*На правах рукописи*

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

**«Оренбургский государственный университет»**

Кафедра прикладной информатики в экономике и управлении

Методические указания для обучающихся по освоению дисциплины

*«Информационная безопасность»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

*09.03.03 Прикладная информатика*

(код и наименование направления подготовки)

*Прикладная информатика в экономике*

(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

*Программа академического бакалавриата*

Квалификация

*Бакалавр*

Форма обучения

*Заочная*

Год набора 2022

Составитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Позевалкин

«\_7\_» \_\_ февраля\_\_\_\_\_ 20\_22\_ г.

Методические указания рассмотрены и одобрены на заседании кафедры прикладной информатики в экономике и управлении

Протокол № \_\_9\_\_ от «\_\_7\_\_» \_\_ февраля\_\_\_\_ 20\_22\_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.А. Жук

Методические указания является приложением к рабочей программе по дисциплине *«Информационная безопасность»*, зарегистрированной в ЦИТ под учетным номером \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1 Методические указания преподавателю**

**Методика чтения лекций**

Лекции являются одним из основных методов обучения по дисциплине «Информационная безопасность», которые должны решать следующие задачи:

* изложить важнейший материал программы курса, освещающий основы информационной безопасности;
* ознакомить с принципами обеспечения информационной безопасности;
* развить у студентов потребность к самостоятельной работе над учебниками, научной литературой.

Главной задачей каждой лекции является раскрытие сущности темы и анализа ее основных положений. Преподавателю следует иметь план лекции и следовать ему, необходимо доступно разъяснять новые термины и понятия, доказательно и аргументировано излагать материал лекции, выделяя главные мысли и выводы. Рекомендуется на первой лекции кратко довести до внимания студентов структуру курса и его разделы, а в дальнейшем указывать суть и задачи каждого раздела, а, закончив изложенное, подводить итог этому разделу, чтобы связать его со следующим.

**Содержание лекции**

Содержание лекции определяется программой курса и рабочей программой по дисциплине. Желательно, чтобы каждая лекция охватывала и исчерпывала определенную тему курса и представляла собой логически вполне законченную работу. Лучше сократить тему, но не допускать перерыва ее в таком месте, когда основная идея еще полностью не раскрыта. Цель лекции – формирование ориентировочной основы для последующего усвоения студентами учебного материала.

Лекция должна выполнять информационную (излагать необходимые сведения), стимулирующую (пробуждать интерес к теме), развивающую (развивать мышление) и разъясняющую (направлять на формирование основных понятий науки) функции. В ходе лекции следует повышать активизацию познавательной деятельности студентов, повышать мотивацию студентов по поиску необходимой информации, оперировать ею. Теоретические положения лекции следует тесно увязывать с практикой.

**Методика проведения лабораторных занятий**

Лабораторные занятия направлены на расширение и детализацию знаний, полученных на лекциях, на выработку и закрепление умений и практических навыков.

Методика проведения лабораторных занятий может быть различной, она зависит от авторской индивидуальности преподавателя. Важно, чтобы различными методами достигалась общая дидактическая цель. Особенности выполнения лабораторных работ заключается в том, что преподаватель работает со своей группой фронтально, консультируя как всю группу, так и отдельно взятого студента.

В начале каждого лабораторного занятия необходимо сформулировать цель, поставить задачи, указать содержание работы и технологию выполнения работы. В ходе лабораторного занятия преподаватель решает такие задачи как повторение и закрепление знаний, контроль (проверка индивидуальных отчетов) и педагогическое общение.

Подготовка к лабораторным занятиям не может ограничиваться слушанием лекции, а предполагает предварительную самостоятельную работу студентов по каждой запланированной теме.

**Критерии оценки знаний, умений и навыков**

В зависимости от вида итогового контроля по дисциплине (экзамен, зачет) и формы его организации могут быть использованы различные критерии оценки знаний, умений и навыков.

