

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Тольяттинский государственный университет»

**Б1.О.28**  
(индекс дисциплины)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Экономическая и информационная безопасность

(наименование дисциплины)

по направлению подготовки

38.03.02 Менеджмент

направленность (профиль)

Предпринимательство

Форма обучения: очная

Год набора: 2022

Общая трудоемкость: 6 ЗЕТ

**Распределение часов дисциплины по семестрам**

| Семестр                                      | 7          | Итого      |
|--|------------|------------|
| Форма контроля                               | экзамен    |            |
| Вид занятий                                  |            |            |
| Лекции                                       | 16         | 16         |
| Лабораторные                                 | 4          | 4          |
| Практические                                 | 32         | 32         |
| Руководство: курсовые работы (проекты) / РГР | -          | -          |
| Промежуточная аттестация                     | 0,35       | 0,35       |
| Контактная работа                            | 52,35      | 52,35      |
| Самостоятельная работа                       | 128        | 128        |
| Контроль                                     | 35,65      | 35,65      |
| <b>Итого</b>                                 | <b>216</b> | <b>216</b> |

Рабочую программу составил:  
Доцент департамента бакалавриата (экономических и управленческих программ),  
к.э.н., Данилова С.Ю.  

---

(должность, ученое звание, степень, Фамилия И.О.)

**Рецензирование рабочей программы дисциплины:**

☒ \* Отсутствует

☐ Рецензент

---

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана специальности

38.03.02 Менеджмент

---

**Срок действия рабочей программы дисциплины до «26» августа 2026 г.**

**УТВЕРЖДЕНО**

На заседании института финансов, экономики и управления (протокол заседания № 1 от 26.08.2021).

## 1. Цель освоения дисциплины

Цель освоения дисциплины – формирование целостной системы знаний о подходах к управлению комплексными системами защиты информации (КСЗИ), навыков профессиональной эксплуатации современного электронного оборудования и программного обеспечения комплексных систем защиты информации с учетом применения различных подходов к автоматизации и информатизации предприятий и организаций; опыта работы с нормативной документацией, регламентирующей процессы функционирования комплексных систем защиты информации. в том числе в условиях неопределенности и риска.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: «Цифровая культура», «Правоведение» и «Экономико-правовое сопровождение бизнеса».

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: «Внутренний аудит в системе контроля» и «Расследование экономических преступлений».

## 3. Планируемые результаты обучения

| Формируемые и контролируемые компетенции<br>(код и наименование)   | Индикаторы достижения компетенций<br>(код и наименование)   | Планируемые результаты обучения   |
|--|---|---|
| ОПК-5 -Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ. | ОПК 5.3 Применяет в профессиональной деятельности современные информационные технологии и программные средства                        | Знать: требования правовой и нормативной базы и внутренних регламентов в различных сферах профессиональной деятельности   |
|  |   | Уметь: применять информационно-коммуникационных технологии с учетом основных требований информационной безопасности для решения стандартных задач профессиональной деятельности |
|  |   | Владеть: навыками решения стандартных задач профессиональной деятельности с применением современных информационных технологий и программных средств                             |
| ОПК-6 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.   | ОПК-6.2 Понимает принцип работы современных информационных технологий и использует их для решения задач профессиональной деятельности | Знать: требования правовой и нормативной базы и внутренних регламентов в различных сферах профессиональной деятельности   |
|  |   | Уметь: применять современные технологии в ведении бухгалтерского учета и составления бухгалтерской (финансовой) отчетности  |
|  |   | Владеть: навыками применения информационных технологий в решение профессиональных задач   |

#### 4. Структура и содержание дисциплины

| Модуль (раздел)                        | Вид учебной работы | Наименование тем занятий (учебной работы)   | Семестр | Объем, ч. | Баллы | Интерактив, ч. | Формы текущего контроля (наименование оценочного средства) |
|--|--------------------|---|---------|-----------|-------|----------------|--|
| 1. Основы информационной безопасности. | Лек                | <i>Лекция 1.</i> Основные понятия и законодательная база информационной безопасности.   | 7       | 2         | -     | -              | Тестирование   |
|  | Пр                 |   |         | 3         |       |                |  |
|  | Ср                 |   |         | 16        |       |                |  |
|  | Лек                | <i>Лекция 2.</i> Основные подходы и требования к организации системы защиты информации на предприятиях и в организациях<br><i>Практическая работа № 1.</i> Анализ и оценка угроз безопасности защищаемой информации   | 7       | -         | 10    | -              | Тестирование<br>Отчёт по практической работе №1            |
|  | Пр                 |   |         | 3         |       |                |  |
|  | Ср                 |   |         | 16        |       |                |  |
|  | Лек                | <i>Лекция 3.</i> Кадрово-организационные и режимно-административные меры безопасности<br><i>Практическая работа № 2</i> Закрепление права предприятия на защиту информации в нормативных документах<br><i>Практическая работа № 3</i> Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации<br><i>Практическая работа №4</i> Обеспечение защиты информации при работе с кадрами | 7       | 2         | 20    | -              | Тестирование<br>Отчёты по практическим работам № 2,3,4     |
|  | Пр                 |   |         | 3         |       |                |  |
|  | Ср                 |   |         | 19        |       |                |  |
|  | Лек                | <i>Лекция 4.</i> Организация контроля доступа к информационным системам<br><i>Практическая работа № 5</i> Правовые нормы защиты информации в автоматизированных системах  | 7       | -         | 20    | -              | Тестирование<br>Отчёт по практической работе №5            |
|  | Пр                 |   |         | 3         |       |                |  |

