия ключевой информации. Типовые схемы хранения ключевой информации
4		Подходы к распределению ключевой информации
5		Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования
6		Протоколы безопасной удаленной аутентификации пользователей
7		Шифрование методом замены. Примеры шифров замены
8		Шифрование методами перестановки. Примеры шифров перестановки
9		Проблема защиты программного обеспечения от несанкционированного использования
10		Политика безопасности контроля целостности информации (модель Биба)
11		Современные симметричные системы шифрования (на примере DES

		и ГОСТ)
12		Электронные ключи HASP. Инфраструктура открытых ключей PKI
13		Понятие политики безопасности и их классификация. Мандатные политики безопасности (модель Белла-ЛаПадуллы)
14		Принципы симметричного шифрования. Примеры простейших симметричных шифров
15		Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя
16		Идентификация и аутентификация пользователей с использованием технических устройств
17		Парольные системы идентификации и аутентификации пользователей
18		Понятие идентификации и аутентификации субъектов. Классификация подсистем идентификации и аутентификации
19		Понятие политики безопасности и их классификация. Политики избирательного разграничения доступа (модель Харрисона-Руззо-Ульмана)
20		Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей
21		Функции хэширования и электронно-цифровая подпись
22		Недостатки симметричных криптосистем. Принципы асимметричного шифрования
23		Комбинированный метод шифрования и его достоинства

Критерии оценивания

Суммарно оцениваются ответы на вопросы. Ответы должны быть развернутыми, полными. Каждый правильный ответ на вопрос оценивается до 15 баллов в зависимости от полноты ответа.

Оценивается полнота раскрытия материала; логичность изложения материала; умение иллюстрировать конкретными примерами; знание формул, терминологии, обозначений; использование профессиональной терминологии; демонстрация усвоенного ранее материала; самостоятельность в изложении материала.

Пример балльной системы оценивания:

Критерии оценивания	Количество баллов
– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов; – ответ дан самостоятельно, без наводящих вопросов; – продемонстрирована способность творчески применять знание теории к решению профессиональных задач;– допущены одна-две неточности	10-15

при освещении второстепенных вопросов, которые исправляются по замечанию;	
– вопросы излагаются систематизировано и последовательно; – продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; – продемонстрировано усвоение основной литературы; – ответ удовлетворяет в основном требованию на максимальную оценку, но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие содержание ответа; допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; – допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя;	7-9
– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – усвоены основные категории по рассматриваемому и дополнительным вопросам; – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих ответов; – неполное знание теоретического материала, обучающийся не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы;	4-6
– не раскрыто основное содержание учебного материала либо отказ от ответа; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, некоторые не исправлены после нескольких наводящих вопросов.	1-3
-ответ не получен.	0

Пример балльной системы оценивания вопросов:

Задание	Критерии оценивания	Количество баллов
Теоретический вопрос	– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов; – допущены одна-две неточности при освещении второстепенных вопросов, которые исправляются по замечанию;	0-15