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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для студентов, обучающихся по направлению 09.03.02 - “Информационные системы и технологии”, очной, очно-заочной, заочной форм обучения

г. Воронеж
2023

Методические рекомендации для самостоятельной работы по дисциплине «Основы информационной безопасности**»** / Сост. О. А. Скрипников. - Воронеж: Воронежский филиал ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова», 2023. - 23 с. – Текст : непосредственный.

Методические рекомендации для самостоятельной работы составлены в соответствии с программой дисциплины «Основы информационной безопасности», изучаемой в Воронежском филиале ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова. Рекомендации предназначены для организации контактной работы с обучающимися по дисциплине «Основы информационной безопасности», а также для самостоятельной внеаудиторной работы обучающихся.

Методические рекомендации утверждены на заседании кафедры математики, информационных систем и технологий Воронежского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» 29.06.2023 г., протокол № 10.

Содержание

Введение

Для успешного освоения учебной дисциплины обучающимся необходимо изучить лекционный материал и рекомендуемую литературу, отработать изученный материал на практических занятиях, выполнить задания для самостоятельной работы. Практические занятия проводятся с целью закрепления лекционного материала, овладения понятийным аппаратом предмета, методами работы, изучаемыми в рамках учебной дисциплины.

Все формы практических занятий (семинары – практикумы, практические, лабораторные) направлены на практическое усвоение теоретических знаний, полученных на лекциях. Главной целью такого рода занятий является: научить студентов применению теоретических знаний на практике. С этой целью на занятиях моделируются фрагменты их будущей деятельности в виде учебных ситуационных задач, при решении которых студенты отрабатывают различные действия по применению соответствующих практических навыков.

Самостоятельная работа студента – это планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа в современном образовательном процессе рассматривается как форма организации обучения, которая способна обеспечивать самостоятельный поиск необходимой информации, творческое восприятие и осмысление учебного материала в ходе аудиторных занятий, разнообразные формы познавательной деятельности студентов на занятиях и во внеаудиторное время, развитие аналитических способностей, навыков контроля и планирования учебного времени, выработку умений и навыков рациональной организации учебного труда. Таким образом, самостоятельная работа – форма организации образовательного процесса, стимулирующая активность,

самостоятельность, познавательный интерес студентов.

Самостоятельная работа обучающихся является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения. Государственным стандартом предусматривается, как правило, не менее 50% часов из общей трудоемкости дисциплины на самостоятельную работу обучающихся (далее СРО). В связи с этим, обучение включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому СРО должна стать эффективной и целенаправленной работой студента.

Самостоятельная работа обучающихся является одной из основных форм внеаудиторной работы при реализации учебных планов и программ.

Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления ученика, его умственных и практических операций и действий зависит и определяется самим студентом.

Обучающийся в процессе изучения дисциплины должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Студенту предоставляется возможность работать во время учебы более самостоятельно, чем учащимся в средней школе. Обучающихся должен уметь планировать и выполнять свою работу.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности.

1. Цели и задачи дисциплины

Целями освоения дисциплины «Основы информационной безопасности**»** является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности.

Связь, информационные и коммуникационные технологии в сфере разработки, внедрения и сопровождения информационных технологий и систем

В рамках освоения образовательной программы высшего образования выпускники готовятся к решению задач профессиональной деятельности следующих типов:

- производственно-технологический;
- научно-исследовательский.

2. Методические указания по изучению дисциплины «Основы информационной безопасности»

Основными формами обучения дисциплине являются:

1) лекции,
2) лабораторные занятия,
3) самостоятельная работа.

2.1. Методические рекомендации по подготовке к лекциям

Лекция – логическое изложение материала в соответствии с планом лекции, который сообщается в начале каждой лекции, и имеет законченную форму, т.е. содержит пункты, позволяющие охватить весь материал, который необходимо довести до студентов.

Главной задачей лектора является организация процесса познания студентами материала изучаемой дисциплины на всех этапах ее освоения, предусмотренных федеральным государственным образовательным стандартом.

На лекциях особое внимание уделяется не только усвоению изучаемых проблем, но и стимулированию Вашей активной познавательной деятельности, творческого мышления, развитию научного мировоззрения, профессионально-значимых свойств и

качеств. Лекции по учебной дисциплине проводятся, как правило, как проблемные в форме диалога (интерактивные).