При традиционной форме итогового контроля в виде собеседования, в программе представлены критерии выставления оценок по бинарной системе «зачтено», «не зачтено». Эти оценки проставляются в аттестационную ведомость. Оценки «не зачтено» в зачетную книжку студентов не проставляются.

Оценка «зачтено» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения задач. Допускаются неточности в ответе и недостаточно правильные формулировки.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Ведущий экзаменатор (кафедра) имеет право выставлять итоговую оценку с учетом успеваемости студента по дисциплине.

Неявка на экзамен или зачет отмечается в аттестационной ведомости словами «не явился» и в случае последующего выявления неуважительности причины деканом факультета проставляется неудовлетворительная оценка.

**2 Методические указания студентам по освоению дисциплины**

Успешное освоение дисциплины «Информационная безопасность» предполагает регулярное посещение лекционных занятий, практических занятий и выполнение заданий.

**2.1 Методические указания по лекционным занятиям**

Лекции являются одним из основных методов обучения по дисциплине «Информационная безопасность», решающим следующие задачи:

* изложить важнейший материал программы курса, освещающий основы информационной безопасности;
* ознакомить с принципами обеспечения информационной безопасности;
* развить у студентов потребность к самостоятельной работе над учебниками, научной литературой.

Изучение дисциплины следует начинать с проработки рабочей программы, особое внимание необходимо уделить целям и задачам, структуре и содержанию курса.

При конспектировании лекций обучающиеся должны излагать услышанный материал на лекции своими словами. Необходимо выделять важные места в своих записях. Каждый раз, когда что-либо не понятно, необходимо записывать свои вопросы. По возможности можно сравнивать свои конспекты с конспектами двух-трех других обучающихся, при этом дополняя и исправляя свои записи.

Конспект лекций следует просматривать регулярно после каждого занятия. Если тот или иной фрагмент вызывает затруднения, необходимо обратиться за помощью к преподавателю. Лекции предусматривают изучение теоретических основ.

Успешное освоение курса предполагает активное, творческое участие обучающегося путем планомерной, повседневной работы.

Лекционный материал необходимо кратко записывать, обращая внимание, на логику изложения материла, аргументацию и приводимые примеры.

Лекционный материал следует просматривать в тот же день, когда читалась лекция, помечая непонятные места. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за консультацией на ближайшей лекции к преподавателю.

Рекомендуемую дополнительную литературу следует прорабатывать после изучения данной темы по учебнику и материалам лекции.

При подготовке материала необходимо обращать внимание на точность определений, последовательность изучения материала, аргументацию, собственные примеры.

Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

**2.2 Методические указания по выполнению контрольной работы**

По дисциплине предусматривается выполнение контрольной работы (КонтрР).

Целью выполнения контрольной работы по дисциплине «Информационная безопасность» является приобретение практических навыков работы, а также закрепление и расширение знаний, полученных при изучении теоретического материала.

При выполнении контрольной работы студент должен показать умение анализировать, и на практике применить теоретические знания.

Контрольная работа – самостоятельная творческая завершенная работа студента, выполненная под руководством преподавателя. Она обычно состоит из двух частей: теоретической и практической.

Основные цели работы: развитие активной творческой личности, способной самостоятельно приобретать новые знания, развитие навыков самостоятельной исследовательской работы у студентов.

Выполнение КонтрР предусматривает следующие этапы выполнения:

1. Получить задание и график выполнения ИТЗ.

2. Определить свой вариант.

3. Изучить и описать теоретическую часть.

4. Выполнить и описать практическую часть.

5. Оформить КонтрР по правилам оформления студенческих работ.

6. Пройти защиту.

Индивидуальное задание состоит из двух частей, взаимосвязанных между собой по объекту защиты информационных процессов (далее - объекта). Объект необходимо исследовать таким образом, чтобы можно было применить все основные элементы защиты информации, определяя его возможное размещение, внешние и внутренние характеристики среды с учетом возможных сценариев атаки.

