



Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Государственный университет морского и речного флота
имени адмирала С.О. Макарова»**
Воронежский филиал ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

Кафедра математики, информационных систем и технологий

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Основы информационной безопасности»
(приложение к рабочей программе дисциплины)

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) Информационные системы на транспорте

Уровень высшего образования бакалавриат

Форма обучения очная, заочная

Воронеж
2025

1. Перечень компетенций и этапы их формирования в процессе освоения дисциплины

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Таблица 1

Планируемые результаты обучения по дисциплине

Код и наименование компетенции	Код индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2 Решение стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности	Знать: виды угрозы и основные требования информационной безопасности Уметь: определять виды угроз и выбирать способы защиты от информационных угроз Владеть: навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности

2. Паспорт фонда оценочных средств для проведения текущей и промежуточной аттестации обучающихся

Таблица 2

Оценочные средства для проведения текущей и промежуточной аттестации обучающихся

№ п/п	Наименование раздела (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Информационная безопасность и уровни ее обеспечения.	ОПК-3	Тестирование, зачет
2	Компьютерные вирусы и защита от них.	ОПК-3	Тестирование, зачет
3	Информационная безопасность вычислительных сетей. Информационная безопасность при использовании Internet.	ОПК-3	Тестирование, РГР, зачет
4	Механизмы обеспечения "информационной безопасности".	ОПК-3	Тестирование, РГР, зачет
5	Безопасность операционных систем.	ОПК-3	Тестирование, РГР, зачет

Таблица 3

Критерии оценивания результата обучения по дисциплине и шкала оценивания по дисциплине

Результат обучения по дисциплине	Критерии оценивания результата обучения по дисциплине и шкала оценивания по дисциплине				Процедура оценивания
	2	3	4	5	
	Не зачтено	Зачтено			
ОПК-3.2 Знать: виды угрозы и основные требования информационной безопасности	Отсутствие или фрагментарные представления о видах угроз и основных требованиях информационно й безопасности	Неполные представления о видах угроз и основных требованиях информационно й безопасности	Сформированные, но содержащие отдельные пробелы представления о видах угроз и основных требованиях информационной безопасности	Сформированн ые систематическ ие представления о видах угроз и основных требованиях информацион ной безопасности.	Тестирование, зачет
ОПК-3.2 Уметь: определять виды угроз и выбирать способы защиты от информационных угроз	Отсутствие умений определять виды угроз и выбирать способы защиты от информационны х угроз.	В целом удовлетворител ьные, но не систематизиро ванные умения определять виды угроз и выбирать способы защиты от информационны х угроз..	В целом удовлетворитель ные, но содержащие отдельные пробелы умения определять виды угроз и выбирать способы защиты от информационных угроз.	Сформированн ые умения определять виды угроз и выбирать способы защиты от информацион ных угроз.	Тестирование, РГР, зачет
ОПК-3.2 Владеть: навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности	Отсутствие владения или фрагментарные владения навыками решения стандартных задач профессиональн ой деятельности с учетом основных требований информационно й безопасности	В целом удовлетворител ьные, но не систематизиро ванные владения навыками решения стандартных задач профессиональн ой деятельности с учетом основных требований информационно й безопасности.	В целом удовлетворитель ные, но содержащие отдельные пробелы владения навыками решения стандартных задач профессионально й деятельности с учетом основных требований информационной безопасности	Сформированн ые владения навыками решения стандартных задач профессионал ьной деятельности с учетом основных требований информацион ной безопасности.	Тестирование, РГР, зачет

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

Тестовые задания для проведения текущего контроля

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

- + Экономической эффективности системы безопасности

- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компания
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

- + Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

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

12) Принципом политики информационной безопасности является принцип:

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

13) Принципом политики информационной безопасности является принцип:

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

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

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

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

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

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- + Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
- + Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелегального ПО
- + Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- + Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

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

21) Утечкой информации в системе называется ситуация, характеризующаяся:

- + Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

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

- + Целостность
- Доступность
- Актуальность

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

- + Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

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

- Регламентированной
- Правовой
- + Защищаемой

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

- + Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

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

- + Владелец сети
- Администратор сети
- Пользователь сети

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

- + Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

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

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- + Аудит, анализ уязвимостей, риск-ситуаций

Таблица 4

Показатели и шкала оценивания тестовых заданий

Текущая аттестация	Количество баллов	Шкала оценивания
выполнение требований по текущей аттестации в полном объеме	90% - 100%	зачтено
	80% - 89%	
	60% - 79%	
невыполнение требований по текущей аттестации	менее 60%	не зачтено

Расчетно-графическая работа (задание)

Текущий контроль по дисциплине проводится в форме расчетно-графической работы (задания).

