



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, очно-заочная

г. Воронеж
2021

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-3.1	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.2	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.3	Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом 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, 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-3.1 Знать: принципы, методы и средства применения технологий программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	<i>Отсутствие или фрагментарные представления о принципах, методах и средствах применения технологий программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</i>	<i>Неполные представления о принципах, методах и средствах применения технологий программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</i>	<i>Сформированные, но содержащие отдельные пробелы представления о принципах, методах и средствах применения технологий программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</i>	<i>Сформированные систематические представления о принципах, методах и средствах применения технологий программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</i>	<i>Тестирование, зачет</i>
ОПК-3.2 Уметь: применять технологии программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе информационной и библиографической культуры с применением	<i>Отсутствие умений применять технологии программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения на основе</i>	<i>В целом удовлетворительные, но не систематизированные умения применять технологии программирования для решения стандартных задач профессиональной деятельности по разработке</i>	<i>В целом удовлетворительные, но содержащие отдельные пробелы умения применять технологии программирования для решения стандартных задач профессиональной деятельности по разработке</i>	<i>Сформированные умения применять технологии программирования для решения стандартных задач профессиональной деятельности по разработке программного обеспечения</i>	<i>Тестирование, РГР, зачет</i>

Результат обучения по дисциплине	Критерии оценивания результата обучения по дисциплине и шкала оценивания по дисциплине				Процедура оценивания
	2	3	4	5	
информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	<i>информационно й и библиографической культуры с применением информационно - коммуникацион ных технологий и с учетом основных требований информационно й безопасности.</i>	<i>программного обеспечения на основе информационно й и библиографической культуры с применением информационно - коммуникацион ных технологий и с учетом основных требований информационно й безопасности.</i>	<i>программного обеспечения на основе информационной и библиографической культуры с применением информационно-коммуникационн ых технологий и с учетом основных требований информационной безопасности.</i>	<i>на основе информацион ной и библиографической культуры с применением информацион но-коммуникацио нных технологий и с учетом основных требований информацион ной безопасности.</i>	
ОПК-3.1 Владеть: навыками подготовки технических заданий, отчетов, обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	<i>Отсутствие владения или фрагментарные владения навыками подготовки технических заданий, отчетов, обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационно й безопасности.</i>	<i>В целом удовлетворительные, но не систематизированные владения навыками подготовки технических заданий, отчетов, обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационно й безопасности.</i>	<i>В целом удовлетворительные, но содержащие отдельные пробелы владения навыками подготовки технических заданий, отчетов, обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.</i>	<i>Сформированные владения навыками подготовки технических заданий, отчетов, обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.</i>	<i>Тестирование, РГР, зачет</i>

2. 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

Критерии оценки результатов тестирования

Оценка результатов тестирования. За каждый правильный ответ начисляется 1 балл. Для перевода баллов в оценку применяется универсальная шкала оценки образовательных достижений. Если обучающийся набирает

- от 90 до 100% от максимально возможной суммы баллов - выставляется оценка «отлично»;
- от 80 до 89% - оценка «хорошо»,
- от 51 до 79% - оценка «удовлетворительно»,
- менее 51% - оценка «неудовлетворительно».

Расчетно-графическая работа

Выполнение расчета рисков проекта (по вариантам)

- 1 «Расчет показателей надежности нерезервированных невосстанавливаемых автоматизированных систем»
- 2 «Исследование свойств структурно резервированных автоматизированных систем при общем резервировании с постоянно включенным резервом»
- 3 «Исследование свойств структурно резервированных систем при общем резервировании замещением»
- 4 «Исследование надежности автоматизированных систем с учетом их физической реализуемости»
- 5 «Исследование надежности и риска нерезервированных невосстанавливаемых автоматизированных систем»
- 6 «Исследование надежности и риска нерезервированных восстанавливаемых автоматизированных систем»
- 7 «Исследование надежности и риска резервированных восстанавливаемых автоматизированных систем»
- 8 «Исследование надежности восстанавливаемых автоматизированных информационных систем»
- 9 «Анализ влияния профилактики на надежность автоматизированных систем»

Критерии оценивания:

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

Таблица 4

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.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

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 5

Критерии оценки			
Наименование показателя	Критерии оценки	Максимальное количество баллов	Количество баллов
I. КАЧЕСТВО ОТВЕТА			
1 Соответствие ответов, поставленным вопросам	- систематизированные, глубокие и полные знания по всем разделам учебной программы - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины - умение ориентироваться в теориях, концепциях и направлениях по изучаемой дисциплине	10	
2. Грамотность изложения	- владение терминологией и понятийным аппаратом проблемы; - научный стиль изложения.	5	
3. Самостоятельность выполнения работы, глубина проработки материала, использование рекомендованной и справочной литературы	- степень знакомства автора работы с актуальным состоянием изучаемой проблематики; - дополнительные знания, использованные при написании работы, которые получены помимо предложенной образовательной программы;	5	
Общая оценка за выполнение		20	
ОТВЕТЫ НА ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ ПО СОДЕРЖАНИЮ РАБОТЫ			
Вопрос 1		5	
Вопрос 2		5	
Общая оценка за ответы на вопросы		10	
Итого		30	

Для перевода баллов критериально-шкалированной таблицы в оценку применяется универсальная шкала оценки образовательных достижений. Если студент набирает 18-30 баллов и выше - оценка «зачтено», 26 -21 баллов и выше - оценка «хорошо», 18-21 баллов и выше - оценка «удовлетворительно», менее 18 - оценка «не зачтено».

Составитель: д.ф.-м.н., профессор Кузьменко Р. В.

Зав. кафедрой: д.т.н., профессор Лапшина М. Л.

Рабочая программа рассмотрена на заседании кафедры математики, информационных систем и технологий и утверждена на 2021/2022 учебный год.

Протокол № 10 от 22 июня 2021 г.

Лист актуализации фонда оценочных средств

«Основы информационной безопасности»

шифр по учебному плану, наименование

для подготовки бакалавров

Направление: (шифр – название) 09.03.02 Информационные системы и технологии

Профиль: Информационные системы на транспорте

Форма обучения очная, очно-заочная

Год начала подготовки: 2021

Курс 4, 5

Семестр 8, 10

а) в фонд оценочных средств не вносятся изменения. ФОС актуализирован на 2024 / 2025 г. учебный год.

б) в фонд оценочных средств вносятся следующие изменения:

- 1) _____;
- 2) _____;
- 3) _____.

Разработчик (и): д.ф.-м.н., профессор Кузьменко Р. В.
(ФИО, ученая степень, ученое звание)

Фонд оценочных средств пересмотрен и одобрен на заседании кафедры математики, информационных систем и технологий протокол № 12 от «28» июня 2024 г.

Заведующий кафедрой: Черняева С. Н., к. ф.-м. н., доцент / 
(ФИО, ученая степень, ученое звание) (подпись)