Для выполнения первой части работы необходимо для предложенного объекта провести анализ его защищенности по следующим направлениям:

* виды угроз;
* характер и виды происхождения угроз;
* классы каналов несанкционированного получения информации (нарушения конфиденциальности);
* возможные причины нарушения целостности информации;
* возможные причины нарушения доступности;
* определить класс защиты информации в соответствии с Руководящими документами Гостехкомиссии России.

Для выполнения второй части работы необходимо предложить методы повышения уровня защищенности объекта в соответствии со следующим анализом:

* определить требования к системе защиты;
* определить факторы, влияющие на требуемый уровень;
* предложить программно-аппаратные и организационно-административные способы защиты объекта;
* разработать основы политики безопасности в области эксплуатации анализируемого объекта.

Отчет по КонтрР должен включать:

* титульный лист;
* лист задания;
* введение (1–2 стр.) с характеристикой защищаемого объекта;
* анализ уязвимостей и угроз для объекта защиты (12–15 стр.);
* методы повышения уровня защищенности объекта (12–15 стр.);
* заключение (1–2 стр.);
* список использованных источников (не менее 10).

Оформление отчета по КонтрР должно соответствовать общим требованиям к оформлению студенческих работ, которые можно скачать с сайта ОГУ. Общий объем отчета по КонтрР — примерно 30–35 страниц.

**Варианты для творческих заданий:**

1. Сервер базы данных, содержащий сведения о клиентах компании
2. Компьютер в бухгалтерии, используемый для передачи отчетности в головной офис через VPN
3. Почтовый сервер крупной компании
4. Веб-сервер, используемый для электронной коммерции
5. Сервер, содержащий бухгалтерские отчеты крупной компании
6. Локальная сеть с выходом в Интернет
7. Корпоративная сеть с выходом в Интернет
8. Программно-аппаратные средства платежных банковских систем
9. Программно-аппаратные средства системы дистанционного обучения
10. Система автоматизированного проектирования узлов вычислительной сети
11. Информационная система управления бизнесом в области объектов недвижимости
12. Информационная система управления производственным предприятием
13. Автоматизированная система управления персоналом в крупной компании
14. Сервер, содержащий данные о сделках на рынке ценных бумаг
15. Телекоммуникационный канал связи между филиалами банка
16. Телекоммуникационный канал связи между дилерами банка и валютной биржей
17. Широкополосный канал выхода в Интернет крупной международной компании
18. Межсетевой экран, обеспечивающий сегментацию локальной сети
19. Сервер федеральной налоговой службы
20. Сервер учебного заведения, содержащий результаты тестирования студентов

**2.3 Методические указания по подготовке к промежуточной аттестации по дисциплине**

Изучение дисциплины «Информационная безопасность» завершается зачетом. Для допуска к зачету (экзамену) необходимо представить отчет по типовым заданиям и выполнить КонтрР. Отчет по типовым заданиям описывает результаты выполнения и включает описание.

Подготовка к зачету (экзамену) способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к зачету (экзамену), студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачете (экзамене) студент демонстрирует то, что он приобрел в процессе обучения по данной учебной дисциплине.

В период подготовки к зачету (экзамену) студенты вновь обращаются к пройденному учебному материалу. При этом они не только скрепляют полученные знания, но и получают новые. Подготовка студента к зачету (экзамену) включает в себя три этапа:

- самостоятельная работа в течение семестра;

- непосредственная подготовка в дни, предшествующие зачету (экзамену) по темам курса;

- подготовка к ответу на вопросы.

Подготовка к зачету (экзамену) осуществляется на основании методических рекомендаций по дисциплине и списка вопросов изучаемой дисциплины, конспектов лекций, учебников и учебных пособий, научных статей, информации среды интернет.

Студент должен иметь хороший собственный конспект лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить, обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным.

Кроме того, при подготовке к зачету (экзамену) у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра.

Вначале следует просмотреть весь материал по дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения.