Излагаемый материал может показаться Вам сложным, поскольку включает знания, почерпнутые преподавателем из различных отраслей психологии – общей психологии, психологии познавательных процессов, психологии личности, социальной психологии и т.д. Вот почему необходимо добросовестно и упорно работать на лекциях. Осуществляя учебные действия на лекционных занятиях, Вы должны внимательно воспринимать действия преподавателя, запоминать складывающиеся образы, мыслить, добиваться понимания изучаемого предмета, применения знаний на практике, при решении учебно-профессиональных задач. В ходе лекционных занятий необходимо вести конспектирование учебного материала, обращая внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Правила конспектирования:

1. Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля (4-5 см) для дополнительных записей.

2. Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

3. Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их.

4. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

5. Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий. Однако чрезмерное увлечение сокращениями может привести к тому, что со временем в них будет трудно разобраться.

6. В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д. Надо иметь в виду, что изучение и отработка прослушанных лекций без промедления значительно экономит время и способствует лучшему усвоению материала.

Перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на лабораторных занятиях.

Содержание разделов учебной дисциплины «Основы информационной безопасности»

1. Информационная безопасность и уровни ее обеспечения.

Понятие "информационная безопасность". Проблема информационной безопасности общества. Определение понятия "информационная безопасность". Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Механизмы безопасности. Администрирование средств безопасности. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности. Классификация угроз "информационной безопасности". Классы угроз информационной безопасности.

2. Компьютерные вирусы и защита от них.

Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивные возможностям. Характеристика "вирусоподобных" программ. Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Обнаружение неизвестного вируса. Обнаружение загрузочного вируса. Обнаружение резидентного вируса. Обнаружение макровируса. Общий алгоритм обнаружения вируса. Ссылки на дополнительные материалы (печатные и электронные ресурсы).

3. Информационная безопасность вычислительных сетей. Информационная безопасность при использовании Internet.

Особенности обеспечения информационной безопасности в компьютерных сетях. Особенности информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Сетевые модели передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP. Модель взаимодействия открытых систем OSI/ISO. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Адресация в глобальных сетях. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классификация удаленных угроз в вычислительных сетях. Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Удаленная атака "анализ сетевого трафика". Удаленная атака "подмена доверенного объекта". Удаленная атака "ложный объект". Удаленная атака

"отказ в обслуживании". Причины успешной реализации удаленных угроз в вычислительных сетях. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей.

Информационная безопасность при использовании Internet.

4. Механизмы обеспечения "информационной безопасности".

Идентификация и аутентификация. Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей. Криптография и шифрование. Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи. Методы разграничение доступа. Методы разграничения доступа. Мандатное и дискретное управление доступом. Регистрация и аудит. Определение и содержание регистрации и аудита информационных систем. Этапы регистрации и методы аудита событий информационной системы. Межсетевое экранирование. Классификация межсетевых экранов. Характеристика межсетевых экранов. Технология виртуальных частных сетей (VPN). Сущность и содержание технологии виртуальных частных сетей. Понятие "туннеля" при передаче данных в сетях.

5. Безопасность операционных систем.

Безопасность операционных систем. Безопасность ОС Windows 10

2.2. Методические рекомендации по подготовке к лабораторным занятиям

Семинар – это один из наиболее сложных и в то же время плодотворных видов (форм) вузовского обучения и воспитания. В условиях высшей школы Лабораторная работа – вид практической работы, проводимой под руководством преподавателя, ведущего научные исследования по тематике лабораторной работы и в данной отрасли научного знания.

Лабораторная работа предназначен: для углубленного изучения той или иной дисциплины и овладения методологией применительно к особенностям изучаемой отрасли науки; для активной самостоятельной групповой работы, когда студенты могут подготовить, обдумать поставленные перед ними проблемы, проверить свою позицию, услышать и обсудить другие.

Целесообразно готовиться к лабораторной работе занятиям за 1- 2 недели до их начала. Начинать надо с изучения рекомендованной литературы, так как на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы вы должны стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.

Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам.

На лабораторной работе каждый из Вас должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении. Выступление должно строиться свободно, убедительно и аргументировано. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного. При этом Вы можете обращаться к записям конспекта и лекций, непосредственно к первоисточникам, использовать знание художественной литературы и искусства, факты и наблюдения современной жизни и т.д. Вокруг такого выступления могут разгореться споры, дискуссии, к участию в которых должен стремиться каждый.

При подготовке к лабораторной работе вам следует:

- приносить с собой рекомендованную преподавателем литературу к конкретному занятию;
- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;
- при подготовке к лабораторной работе следует обязательно использовать не только лекции, но учебную, методическую литературу;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- в ходе лабораторной работы давать конкретные, четкие ответы по существу вопросов;
- на занятии демонстрировать понимание проведенных анализов, ситуаций, в случае затруднений обращаться к преподавателю.

