Приложение А

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Основы информационной безопасности»

Уровень образования **бакалавриат**
(бакалавриат/магистратура/специалитет)

Направление **10.03.01 Информационная безопасность**
(код, наименование направления)

Профиль **Безопасность автоматизированных систем**
(наименование)

Разработчик ____________ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол № 2

Зав. кафедрой ____________ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Основы информационной безопасности» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению 10.03.01 Информационная безопасность.

Рабочей программой дисциплины «Основы информационной безопасности» предусмотрено формирование следующих компетенций:

ОПК – 1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)

- *Устный опрос*
- *Вопросы для проведения зачета*

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	**Код и наименование индикатора достижения формируемой компетенции**	**Критерии оценивания**	**Наименование контролируемых разделов и тем1**
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации	знает источники и классификацию угроз информационной безопасности; знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации	№№1-9
	ОПК-1.2. Умеет классифицировать и оценивать угрозы информационной безопасности		
	ОПК-1.3. Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире		

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Основы информационной безопасности определяется на следующих этапах:

1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2)*

2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности,	ОПК-1.1.1 - знает понятия информации и информационной безопасности	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	реферат	-	Вопросы для проведения экзамена
	ОПК-1.1.2 - знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики						
	ОПК-1.1.3 - знает источники и классификацию угроз информационной безопасности						

общества и государства	ОПК-1.2.1 умеет классифицировать угрозы информационной безопасности						

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины Основы информационной безопасности является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно», «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

3.1. Задания и вопросы для входного контроля

1. Информация, информационное общество, информационная среда.
2. Личность, общество, государство.
3. Информационный строй.
4. Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи.
5. Национальные интересы Российской Федерации в информационной сфере.
6. Приоритетные направления в области защиты информации в Российской Федерации

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Определение понятия "информационная безопасность"
2. Доступность ,целостность и конфиденциальность информации
3. Задачи информационной безопасности общества.
4. Уровни формирования режима информационной безопасности
5. Правовые основы информационной безопасности общества
6. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации
7. Ответственность за нарушения в сфере информационной безопасности
8. Стандарты информационной безопасности: "Общие критерии"
9. Стандарты информационной безопасности распределенных систем
10. Стандарты информационной безопасности в РФ.
11. Цели, задачи и содержание административного уровня.
12. Разработка политики информационной безопасности.

3.2.2. Аттестационная контрольная работа №2

1. Классы угроз информационной безопасности
2. Каналы несанкционированного доступа к информации
3. Компьютерные вирусы и информационная безопасность.
4. Характерные черты компьютерных вирусов
5. Классификация компьютерных вирусов по среде обитания.
6. Классификация компьютерных вирусов по особенностям алгоритма работы.
7. Классификация компьютерных вирусов по деструктивные возможностям
8. Виды "вирусоподобных" программ.
9. Характеристика "вирусоподобных" программ Государственное экономическое регулирование. Объекты и цели ГРЭ
10. Утилиты скрытого администрирования
11. "Intended"-вирусы.
12. Особенности работы антивирусных программ. Классификация антивирусных программ
13. Факторы, определяющие качество антивирусных программ.

3.2.3. Аттестационная контрольная работа №3

14. Харак Характеристика путей проникновения вирусов в компьютеры
15. Правила защиты от компьютерных вирусов
16. Обнаружение загрузочногоирезидентного вируса,макровируса

17. Общий алгоритм обнаружения вируса
18. Сетевые модели передачи данных.
19. Модель взаимодействия открытых систем OSI/ISO
20. Особенности обеспечения информационной безопасности в компьютерных сетях
21. Адресация в глобальных сетях.
22. Принципы защиты распределенных вычислительных сетей
23. Классификация удаленных угроз в вычислительных сетях
24. Типовые удаленные атаки и их характеристика
25. Причины успешной реализации удаленных угроз в вычислительных сетях
26. Технология виртуальных частных сетей (VPN)
27. Идентификация и аутентификация
28. Криптография и шифрование
29. Методы разграничение доступа
30. Регистрация и аудит
31. Межсетевое экранирование