| Модуль (раздел)               | Вид учебной работы | Наименование тем занятий (учебной работы)  | Семестр | Объем, ч. | Баллы | Интерактив, ч. | Формы текущего контроля (наименование оценочного средства) |
|-------------------------------|--------------------|--|---------|-----------|-------|----------------|--|
|                               | Ср                 |  |         | 16        |       |                |  |
|                               | Лек                | Лекция 5. Организация службы защиты информационной безопасности  | 7       | 2         | -     | -              | Тестирование   |
|                               | Пр                 |  |         | 3         |       |                |  |
|                               | Ср                 |  |         | 16        |       |                |  |
|                               | Лек                | Лекция 6. Экономическая эффективность защиты информации<br>Практическая работа № 6<br>Определение размера целесообразных затрат на обеспечение безопасности информации | 7       | -         | 20    | -              | Тестирование<br>Отчёт по практической работе №6            |
|                               | Пр                 |  |         | 3         |       |                |  |
|                               | Ср                 |  |         | 16        |       |                |  |
| 2. Экономическая безопасность | Лек                | Лекция 7. Теоретические основы экономической безопасности предприятия  | 7       | 2         | -     | -              | Тестирование   |
|                               | Пр                 |  |         | 3         |       |                |  |
|                               | Ср                 |  |         | 16        |       |                |  |
|                               | Лек                | Лекция 8. Основные угрозы экономической безопасности предприятия   | 7       | -         | -     | -              | Тестирование   |
|                               | Пр                 |  |         | 3         |       |                |  |
|                               | Ср                 |  |         | 16        |       |                |  |
|                               | Лек                | Лекция 9. Уровни экономической безопасности предприятия  | 7       | 2         | -     | -              | Тестирование   |
|                               | Пр                 |  |         | 3         |       |                |  |
|                               | Ср                 |  |         | 16        |       |                |  |
|                               | Лек                | Лекция 10. Критерии и индикаторы экономической безопасности предприятия  | 7       | 2         | 10    | -              | Тестирование<br>Отчёт по практической работе №7            |
|                               | Пр                 |  |         | 3         |       |                |  |

| Модуль (раздел)          | Вид учебной работы | Наименование тем занятий (учебной работы)   | Семестр | Объем, ч. | Баллы | Интерактив, ч. | Формы текущего контроля (наименование оценочного средства) |
|--------------------------|--------------------|---|---------|-----------|-------|----------------|--|
|                          | Ср                 | Практическая работа № 7.<br>Индикаторы финансовой безопасности  |         | 16        |       |                |  |
|                          | Лек                | Лекция 11. Прикладные и гуманитарные аспекты экономической безопасности.  | 7       | 2         | -     | -              | Тестирование   |
|                          | Пр                 |   |         | 3         |       |                |  |
|                          | Ср                 |   |         | 16        |       |                |  |
|                          | Лек                | Лекция 12. Анализ и оценка предпринимательских рисков.<br>Практическая работа № 8<br>Анализ и оценка предпринимательского риска | 7       | 2         | 10    | -              | Тестирование<br>Отчёт по практической работе №8            |
|                          | Пр                 |   |         | 3         |       |                |  |
|                          | Ср                 |   |         | 16        |       |                |  |
| Промежуточная аттестация |                    |   | 7       | 0,35      | -     | -              |  |
| Посещаемость             |                    |   | 7       |           | 10    |                |  |
| Контроль                 |                    |   | 7       | 35,65     | 100   | -              | Итоговое тестирование (Вопросы к экзамену)                 |
| Итого:                   |                    |   |         | 216       | 100   |                |  |

### Схема расчета итогового балла

(Текущий рейтинг + Результат итогового тестирования)/2

## 5. Образовательные технологии

С целью формирования компетенций у студентов в учебном процессе используется: технология традиционного обучения.

