**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ**

**УТВЕРЖДАЮ**

Директор/Декан
института экономики, финансов и управления в АПК
Гунько Юлия Александровна
_____
_____
«___» _____ 20___ г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

## Б1.О.28 Информационная безопасность

38.03.05 Бизнес-информатика

Электронный бизнес

бакалавр

очная

Ставрополь, 2025

**1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

| Код и наименование компетенции | Код и наименование индикатора достижения | Перечень планируемых результатов обучения по дисциплине |
|---|---|---|
| ПК-2 Управление операционной деятельностью организации в области ИТ | ПК-2.3 Управление информационной безопасностью | **знает** как управлять операционной деятельностью организации в области ИТ |
| | | **умеет** управлять информационной безопасностью |
| | | **владеет навыками** навыками управления информационной безопасностью |

**2. Перечень оценочных средств по дисциплине**

| № | Наименование раздела/темы | Семестр | Код индикаторов достижения компетенций | Оценочное средство проверки результатов достижения индикаторов компетенций |
|---|---|---|---|---|
| 1. | 1 раздел. 1 | | | |
| 1.1. | Общая характеристика информационной безопасности. Угроза (утечка) информации | 5 | ПК-2.3 | Тест |
| 1.2. | КТ 1 | 5 | ПК-2.3 | Тест |
| 1.3. | Уровни информационной безопасности | 5 | ПК-2.3 | Устный опрос |
| 1.4. | КТ 2 | 5 | ПК-2.3 | Тест |
| 1.5. | Политика информационной без-опасности и формирование методов защиты информационных ресурсов | 5 | ПК-2.3 | Устный опрос |
| | Промежуточная аттестация | | | Эк |

**3. Оценочные средства (оценочные материалы)**

Примерный перечень оценочных средств для текущего контроля успеваемости и промежуточной аттестации

| № п/п | Наименование оценочного средства | Краткая характеристика оценочного средства | Представление оценочного средства в фонде (Оценочные материалы) |
|---|---|---|---|
| Текущий контроль | | | |
| | Для оценки знаний | | |

| | | | |
|---|---|---|---|
| 1 | Устный опрос | Средство контроля знаний студентов, способствующее установлению непосредственного контакта между преподавателем и студентом, в процессе которого преподаватель получает широкие возможности для изучения индивидуальных особенностей усвоения студентами учебного материала. | Перечень вопросов для устного опроса |
| 2 | Тест | Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. | Фонд тестовых заданий |
| | Для оценки умений | | |
| | Для оценки навыков | | |
| | Промежуточная аттестация | | |
| 3 | Экзамен | Средство контроля усвоения учебного материала и формирования компетенций, организованное в виде беседы по билетам с целью проверки степени и качества усвоения изучаемого материала, определить необходимость введения изменений в содержание и методы обучения. | Комплект экзаменационных билетов |

**4. Примерный фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) "Информационная безопасность"**

***Примерные оценочные материалы для текущего контроля успеваемости***

Тестовые задания по дисциплине «Информационная безопасность»

1. Информационная безопасность — это:
а) состояние защищённости информации и информационных систем от угроз;
б) только установка антивирусной программы;
в) только хранение документов в архиве;
г) только ограничение доступа в помещение.

2. Конфиденциальность информации означает:
а) защиту информации от несанкционированного доступа;
б) возможность изменения информации любым пользователем;
в) удаление информации после использования;
г) свободное распространение информации.

3. Целостность информации предполагает:
а) сохранение точности и полноты данных;
б) открытый доступ к информации;
в) обязательное удаление устаревших файлов;
г) отсутствие резервного копирования.

4. Доступность информации означает:
а) возможность получения информации уполномоченными пользователями в нужное время;
б) свободный доступ для всех пользователей;
в) запрет на использование информационных систем;
г) обязательную публикацию данных в сети Интернет.

5. Угроза информационной безопасности — это:
а) потенциальная возможность нарушения безопасности информации;
б) способ ускорения работы компьютера;
в) метод создания базы данных;
г) средство форматирования документа.

6. Несанкционированный доступ — это:
а) получение доступа к информации без соответствующих прав;
б) вход пользователя в систему по своему логину и паролю;
в) резервное копирование данных;
г) обновление программного обеспечения.

7. К вредоносному программному обеспечению относится:
а) компьютерный вирус;
б) текстовый редактор;
в) электронная таблица;
г) графический редактор.

8. Антивирусное программное обеспечение предназначено для:
а) обнаружения, блокирования и удаления вредоносных программ;
б) создания презентаций;
в) проектирования баз данных;
г) печати документов.

9. Парольная защита используется для:
а) аутентификации пользователя и ограничения доступа;
б) увеличения яркости экрана;
в) удаления временных файлов;
г) изменения формата изображения.