1. Криптография и шифрование

1. Сравнение скорости шифрования AES-256 vs RSA-2048 vs ECC-384 (график зависимости времени от размера файла)
2. Расчет стойкости пароля к brute-force (график времени взлома в зависимости от длины/сложности)

3. Анализ уязвимости устаревших протоколов (SSL 3.0 vs TLS 1.3 – диаграммы успешных атак)

2. Защита сетей

4. Оптимизация правил межсетевого экрана (график снижения нагрузки при фильтрации пакетов)
5. Расчет эффективности IDS/IPS (количество ложных срабатываний vs реальных угроз)
6. Моделирование DDoS-атаки и защитных механизмов (график нагрузки на канал)

3. Управление доступом

7. Сравнение методов аутентификации (пароль, 2FA, биометрия – диаграммы надежности)
8. Анализ рисков RBAC-модели (матрица прав доступа с оценкой уязвимостей)
9. Расчет времени блокировки учетной записи при brute-force (график зависимости от настроек политики)

4. Безопасность ОС и ПО

10. Оценка уязвимостей Windows vs Linux (диаграмма CVE-базы за год)
11. Анализ эффективности антивирусов (график обнаружения угроз для разных решений)
12. Расчет времени установки критических обновлений (моделирование «окна уязвимости»)

5. Социальная инженерия

13. Статистика успешных фишинговых атак (график кликабельности в зависимости от типа письма)
14. Эффективность обучения сотрудников (сравнение количества инцидентов до/after тренинга)

6. Юридические аспекты

15. Сравнение штрафов за нарушения GDPR и 152-ФЗ (инфографика по странам/компаниям)

Критерии оценивания:

- полнота и правильность ответа;
- степень осознанности, понимания изученного;
- языковое оформление ответа.

Таблица 5

Показатели и шкала оценивания выполнения
расчетно-графической работы (задания)

Оценка	Показатели
5	– Содержание ответа в целом соответствует теме задания. Продемонстрировано