## 6. Методические указания по освоению дисциплины

Изучение дисциплины предусматривает чтение лекций, проведение практических занятий, самостоятельное изучение специальной литературы по вопросам программы, заданий из соответствующего практикума.

*Виды самостоятельной работы студентов:*

1. Повторение пройденного учебного материала, чтение рекомендованной литературы;
2. подготовка к практическим занятиям и лабораторной работе;
3. работа с электронными источниками;
4. подготовку к сдаче экзамена.

*Изучение теоретического материала* определяется рабочей учебной программой дисциплины, включенными в нее календарным планом изучения дисциплины и перечнем литературы; рекомендуется при подготовке к занятиям повторить материал предшествующих тем рабочего учебного плана, а также материал предшествующих учебных дисциплин, который служит базой изучаемого раздела данной дисциплины.

*При подготовке к практическому занятию* необходимо изучить материалы лекции, рекомендованную литературу. Изученный материал следует проанализировать в соответствии с планом занятия, затем проверить степень усвоения содержания вопросов.

*При подготовке к экзамену* следует руководствоваться перечнем вопросов для подготовки к итоговому контролю по курсу. При этом необходимо уяснить суть основных понятий дисциплины.

Самостоятельная работа студентов, прежде всего, заключается в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

Предполагается, что, прослушав лекцию, студент должен ознакомиться с рекомендованной литературой из основного списка, затем обратиться к источникам, указанным в библиографических списках изученных книг, осуществить поиск и критическую оценку материала на сайтах Интернет, собрать необходимую информацию.

## 7. Оценочные средства

### 7.1. Паспорт оценочных средств

| Семестр | Код контролируемой компетенции<br>(или ее части) | Наименование<br>оценочного средства  |
|---------|--|--|
| 7       | ОПК-5  | Тестирование<br>Отчёты по практическим работам № 1-8<br>Вопросы к экзамену |
| 7       | ОПК-6  | Тестирование<br>Отчёты по практическим работам № 1-8<br>Вопросы к экзамену |

### 7.2. Типовые задания или иные материалы, необходимые для текущего контроля

### 7.2.1. Типовые практические задания

#### Практическая работа 1

##### Задания:

Изучить факторы, определяющие состав угроз защищаемой информации и методику анализа и оценки возможностей доступа нарушителей к защищаемой информации.

Представить графическую схему, отражающую содержание основных этапов процедуры выявления угроз информации и основных категорий нарушителей; объяснить, каким образом действия нарушителей различных категорий оказывают влияние на обеспечение функционирования системы защиты информации.

Для реализации поставленных задач необходимо заполнить таблицу следующего вида:

| Категории<br>нарушителей | Дестабилизирующие воздействия |    |   |     |  |   |     |  |     |
|--------------------------|-------------------------------|----|---|-----|--|---|-----|--|-----|
|                          | Объекты защиты                |    |   |     |  |   |     |  |     |
|                          | I                             | II |   |     |  |   | ... |  | VII |
|                          |                               | A  | B | ... |  | Z |     |  |     |
|                          |                               |    |   |     |  |   |     |  |     |

Угрозы (A, B, C, Z)

A — вывод из строя основного оборудования;

B — перехват информации;

C — ...;

Z — физическое воздействие на информацию.

Объекты защиты (I, II, ..., X)

I — выделенные помещения;

II — средства обработки информации и связи;

III — ...;

X — системы обеспечения функционирования объекта.

Вербально-числовая оценка степени опасности дестабилизирующего воздействия (на пересечении клеток нарушителей и угроз)

— незначительная;

— малая;

— средняя;

— высокая.

Категории нарушителей:

- специалисты функциональных подразделений;
  - специалисты службы безопасности;
  - ...
- вспомогательный (технический) персонал.

##### Критерии оценки:

1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;

5 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

10 баллов - студент выполнил методические указания в полном объеме, отчет без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

## **Практическая работа 2**

### **Задания:**

Освоить метод правовой защиты служебной или коммерческой тайны на предприятии.

1. Определите название фирмы, выберите вид и область деятельности.
2. Составьте план мероприятий по защите коммерческой тайны (в соответствии с законом РФ «О коммерческой тайне»).
3. Укажите перечень внутрифирменных документов, которые будут использоваться в целях правовой защиты секретов вашей фирмы.
4. Составьте перечень сведений, составляющих коммерческую тайну вашей фирмы.
5. Опишите методы конкурентной разведки, которые будут использоваться вашей информационно-аналитической службой.
6. Отчет о выполненной работе оформляется в соответствии с общепринятыми требованиями и предоставляется преподавателю.