10. Резервное копирование необходимо для:
а) восстановления данных при их потере или повреждении;
б) ускорения набора текста;
в) удаления программ;
г) изменения настроек монитора.

11. Политика информационной безопасности организации — это:
а) совокупность правил и требований по защите информации;
б) список сотрудников организации;
в) рекламный документ предприятия;
г) график проведения совещаний.

12. К организационным мерам защиты информации относится:

а) разработка инструкций, распределение прав доступа, обучение сотрудников;
б) только покупка нового компьютера;
в) только замена офисной мебели;
г) только установка принтера.

13. К техническим средствам защиты информации относится:
а) межсетевой экран;
б) текстовый документ;
в) калькулятор;
г) презентация.

14. Инцидент информационной безопасности — это:
а) событие, которое может привести к нарушению безопасности информации;
б) плановое обновление программ;
в) обычное включение компьютера;
г) создание нового файла.

15. Основная цель защиты информации — это:
а) предотвращение утечки, искажения, уничтожения и несанкционированного доступа к данным;
б) увеличение количества документов;
в) замена всех сотрудников;
г) отказ от использования информационных технологий.

***Примерные оценочные материалы***
***для проведения промежуточной аттестации (зачет, экзамен)***
***по итогам освоения дисциплины (модуля)***

Вопросы для подготовки к экзамену

1. Дайте характеристику понятие секретной информации.
2. Охарактеризуйте понятие коммерческой тайны.
3. Что такое разрушение информации?
4. Методы уменьшения опасности компьютерных вирусов.
5. Классификация информации по уровню доступа.
6. Что такое открытая информация?
7. Что такое информация ограниченного доступа?
8. Конфиденциальность информации.
9. Целостность информации.
10. Доступность информации.
11. Понятие информационной безопасности.
12. Основные составляющие информационной безопасности.
13. Законодательный уровень информационной безопасности.
14. Обзор российского законодательства в области информационной безопасности.
15. Обзор зарубежного законодательства в области информационной безопасности.
16. Основные классы мер процедурного уровня.
17. Информационная инфраструктура.
18. Основные классы мер процедурного уровня.
19. Физическая защита.
20. Критичные ресурсы.
21. Реагирование на нарушения режима безопасности.
22. Основные понятия административного уровня ИБ.
23. Программа безопасности.
24. Политика безопасности.
25. Политика безопасности нижнего уровня.
26. Синхронизация программы безопасности с жизненным циклом систем.
27. Контроль деятельности в области безопасности.
28. Охарактеризуйте понятие АС.
29. Охарактеризуйте информационную безопасность.
30. Охарактеризуйте понятие угрозы информационной безопасности.
31. Классификация угроз по природе возникновения.
32. Классификация угроз по степени преднамеренности возникновения.
33. Классификация угроз по положению источника.
34. Классификация угроз по степени воздействия на АС.
35. Технические каналы утечки информации.
36. Функциональные каналы утечки информации и условия их образования.
37. Специальные каналы утечки информации и механизмы их возникновения.
38. Процедурный уровень информационной безопасности.
39. Физическая защита информации.
40. Анализ угроз ИБ объекта.
41. Методы и средства обеспечения ИБ на объектах связи специального назначения.
42. Модели нарушителя и угроз безопасности объекта.
43. Методы и средства ограничения доступа к информации и компонентам ЭВМ.
44. Привязка программного обеспечения к аппаратному окружения и физическим носителям.
45. Защита компьютерной информации и компьютерных систем от вредоносных программ.
46. История криптографии.
47. Простейшие шифры и их свойства. Стойкость шифров. Композиции шифров. Влияние криптографических средств на информационную безопасность.
48. Проблемы и методы информационной войны.
49. Методы иностранных технических разведок по ведению информационной войны их возможности.

***Темы письменных работ (эссе, рефераты, курсовые работы и др.)***

1. Понятие информационной безопасности и её роль в деятельности организации.
2. Основные угрозы информационной безопасности.
3. Классификация информации по уровню доступа.
4. Конфиденциальность, целостность и доступность информации.
5. Коммерческая тайна как объект защиты.
6. Персональные данные и особенности их защиты.
7. Правовое регулирование информационной безопасности в Российской Федерации.
8. Организационные меры защиты информации.
9. Технические средства защиты информации.
10. Программные средства защиты информации.
11. Компьютерные вирусы и методы защиты от вредоносного программного обеспечения.
12. Политика информационной безопасности организации.
13. Роль администратора в обеспечении информационной безопасности.
14. Защита данных в корпоративных информационных системах.
15. Резервное копирование и восстановление информации.
16. Защита информации при работе в сети Интернет.
17. Аутентификация и разграничение прав доступа пользователей.
18. Реагирование на инциденты информационной безопасности.
19. Информационная безопасность в электронном бизнесе.
20. Современные средства и технологии защиты информации.