Если Вы пропустили занятие (независимо от причин) или не подготовились к занятию, рекомендуется не позже, чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изученной на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положительную оценку в соответствующем семестре. При такой подготовке лабораторное занятие пройдет на необходимом методологическом уровне и принесет интеллектуальное удовлетворение всей группе.

Содержание лабораторных работ

1. Основные аспекты информационной безопасности
2. Основные направления обеспечения безопасности: правовая защита, организационная защита, инженерно-техническая защита.
3. Вредоносное программное обеспечение
4. Антивирусное программное обеспечение
5. Настройки безопасности Интернет-браузеров
6. Симметричное и асимметричное шифрование

7. Электронная цифровая подпись

8. Настройки безопасности операционной системы Windows

9. Настройки безопасности приложений Microsoft Office. Защита документов.

3. Методические рекомендации по организации самостоятельной работы обучающихся по дисциплине «Основы информационной безопасности»

3.1. Общие методические рекомендации по самостоятельной работе

Самостоятельная работа – это планируемая работа студентов, выполняемая по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Целью самостоятельной работы студентов являются: обучение навыкам работы с научной литературой и практическими материалами, необходимыми для углубленного изучения дисциплины, а также развитие у них устойчивых способностей к самостоятельному (без помощи преподавателя) изучению и изложению полученной информации. В связи с этим основными задачами самостоятельной работы студентов, изучающих дисциплину являются:

– во-первых, продолжение изучения учебной дисциплины в домашних условиях по программе, предложенной преподавателем;

– во-вторых, привитие студентам интереса к психологической литературе;

– в-третьих, развитие познавательных способностей.

Изучение и изложение информации, полученной в результате изучения научной литературы и практических материалов, предполагают развитие у студентов как владения навыками устной речи, так и способностей к четкому письменному изложению материала.

Основными формами самостоятельной работы студентов являются:

- подготовку к аудиторным занятиям, изучение материала по учебникам (в т.ч. по конспекту лекций);

- оформление отчетов по лабораторным работам (подготовка к лабораторным занятиям);

- выполнение курсовой работы.

Основной формой контроля за самостоятельной работой студентов являются лабораторные занятия, промежуточная аттестация, а также еженедельные консультации преподавателя по выполнению курсовой работы.

4. Промежуточная аттестация

Итоговой оценкой по дисциплине является результат промежуточной аттестации, выставленный с учетом результатов 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-компании
- 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 нелицензионного 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, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальностьl

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 перчисленное 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

Показатели и шкала оценивания
тестовых заданий на зачете

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

Примерные вопросы 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».

Показатели, критерии и шкала оценивания
письменных ответов на экзамене

Критерии оценивания	Показатели и шкала оценивания			
	5	4	3	2
текущая аттестация	выполнение требований по текущей аттестации в полном объеме		выполнение требований по текущей аттестации в неполном объеме	невыполнение требований по текущей аттестации
полнота и правильность ответа	обучающийся полно излагает материал, дает правильное определение основных понятий	обучающийся достаточно полно излагает материал, однако допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочета в последовательности и языковом оформлении излагаемого	обучающийся демонстрирует знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил	обучающийся демонстрирует незнание большей части соответствующего вопроса
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	присутствуют 1-2 недочета в обосновании своих суждений, количество приводимых примеров ограничено	не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры	допускает ошибки в формулировке определений и правил, искажающие их смысл
языковое оформление ответа	излагает материал последовательно и правильно с	излагает материал последовательно, с 2-3 ошибками в	излагает материал непоследовательно и допускает	беспорядочно и неуверенно излагает материал

	точки зрения норм литературного языка	языковом оформлении	много ошибок в языковом оформлении излагаемого	

5. Перечень основной, дополнительной учебной литературы и учебно-методической литературы для самостоятельной работы обучающихся, необходимой для освоения дисциплины

Основная литература

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927

Дополнительная литература

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239

Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. —

Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519079

Издается в авторской редакции
Подписано в печать 29.06.2023. Формат 60х90 $^{1}/_{16}$
Бумага кн.-журн. П.л. 1,44 Гарнитура Таймс.
Тираж 15 экз.

Воронежский филиал Федерального государственного образовательного учреждения высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»
Типография Воронежского филиала ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова», Воронеж, Ленинский проспект, 174л.