### **Критерии оценки:**

1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;

5 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчету;

8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчету;

10 баллов - студент выполнил методические указания в полном объеме, отчет без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

## **Практическая работа 3**

### **Задания:**

Освоить методы защиты конфиденциальной информации при использовании государственных систем лицензирования и сертификации. Для выбранного предприятия:

1. Обоснуйте необходимость проведения лицензирования выбранного вида деятельности.
2. Укажите порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности.
3. Укажите перечень сертификационных документов, необходимых для выбранной деятельности фирмы.
4. Составьте для вашей фирмы документы, необходимые для осуществления заданного вида деятельности.
5. Сформировать отчет о выполненной работе.

### **Критерии оценки:**

1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;

5 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчету;

8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчету;

10 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

#### Практическая работа 4

##### Задания:

Изучить методы защиты информации при профотборе сотрудников. Для выбранного предприятия:

1. Укажите основные мероприятия комплексного профотбора, проводимые службами безопасности фирмы в каждом случае.
2. Разработайте тест, который будет использоваться для проверки каждого из кандидатов.
3. Укажите особенности процедуры увольнения прежних работников с точки зрения обеспечения сохранности коммерческих секретов.
4. Составьте профили требований (профессиограммы) к данным сотрудникам.

| Качества работника           |  | Оценочная шкала |   |   |   |   |   |   |
|------------------------------|--|-----------------|---|---|---|---|---|---|
|                              |  | 1               | 2 | 3 | 4 | 5 | 6 | 7 |
| Административные             |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |
| Межличностные                |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |
| Интеллектуальные             |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |
| Психологическая устойчивость |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |
| Деловые                      |  |                 |   |   |   |   |   |   |
|                              |  |                 |   |   |   |   |   |   |

5. Сформировать отчет о выполненной работе.

##### Критерии оценки:

1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;

5 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

10 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

#### Практическая работа 5

##### Задания:

Освоить методы правовой защиты информации в автоматизированных системах. Для выбранного предприятия:

1. Оцените угрозы вашим информационным ресурсам (укажите наиболее вероятные виды компьютерных преступлений).
2. Укажите мероприятия, проводимые при создании системы защиты информации в вашей компьютерной сети.

3. Укажите перечень РД ГТК, учитываемых при разработке «Политики безопасности» на вашем предприятии.
4. Определите и обоснуйте требования по защите вашей конфиденциальной информации – группу и класс защищенности СВТ от НСД (с использованием РД ГТК).
5. Сформировать отчет о выполненной работе.

**Критерии оценки:**

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

10 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

16 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

20 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

**Практическая работа 6**

**Задания:**

Рассчитать смету затрат на обеспечение безопасности информации для выбранного предприятия, используя лекции по данной дисциплине, обоснуйте предложенные вами статьи затрат.

**Критерии оценки:**

2 балла - студент присутствовал на занятии, выполнил методические указания фрагментарно;

10 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

16 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

20 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

**Практическая работа 7**

**Задания:**

Сформировать матрицу рисков экономической безопасности бизнеса. Для формирования матрицы использовать виды рисков (экономические, финансовые, социальные, природные и техногенные, политические, информационные) и уровни реализации (нано-уровень, микро-уровень, мезо-уровень, макро-уровень, мега-уровень).

Рассчитать индикаторы финансовой безопасности, учитывая выбранную сферу бизнеса: индикаторы устойчивости федерального бюджета, индикаторы уровня долговой нагрузки предприятий и организаций, индикаторы достаточности золотовалютных резервов, индикаторы макрофинансовых условий функционирования экономики, индикаторы соотношения сбережений и инвестиций в экономике, индикаторы банковской деятельности, индикаторы состояния и процессов финансового рынка.

**Критерии оценки:**

1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;

5 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

10 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

## **Практическая работа 8**

### **Задания:**

Провести анализ и оценку предпринимательского риска для выбранного предприятия: материальные потери, трудовые потери, финансовые потери, потери времени, специальные виды потерь. Предложить способы минимизации риска.

### **Критерии оценки:**

1 балл - студент присутствовал на занятии, выполнил методические указания фрагментарно;

5 баллов - студент выполнил методические указания не в полном объеме, есть замечания по отчёту;

8 баллов - студент выполнял методические указания в полном объеме, но есть замечания по отчёту;

10 баллов - студент выполнил методические указания в полном объеме, отчёт без замечаний, ответы содержательные и полные, применён творческий подход к выполнению задания.