	знание фактического материала, отсутствуют фактические ошибки. – Продемонстрировано уверенное владение понятийно-терминологическим аппаратом дисциплины (уместность употребления, аббревиатуры, толкование и т.д.), отсутствуют ошибки в употреблении терминов. Показано умелое использование категорий и терминов дисциплины в их ассоциативной взаимосвязи. Продемонстрировано умение аргументировано излагать собственную точку зрения. Видно уверенное владение освоенным материалом, изложение сопровождается адекватными иллюстрациями (примерами) из практики. – Ответ четко структурирован и выстроен в заданной логике. Части ответа логически взаимосвязаны. Отражена логическая структура проблемы (задания): постановка проблемы - аргументация - выводы. Объем ответа укладывается в заданные рамки при сохранении смысла. – Высокая степень самостоятельности, оригинальность в представлении материала: стилистические обороты, манера изложения, словарный запас. Отсутствуют стилистические и орфографические ошибки в тексте. Работа выполнена аккуратно, без помарок и исправлений.
4	– Содержание ответа в целом соответствует теме задания. Продемонстрировано знание фактического материала, встречаются несущественные фактические ошибки. – Продемонстрировано владение понятийно-терминологическим аппаратом дисциплины, отсутствуют ошибки в употреблении терминов. Показано умелое использование категорий и терминов дисциплины в их ассоциативной взаимосвязи. Продемонстрировано умение аргументированно излагать собственную точку зрения. Изложение отчасти сопровождается адекватными иллюстрациями (примерами) из практики. – Ответ в достаточной степени структурирован и выстроен в заданной логике без нарушений общего смысла. Части ответа логически взаимосвязаны. Отражена логическая структура проблемы (задания): постановка проблемы - аргументация - выводы. Объем ответа незначительно превышает заданные рамки при сохранении смысла. – Достаточная степень самостоятельности, оригинальность в представлении материала. Встречаются мелкие и не искажающие смысла ошибки в стилистике, стилистические штампы. Есть 1-2 орфографические ошибки. Работа выполнена аккуратно, без помарок и исправлений.
3	– Содержание ответа в целом соответствует теме задания. Продемонстрировано удовлетворительное знание фактического материала, есть фактические ошибки (25-30%). – Продемонстрировано достаточное владение понятийно-терминологическим аппаратом дисциплины, есть ошибки в употреблении и трактовке терминов, расшифровке аббревиатур. Ошибки в использовании категорий и терминов дисциплины в их ассоциативной взаимосвязи. Нет собственной точки зрения либо она слабо аргументирована. Примеры, приведенные в ответе в качестве практических иллюстраций, в малой степени соответствуют изложенным теоретическим аспектам. – Ответ плохо структурирован, нарушена заданная логика. Части ответа разорваны логически, нет связей между ними. Ошибки в представлении логической структуры проблемы (задания): постановка проблемы - аргументация - выводы. Объем ответа в существенной степени (на 25-30%) отклоняется от заданных рамок. – Текст ответа примерно наполовину представляет собой стандартные обороты и фразы из учебника/лекций. Обилие ошибок в стилистике, много стилистических штампов. Есть 3-5 орфографических ошибок. Работа выполнена не очень аккуратно, встречаются помарки и исправления.
2	– Содержание ответа не соответствует теме задания или соответствует ему в очень малой степени. Продемонстрировано крайне низкое (отрывочное) знание фактического материала, много фактических ошибок - практически все факты (данные) либо искажены, либо неверны. – Продемонстрировано крайне слабое владение понятийно-терминологическим аппаратом дисциплины (неуместность употребления, неверные аббревиатуры, искаженное толкование и т.д.), присутствуют многочисленные ошибки в употреблении терминов. Показаны неверные ассоциативные взаимосвязи категорий и терминов дисциплины. Отсутствует аргументация изложенной точки зрения, нет собственной

	позиции. Отсутствуют примеры из практики либо они неадекватны. – Ответ представляет собой сплошной текст без структурирования, нарушена заданная логика. Части ответа не взаимосвязаны логически. Нарушена логическая структура проблемы (задания): постановка проблемы - аргументация - выводы. Объем ответа более чем в 2 раза меньше или превышает заданный. – Текст ответа представляет полную кальку текста учебника/лекций. Стилистические ошибки приводят к существенному искажению смысла. Большое число орфографических ошибок в тексте (более 10 на страницу). Работа выполнена неаккуратно, с обилием помарок и исправлений.
--	--

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Вопросы для подготовки к зачету

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих
14. реализации информационных угроз.
15. Способы воздействия информационных угроз на объекты.
16. Внешние и внутренние субъекты информационных угроз.
17. Компьютерные преступления и их классификация.
18. Исторические аспекты компьютерных преступлений и современность.
19. Субъекты и причины совершения компьютерных преступлений.
20. Вредоносные программы, их виды.
21. История компьютерных вирусов и современность.
22. Государственное регулирование информационной безопасности.
23. Деятельность международных организаций в сфере информационной безопасности.
24. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
25. Доктрина информационной безопасности России.

26. Уголовно-правовой контроль над компьютерной преступностью в России.
27. Федеральные законы по ИБ в РФ.
28. Политика безопасности и ее принципы.
29. Фрагментарный и системный подход к защите информации.
30. Методы и средства защиты информации.
31. Организационное обеспечение ИБ.
32. Организация конфиденциального делопроизводства.
33. Комплекс организационно-технических мероприятий по обеспечению защиты информации.
34. Инженерно-техническое обеспечение компьютерной безопасности.
35. Организационно-правовой статус службы безопасности.
36. Защита информации в Интернете.
37. Электронная почта и ее защита.
38. Защита от компьютерных вирусов.
39. «Больные» мобильники и их «лечение».