Оценочные средства для проведения итоговой формы контроля

Примерные тестовые вопросы

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- a) Разработка аппаратных средств обеспечения правовых данных
- b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- a) Хищение жестких дисков, подключение к сети, инсайдерство
- b) Перехват данных, хищение данных, изменение архитектуры системы
- c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- a) Персональная, корпоративная, государственная
- b) Клиентская, серверная, сетевая
- c) Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- a) несанкционированного доступа, воздействия в сети
- b) инсайдерства в организации
- c) чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- a) Компьютерные сети, базы данных
- b) Информационные системы, психологическое состояние пользователей
- c) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- a) Искажение, уменьшение объема, перекодировка информации
- b) Техническое вмешательство, выведение из строя оборудования сети
- c) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- a) Экономической эффективности системы безопасности
- b) Многоплатформенной реализации системы
- c) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- a) руководители, менеджеры, администраторы компаний
- b) органы права, государства, бизнеса
- c) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- a) Установление регламента, аудит системы, выявление рисков
- b) Установка новых офисных приложений, смена хостинг-компании

c) Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

a) Неоправданных ограничений при работе в сети (системе)
b) Рисков безопасности сети, системы
c) Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

a) Невозможности миновать защитные средства сети (системы)
b) Усиления основного звена сети, системы
c) Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

a) Усиления защищенности самого незащищенного звена сети (системы)
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b) Одноуровневой защиты сети, системы
c) Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

a) Компьютерный сбой
b) Логические закладки («мины»)
c) Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

a) Прочитать приложение, если оно не содержит ничего ценного – удалить
b) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
c) Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

a) Секретность ключа определена секретностью открытого сообщения
b) Секретность информации определена скоростью передачи данных
c) Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

a) Электронно-цифровой преобразователь
b) Электронно-цифровая подпись
c) Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

a) Покупка нелицензионного ПО
b) Ошибки эксплуатации и неумышленного изменения режима работы системы
c) Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

a) Распределенный доступ клиент, отказ оборудования
b) Моральный износ сети, инсайдерство
c) Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

a) Слабый трафик, информационный обман, вирусы в интернет
b) Вирусы в сети, логические мины (закладки), информационный перехват
c) Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) Целостность
b) Доступность
c) Актуальность!

23) Угроза информационной системе (компьютерной сети) – это:

a) Вероятное событие
b) Детерминированное (всегда определенное) событие
c) Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

a) - Регламентированной
b) - Правовой
c) + Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

a) Программные, технические, организационные, технологические
b) Серверные, клиентские, спутниковые, наземные
c) Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

a) Владелец сети
b) Администратор сети
c) Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

a) Руководств, требований обеспечения необходимого уровня безопасности
b) Инструкций, алгоритмов поведения пользователя в сети
c) Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

a) Аудит, анализ затрат на проведение защитных мер
b) Аудит, анализ безопасности
c) Аудит, анализ уязвимостей, риск-ситуаций

29) Основная масса угроз информационной безопасности приходится на:

a) Троянские программы +
b) Шпионские программы
c) Черви

30. Какой вид идентификации и аутентификации получил наибольшее распространение:

a) системы PKI
b) постоянные пароли +
c) одноразовые пароли

31) Под какие системы распространение вирусов происходит наиболее динамично:

a) Windows
b) Mac OS
c) Android

32) Заключительным этапом построения системы защиты является:

a) сопровождение
b) планирование
c) анализ уязвимых мест

33) Какие угрозы безопасности информации являются преднамеренными:

a) ошибки персонала
b) открытие электронного письма, содержащего вирус
c) не авторизованный доступ

34) Какой подход к обеспечению безопасности имеет место:

a) теоретический
b) комплексный
c) логический

35) Системой криптографической защиты информации является:

a) BFox Pro
b) CAudit Pro
c) Крипто Про

36) Какие вирусы активизируются в самом начале работы с операционной системой:

a) загрузочные вирусы
b) троянцы
c) черви

37) Stuxnet — это:

a) троянская программа
b) макровирус
c) промышленный вирус

38) Таргетированная атака — это:

a) атака на сетевое оборудование
b) атака на компьютерную систему крупного предприятия
c) атака на конкретный компьютер пользователя

39) Под информационной безопасностью понимается:

a) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
b) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
c) нет верного ответа

40) Защита информации:

a) небольшая программа для выполнения определенной задачи
b) комплекс мероприятий, направленных на обеспечение информационной безопасности
c) процесс разработки структуры базы данных в соответствии с требованиями пользователей

41) Информационная безопасность зависит от:

a) компьютеров, поддерживающей инфраструктуры
b) пользователей
c) информации

42) Конфиденциальностью называется:

a) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
b) описание процедур
c) защита от несанкционированного доступа к информации

43) Для чего создаются информационные системы:

a) получения определенных информационных услуг
b) обработки информации
c) оба варианта верны

Ключи

1. c
2. b
3. a
4. a
5. a
6. c
7. a
8. b
9. a
10.a
11.a
12.a
13.a
14.b
15.c
16.c
17.b
18.b
19.c
20.b
21.a
22.a
23.a
24.c
25.a
26.a
27.a
28.c
29.a
30.b
31.c
32.a
33.c
34.b
35.c
36.a
37.c
38.b
39.a
40.b
41.a
42.c
43.a

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.