## **7.2.2. Типовые вопросы из банка тестовых заданий для тестирования**

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

- 1) политическая разведка;
- 2) промышленный шпионаж;
- 3) добросовестная конкуренция;
- 4) конфиденциальная информация;
- 5) правильного ответа нет.

2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности ?

- 1) любая информация;
- 2) только открытая информация;
- 3) запатентованная информация;
- 4) закрываемая собственником информация;
- 5) коммерческая тайна.

3. Кто может быть владельцем защищаемой информации?

- 1) только государство и его структуры;
- 2) предприятия акционерные общества, фирмы;
- 3) общественные организации;
- 4) только вышеперечисленные;
- 5) кто угодно.

4. Какие сведения на территории РФ могут составлять коммерческую тайну?
- 1) учредительные документы и устав предприятия;
  - 2) сведения о численности работающих, их заработной плате и условиях труда;
  - 3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
  - 4) другие;
  - 5) любые.
5. Какие секретные сведения входят в понятие «коммерческая тайна»?
- 1) связанные с производством;
  - 2) связанные с планированием производства и сбытом продукции;
  - 3) технические и технологические решения предприятия;
  - 4) только 1 и 2 вариант ответа;
  - 5) три первых варианта ответа.
6. Что называют источником конфиденциальной информации?
- 1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;
  - 2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
  - 3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
  - 4) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
  - 5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.
7. Как называют процессы обмена информацией с помощью официальных, деловых документов?
- 1) непосредственные;
  - 2) межличностные;
  - 3) формальные;
  - 4) неформальные;
  - 5) конфиденциальные.
8. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?
- 1) хищение носителей информации;
  - 2) использование технических средств для перехвата электромагнитных ПЭВМ;
  - 3) разглашение;
  - 4) копирование программой информации с носителей;
  - 5) другое.
9. Каким образом происходит разглашение конфиденциальной информации?
- 1) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;
  - 2) опубликование материалов в печати;
  - 3) сообщение, передача, предоставление в ходе информационного обмена;
  - 4) все вышеперечисленные способы;
  - 5) правильного варианта ответа нет.

10. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

- 1) получить, изменить, а затем передать ее конкурентам;
- 2) размножить или уничтожить ее;
- 3) получить, изменить или уничтожить;
- 4) изменить и уничтожить ее;
- 5) изменить, повредить или ее уничтожить.

11. Какой самый прямой и эффективный способ склонения к сотрудничеству?

- 1) психическое давление;
- 2) подкуп;
- 3) преследование;
- 4) шантаж;
- 5) угрозы.

12. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?

- 1) инициативное сотрудничество;
- 2) пытки;
- 3) наблюдение;
- 4) хищение;
- 5) копирование.

13. Какое из утверждений неверно?

- 1) подкуп — сложный процесс, требует долгой и кропотливой работы;
- 2) пытки — это стремление путем внешне наивных вопросов получить определенные сведения;
- 3) процесс наблюдения не сложен, так как не требует затрат сил и средств;
- 4) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;
- 5) негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.

14. Завершающим этапом любого сбора конфиденциальной информации является

- 1) копирование;
- 2) подделка;
- 3) аналитическая обработка;
- 4) фотографирование;
- 5) наблюдение.

15. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?

- 1) ненадежность;
- 2) угроза;
- 3) несчастный случай;
- 4) авария;
- 5) правильного ответа среди перечисленных нет.

16. Что в скором времени будет являться главной причиной информационных потерь?

- 1) материальный ущерб, связанный с несчастными случаями;
- 2) кража и преднамеренная порча материальных средств;
- 3) информационные инфекции;
- 4) аварии и выход из строя аппаратуры, программ и баз данных;
- 5) ошибки эксплуатации.

17. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

- 1) логические бомбы, троянский конь, червь, вирус;
- 2) червь, вирус логические бомбы, троянский конь;
- 3) червь логические бомбы вирус, троянский конь;
- 4) логические бомбы, вирус, троянский конь червь;
- 5) вирус, логические бомбы, троянский конь червь.

18. Причины связанные с информационным обменом приносящие наибольшие убытки?

- 1) остановка или выход из строя информационных систем;
- 2) потери информации;
- 3) неискренность;
- 4) проникновение в информационную систему;
- 5) перехват информации.

19. Какие цели преследуются при активном вторжении в линии связи?

- 1) анализ информации(содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
- 2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприимчивость передаче сообщений;
- 3) инициализация ложных соединений;
- 4) варианты 1 и 2;
- 5) варианты 2 и 3.

20. Что определяет модель нарушителя?