**2.4 Методические указания по выполнению типовых заданий для обучающихся**

**Общие методические рекомендации**

1 Ознакомиться с общим тематическим планом занятий;

2 Самостоятельно прорабатывать уже пройденный материал лекционных и практических занятий. При необходимости составить список вопросов и обратиться к преподавателю;

3 Перед изучением нового теоретического материала желательно заранее ознакомиться с содержанием предстоящей лекции. При необходимости составить список вопросов и обратиться к преподавателю;

4 Если в ходе рассмотрения нового теоретического или практического материала преподаватель ссылается на полученные ранее знания, умения или навыки, то рекомендуется освежить их в памяти путём повторения;

5 Выполнять индивидуальные задания рекомендуется не только в рамках учебных занятий, но и в большей мере в течение времени, отведённого на самостоятельную работу.

6 Ознакомиться со списком литературы и интернет-ресурсов, рекомендуемых преподавателем для углубленного изучения либо дисциплины в целом, либо отдельных разделов.

Для реализации индивидуальных и творческих способностей и более глубокого освоения дисциплины предусмотрены следующие виды самостоятельной работы: текущая и творческая.

**Типовые задачи**

**Раздел 1. Информационная безопасность: понятия и определения**

**Задача №1**

Сделайте реферат на тему «Информационная безопасность». В реферате обязательно должны быть: таблица, рисунок, от 10 до 12 страниц текста, список источников не менее 7.

В реферате:

* выделить весь текст и очистить формат;
* изменить стили для правильного оформления заголовков и текста;
* оформление документа должно соответствовать требованиям оформления студенческих работ (можно скачать с сайта ОГУ);
* сделать титульный лист;
* вставить номера страниц (кроме первой страницы);
* на листе содержания сделать Автособираемое оглавление;
* проверить правильность перехода по пунктам оглавления;
* научиться обновлять автособираемое оглавление;
* для списка используемых источников (если его нет, то нужно сделать самим) сделать нумерацию (числами);
* список источников расположить по мере встречаемости;
* расставить по тексту реферата ссылки на все источники. Ссылки расставлять как перекрестные (ссылки на источники указывать в квадратных скобках, например, [1]);
* упорядочить список литературы по алфавиту;
* выделить весь документ и нажать кнопку F9;
* проверить правильно ли обновились ссылки на источники;
* в тексте реферата сделать несколько гиперссылок на сайты.

Готовый файл .doc / .docx сдайте на проверку.

**Раздел 2. Угрозы информационной безопасности**

**Задача №2**

**Работа с сервисами google**

1. Зайти на <https://www.google.ru/> и зарегистрироваться (если уже регистрировались раньше, то повторно не нужно).

2. Изучить возможности сервисов google.

3. Зайти на <https://docs.google.com/forms>.

4. Создать форму, в которой сделать тестовые задания по лекционному материалу раздела «Угрозы информационной безопасности».

5. Разработать тестовые задания (10 заданий) с несколькими вариантами ответов. Использовать все возможные представления варианты ответов (один из списка, несколько из списка, шкала, сетка и т.д.).

6. Проверить работу теста. Отправить ссылку на тест преподавателю.

**Раздел 3. Вредоносные программы**

**Задача №3**

**Создание ментальных карт с помощью онлайн-сервисов**

1. Зайти на <https://coggle.it/> и зарегистрироваться (если уже регистрировались раньше, то повторно не нужно).

2. Изучить возможности сервиса coogle для создания майндкарт (ментальных карт).

3. Создать свою ментальную карту по теме «Классификация компьютерных вирусов» лекционного материала.

4. При создании карты использовать картинки, гиперссылки и т.д. При этом учитывать эргономические характеристики.

5. Сохранить карту в формате pdf.

**Раздел 4. Методы и средства защиты компьютерной информации**

**Задача №4**

Сделать реферат и презентацию на тему «Методы и средства защиты компьютерной информации».

Реферат должен быть выполнен по требованиям оформления студенческих работ (можно скачать с сайта ОГУ).

В реферате обязательно должны быть:

* титульный лист;
* введение;
* основная часть
* заключение;
* список используемых источников (5-10 источников);
* приложения.