Критерии оценки ответов на зачете

Таблица 6

Показатели, критерии и шкала оценивания устных ответов на зачете

Критерии оценивания	Показатели и шкала оценивания	
	зачтено	не зачтено
текущая аттестация	выполнение требований по текущей аттестации в полном объеме	невыполнение требований по текущей аттестации
полнота и правильность ответа	обучающийся демонстрирует знание и понимание основных положений данной темы, дает правильное определение основных понятий	обучающийся демонстрирует незнание большей части соответствующего вопроса, излагает материал неполно и допускает неточности в определении понятий или формулировке правил
степень осознанности, понимания изученного	демонстрирует понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные	допускает ошибки в формулировке определений и правил, искажающие их смысл; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры
языковое оформление ответа	излагает материал последовательно и правильно с точки зрения норм литературного языка	излагает материал непоследовательно и допускает много ошибок в языковом оформлении излагаемого

При обучении с применением дистанционных технологий и электронного обучения промежуточная аттестация проводится в форме компьютерного тестирования в СДО. Оценивание компетентности обучающегося по установленным для дисциплины индикаторам может осуществляться с помощью банка заданий, включающих тестовые задания пяти типов:

- 1 – тестовое задание открытого типа; предусматривающее развернутый ответ обучающегося в нескольких предложениях, составленное с использованием вопросов для подготовки к зачету или экзамену;
- 2 – выбор одного правильного варианта из предложенных вариантов ответов;
- 3 – выбор 2-3 правильных вариантов из предложенных вариантов ответов;
- 4 – установление правильной последовательности в предложенных вариантах ответов/расчётные задачи, ответом на которые будет являться некоторое числовое значение;
- 5 – установление соответствия между двумя множествами вариантов ответов.

Компетенция: ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикатор: ОПК-3.2 Решение стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности

Тип задания	Примеры тестовых заданий
1	Хакерская атака — это действие или последовательность действий злоумышленников, направленных на проникновение в информационную систему с целью получения несанкционированного доступа к данным.
1	При работе с электронной почтой важно не открывать подозрительные вложения или ссылки, которые могут содержать вирусы или другие вредоносные программы.
1	Шифрование данных позволяет обеспечить конфиденциальность информации путем преобразования данных в непонятный для посторонних вид.
1	Бэкапирование информации является важной процедурой для сохранения данных в случае аварийной ситуации или потери доступа к основным ресурсам.
1	Для защиты от несанкционированного доступа к сети часто используются пароли, аутентификация по MAC-адресу устройства или биометрические методы идентификации.
1	Фишинг — это метод атаки, при котором злоумышленники пытаются получить чувствительную информацию, такую как пароли или данные кредитных карт, путем маскировки под надежные источники.
1	В информационной безопасности важно обеспечить политику доступа к данным, определяющую права и ограничения пользователей в системе.
1	Антивирусное программное обеспечение помогает обнаруживать и удалять

	вредоносные программы, защищая компьютеры и сети от инфицирования.
2	Вопрос: Какая из перечисленных мер является одной из основных для защиты информации от утечки при использовании общественных Wi-Fi сетей? А) Частые изменения пароля на устройствах В) Использование шифрования данных и виртуальных частных сетей (VPN) С) Публикация конфиденциальной информации на социальных сетях Д) Выключение антивирусного программного обеспечения
3	Какие из нижеследующих методов являются основными мерами обеспечения безопасности информации на компьютере? Выберите все правильные ответы. А) Установка антивирусного программного обеспечения В) Регулярное обновление программ и операционной системы С) Использование слабых паролей для удобства запоминания Д) Открытие всех вложений из электронной почты без проверки
4	Упорядочите следующие уровни доступа к информации от наивысшего к наименьшему по степени привилегий: Администратор системы Пользователь с ограниченными правами Гость (неавторизованный пользователь) Модератор форума
5	Сопоставьте следующие понятия по информационной безопасности с их определениями: Список А: Шифрование данных Фишинг Брандмауэр Мультифакторная аутентификация Список В: А) Механизм защиты, который препятствует несанкционированному доступу к сети В) Процесс зашифрования информации для предотвращения прочтения сообщения посторонними лицами С) Метод социальной инженерии, целью которого является получение конфиденциальной информации Д) Система проверки личности с использованием нескольких способов аутентификации

Составитель: доцент, к.э.н. Скрипников О.А.

Зав. кафедрой: к.ф.-м.н., доцент Черняева С. Н.