- 1) категории лиц, в числе которых может оказаться нарушитель;
- 2) возможные цели нарушителя и их градации по степени важности и опасности;
- 3) предположения о его квалификации и оценка его технической вооруженности;
- 4) ограничения и предположения о характере его действий;
- 5) все выше перечисленные.

21. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.

- 1) ознакомление с информационной системой или вычислительной сетью;
- 2) похитить программу или иную информацию;
- 3) оставить записку, выполнить, уничтожить или изменить программу;
- 4) вариант 2 и 3;
- 5) вариант 1, 2 и 3.

22. Какое из утверждений неверно?

- 1) наблюдается тенденция к стремительному росту попыток получить несанкционированный доступ к информационным системам или вычислительным сетям;
- 2) недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования;
- 3) считается, что компьютерные преступления, более легкий путь добывания денег, чем

ограбление банков;

4) очень малое число фирм могут пострадать от хакеров;

5) к категории хакеров-профессионалов обычно относят: преступные группировки, преследующие политические цели.

23. Какое из утверждений неверно?

1) хакеры могут почерпнуть много полезной информации из газет и других периодических изданий;

2) хакерами часто используется завязывание знакомств для получения информации о вычислительной системе или выявления служебных паролей;

3) один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации и доступа к ЭВМ — просто изучая черновые распечатки;

4) о перехвате сообщений в каналах связи речь может идти лишь в связи с деятельностью военных или секретных служб;

5) после получения необходимого объема предварительной информации, компьютерный хакер-профессионал осуществляет непосредственное вторжение в систему.

24. Какое из утверждений неверно?

1) наибольшие убытки (в среднем) приносит саботаж в нематериальной сфере;

2) убытки, связанные с забастовками не превышают убытков связанных с аварией оборудования;

3) уход ведущих специалистов опасен для малых центров;

4) хищения, в первую очередь осуществляются сотрудниками предприятия или пользователями;

5) аварии оборудования или основных элементов системы являются мало распространенными и определяются надежностью аппаратуры.

25. Метод скрытия — это...

1) максимальное ограничение числа секретов, из-за допускаемых к ним лиц;

2) максимального ограничения числа лиц, допускаемых к секретам;

3) уменьшение числа секретов неизвестных большинству сотрудников;

4) выбор правильного места, для утаивания секретов от конкурентов;

5) поиск максимального числа лиц, допущенных к секретам.

26. Что включает в себя ранжирование как метод защиты информации?

1) регламентацию допуска и разграничение доступа к защищаемой информации;

2) деление засекречиваемой информации по степени секретности;

3) наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;

4) вариант ответа 1 и 2;

5) вариант ответа 1, 2 и 3.

27. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?

1) скрытие;

2) дезинформация;

3) дробление;

4) кодирование;

5) шифрование.

28. Что в себя морально-нравственные методы защиты информации?

1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и

убеждений;

- 2) контроль работы сотрудников, допущенных к работе с секретной информацией;
- 3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
- 4) вариант ответа 1 и 3;
- 5) вариант ответа 1, 2 и 3.

29. Какое из выражений неверно?

- 1) страхование — как метод защиты информации пока еще не получил признания;
- 2) кодирование — это метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации;
- 3) шифрование может быть предварительное и линейное;
- 4) дирекция очень часто не может понять необходимость финансирования безопасности;
- 5) безопасность предприятия — не стабильное состояние предприятия, не поддающееся прогнозированию во времени.

30. Какой должна быть защита информации с позиции системного подхода?

- 1) безопасной для сотрудников;
- 2) активной;
- 3) универсальной;
- 4) надежной;
- 5) непрерывной.

31. Что такое «служба безопасности»?

- 1) система внештатных формирований, предназначенных для обеспечения безопасности объекта;
- 2) структурное подразделение, предназначенное для охраны помещений и территорий предприятия;
- 3) система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации;
- 4) структурное подразделение, предназначенное для хранения и выдачи документов, носителей конфиденциальной информации;
- 5) структурное подразделение, задача которого: подбор персонала и работа с сотрудниками.

32. Кому подчиняется служба безопасности?

- 1) владельцу предприятия;
- 2) владельцу предприятия и лицу которому тот подчиняется;
- 3) руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;
- 4) заместителю руководителя предприятия по организационным вопросам;
- 5) только начальнику службы безопасности.

33. Какие задачи не входят в круг обязанностей службы безопасности ?