Основная часть должна иметь структуру, содержащую теоретический материал по методам и средствам защиты информации и рекомендации по их практическому применению. Объем основной части 8-10 страниц.

Объем презентации 10-15 слайдов.

По итогам выполнения работы сдайте на проверку файлы:

* файл реферата в формате .doc / .docx;
* файл презентации в формате .ppt / .pptx.

**Раздел 5. Криптографические методы защиты информации**

**Задача №5**

**Работа с онлайн-сервисом шифрования**

1. Зайти на сайт <http://translit-online.ru/pasport.html> и выполнить транслитерацию своих фамилии, имени и отчества.
2. Зайти на сайт <http://crypt-online.ru/>.
3. Ознакомиться со структурой сайта.
4. Научиться кодировать и декодировать свои фамилию, имя и отчество (результат транслитерации) с помощью алгоритмов преобразования, представленных на сайте.
5. Сделайте отчет по выполненной работе по стандартам оформления студенческих работ.

В отчете обязательно должны быть:

* титульный лист;
* содержание;
* задание;
* теоретическая часть (теория по криптографическим методам);
* практическая часть (описание работы с сайтом <http://crypt-online.ru/>, обязательно включить скриншоты с кодированием и декодированием своих фамилии, имени и отчества);
* выводы;
* список используемых источников (не менее 5 источников).

Общий объем отчета должен быть 10-12 страниц.

По итогам выполнения работы сдайте на проверку отчет в формате .doc / .docx.

**Раздел 6. Лицензирование и сертификация в области защиты информации**

**Задача №6**

Задача 1. Работа со справочными правовыми системами.

1. Изучите возможности справочной правовой системы КонсультантПлюс (изучите интерфейс и структуру системы, ознакомьтесь с содержанием имеющихся разделов).

2. Изучить возможности справочной правовой системы Гарант (изучите интерфейс и структуру системы, ознакомьтесь с содержанием имеющихся разделов).

3. С помощью справочных правовых систем КонсультантПлюс и Гарант выполните следующие задания:

* Работа со словарем терминов. Найдите в СПС определения следующих понятий: «информация», «документы», «программа для ЭВМ», «безопасность», «государственная тайна»;
* Поиск по запросу. Найдите документы, в названиях которых присутствуют слово сети и слово связь в любых падежах и словоформах. Укажите количество найденных документов;
* Поиск по дате. Найдите федеральный закон от 27 июля 2006 г. N 149-ФЗ;
* Поиск по статусу. Найдите действующие и не утратившие силу законы в области защиты информации;
* Найдите правовые документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

Задача 2. Сделайте отчет по выполненной работе по стандартам оформления студенческих работ.

В отчете обязательно должны быть:

* титульный лист;
* содержание;
* задание;
* теоретическая часть (описание возможностей справочных правовых систем КонсультантПлюс и Гарант);
* практическая часть (описание работы со справочными правовыми системами, обязательно включить скриншоты);
* выводы;
* список используемых источников (не менее 5 источников).

Общий объем отчета должен быть 10-12 страниц.

По итогам выполнения работы прикрепите в курс Moodle файл отчета.

**Раздел 7. Критерии безопасности компьютерных систем**

**Задача №7**

**Анализ критериев безопасности компьютерных систем**

Создание ментальных карт с помощью онлайн-сервисов.

1. Зайти на <https://coggle.it/> и зарегистрироваться (если уже регистрировались раньше, то повторно не нужно).

2. Изучить возможности сервиса coogle для создания майндкарт (ментальных карт).

3. Создать свою ментальную карту по теме «Критерии безопасности компьютерных систем» лекционного материала.

4. При создании карты использовать картинки, гиперссылки и т.д. При этом учитывать эргономические характеристики.

5. Сохранить ментальную карту в формате .pdf и прикрепить ее в курс.

По итогам выполнения работы сдайте файл с ментальной картой в формате .pdf.