- 1) внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической безопасности предприятия;
- 2) определение участков сосредоточения сведений, составляющих коммерческую тайну;
- 3) определение на предприятии технологического оборудования, выход из строя которого может привести к большим экономическим потерям;
- 4) ограничение круга сторонних предприятий, работающих с данным предприятием, на которых возможен выход из-под контроля сведений составляющих коммерческую тайну

предприятия;

5) определение круга сведений, составляющих коммерческую тайну.

34. Какие средства использует инженерно-техническая защита (по функциональному назначению)?

- 1) программные, аппаратные, криптографические, технические;
- 2) программные, физические, шифровальные, криптографические;
- 3) программные, аппаратные, криптографические физические;
- 4) физические, аппаратные, материальные, криптографические;
- 5) аппаратные, физические, программные, материальные.

35. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?

- 1) в Конституции РФ;
- 2) в Законе об оперативно розыскной деятельности;
- 3) в Законе об частной охране и детективной деятельности;
- 4) в Законе об информации, информатизации и защите информации;
- 5) в Указе Президента РФ № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации».

36. На какую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны

- 1) Министерство Информатики РФ;
- 2) Комитет по Использованию Информации при Госдуме;
- 3) Росинформресурс;
- 4) все выше перечисленные;
- 5) правильного ответа нет.

37. На каком уровне защиты информации создаются комплексные системы защиты информации?

- 1) на организационно-правовом;
- 2) на социально политическом;
- 3) на тактическом;
- 4) на инженерно-техническом;
- 5) на всех вышеперечисленных.

38. Какие существуют наиболее общие задачи защиты информации на предприятии?

- 1) снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной;
- 2) предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
- 3) документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
- 4) создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;
- 5) все вышеперечисленные.

39. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?

- 1) воспитание понимания важности сохранения в тайне доверенных им секретных или конфиденциальных сведений;
- 2) подбор людей, допускаемых к секретным работам;
- 3) обучение лиц, допущенных к секретам, правилам их сохранения;
- 4) добровольное согласие на запрет работы по совместительству у конкурентов;

5) стимулирование заинтересованности работы с засекреченной информацией и сохранения этих сведений в тайне.

40. В каком документе содержатся основные требования к безопасности информационных систем в США?

- 1) в красной книге;
- 2) в желтой прессе;
- 3) в оранжевой книге;
- 4) в черном списке;
- 5) в красном блокноте.

### **Критерии оценки:**

Баллы выставляются пропорционально правильным ответам на тестовые вопросы автоматически. Максимум – 100 баллов.

## **7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины**

### **7.3.1. Вопросы к промежуточной аттестации**

Семестр 7

| № п/п | Вопросы к экзамену  |
|-------|---|
| 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 реализации информационных угроз. |
| 14    | Способы воздействия информационных угроз на объекты.  |
| 15    | Внешние и внутренние субъекты информационных угроз.   |
| 16    | Компьютерные преступления и их классификация.   |
| 17    | Вредоносные программы, их виды.   |
| 18    | Государственное регулирование информационной безопасности.  |
| 19    | Деятельность международных организаций в сфере информационной безопасности.                                       |
| 20    | Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.                         |
| 21    | Доктрина информационной безопасности России.  |
| 22    | Федеральные законы по ИБ в РФ.  |

| № п/п | Вопросы к экзамену   |
|-------|--|
| 23    | Политика безопасности и ее принципы.   |
| 24    | Фрагментарный и системный подход к защите информации.                                    |
| 25    | Методы и средства защиты информации.   |
| 26    | Организационное обеспечение ИБ.  |
| 27    | Организация конфиденциального делопроизводства.  |
| 28    | Защита информации в Интернете.   |
| 29    | Защита от компьютерных вирусов.  |
| 30    | Организация системы защиты информации экономических объектов.                            |
| 31    | Этапы построения системы защиты информации.  |
| 32    | Оценка эффективности инвестиций в информационную безопасность.                           |
| 33    | Управление информационной безопасностью на государственном уровне.                       |
| 34    | Менеджмент и аудит информационной безопасности на уровне предприятия.                    |
| 35    | Информационная безопасность предпринимательской деятельности.                            |
| 36    | Обеспечение информационной безопасности должностных лиц и представителей деловых кругов. |
| 37    | Каковы основные типы угроз экономической безопасности?                                   |
| 38    | Что должно стать итогом реализации Стратегии экономической безопасности?                 |
| 39    | Назовите основные уровни реализации экономической безопасности                           |
| 40    | Какие индикаторы финансовой безопасности Вам известны?                                   |

### 7.3.2. Критерии и нормы оценки

| Семестр | Форма проведения промежуточной аттестации | Критерии и нормы оценки          |  |
|---------|---|----------------------------------|--|
| 7       | экзамен                                   | Отлично (зачтено)                | Студент набрал 85 и более баллов по накопительному рейтингу  |
|         |   | Хорошо (зачтено)                 | Студент набрал от 70 до 84 баллов по накопительному рейтингу |
|         |   | Удовлетворительно (зачтено)      | Студент набрал от 55 до 69 баллов по накопительному рейтингу |
|         |   | Неудовлетворительно (не зачтено) | Студент набрал 54 и менее баллов по накопительному рейтингу  |

## 8. Учебно-методическое и информационное обеспечение дисциплины

### 8.1. Обязательная литература

| №<br>п/п | Авторы, составители            | Заглавие (заголовок)                            | Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.) | Год издания | Количество в научной библиотеке /<br>Наименование ЭБС |
|----------|--------------------------------|---|---|-------------|---|
| 1.       | Баранова Е.К., Бабаш А.В.      | Информационная безопасность и защита информации | учебное пособие   | 2021        | ЭБС<br>"ZNANIUM.COM"                                  |
| 2.       | Под общ. ред. С.А. Коноваленко | Экономическая безопасность                      | учебник   | 2021        | ЭБС<br>"ZNANIUM.COM"                                  |
| 3.       | Партыка Т.Л., Попов И.И.       | Информационная безопасность                     | учебное пособие   | 2019        | ЭБС<br>"ZNANIUM.COM"                                  |

### 8.2. Дополнительная литература

| №<br>п/п | Авторы, составители                  | Заглавие (заголовок)   | Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.) | Год издания | Количество в научной библиотеке /<br>Наименование ЭБС |
|----------|--------------------------------------|--|---|-------------|---|
| 1        | Коллектив авторов: Бобошко Н.М. и др | Актуальные проблемы обеспечения экономической безопасности   | Сборник научных трудов  | 2016        | ЭБС<br>"ZNANIUM.COM"                                  |
| 2        | Беловицкий К.Б., Николаев В.Г.       | Методы, модели, средства хранения и обработки данных         | учебник   | 2017        | ЭБС<br>"ZNANIUM.COM"                                  |
| 3        | Васильков А.В., Васильков И.А.       | Безопасность и управление доступом в информационных системах | Учебное пособие   | 2019        | ЭБС<br>"ZNANIUM.COM"                                  |

### 8.3. Перечень профессиональных баз данных и информационных справочных систем

- КонсультантПлюс — Режим доступа к журн.: <http://www.consultant.ru/>
- Гарант.РУ [Электронный ресурс] : информационно-правовой портал — Режим доступа к журн.: <http://www.garant.ru/>
- Scopus [Электронный ресурс]: реферативная база данных. – Netherlands: Elsevier, 2021. – Режим доступа: [scopus.com](http://scopus.com). – Загл. с экрана. – Яз. рус., англ.
- Elibrary [Электронный ресурс]: научная электронная библиотека. – Москва: НЭБ, 2021. – Режим доступа: [elibrary.ru](http://elibrary.ru). – Загл. с экрана. – Яз. рус., англ.

### 8.4. Перечень программного обеспечения

| № п/п | Наименование ПО                    | Реквизиты договора<br>(дата, номер, срок действия)  |
|-------|------------------------------------|---|
| 1     | Windows                            | Договор № 690 от 19.05.2015г., срок действия - бессрочно  |
| 2     | Office Standart                    | Договор № 690 от 19.05.2015г., срок действия - бессрочно;<br>Договор № 727 от 20.07.2016г., срок действия - бессрочно |
| 3     | Mirapolis Human Capital Management | № 42/02/22-К от 02.02.2022 до 31.08.2022  |

### 8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

| № п/п | Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)   | Перечень основного оборудования  |
|-------|---|--|
| 1     | Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (С-709) | Стол� ученические двухместные (моноблок), стол ученический двухместный, стол преподавательский, стул преподавательский , доска аудиторная (маркерная), доска аудиторная (меловая), трибуна , проектор, экран; компьютер .                  |
| 3     | Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (С-807)  | Стол� ученические двухместные, Стол� преподавательские, стулья, доска аудиторная (маркерная), доска аудиторная (меловая), экран, кресло., шкафы, стенды, электроцит, огнетушитель, ПК, принтер, компьютер, монитор, проектор, беспроводной |

| №<br>п/п | Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)   | Перечень основного оборудования                                     |
|----------|---|---|
|          |   | маршрутизатор , принтер.  |
| 4        | Компьютерный класс. Помещение для самостоятельной работы. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации (Г-401) | Стол� ученические, стулья ученические, ПК с выходом в сеть Интернет |