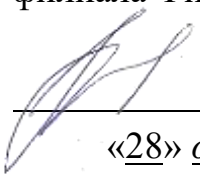
Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Липецкий филиал Финуниверситета

Кафедра «Учет и информационные технологии в бизнесе»

УТВЕРЖДАЮ
Заместитель
директора по учебно-
методической работе Липецкого
филиала Финуниверситета



_____О.Н. Левчегов
«28» *октября* 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
ОП.10 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

09.02.13 Интеграция решений с применением
технологий искусственного интеллекта

Липецк 2026

Фонд оценочных средств по учебной дисциплине «Основы информационной безопасности» разработан на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта.

Разработчик:

Черпаков И.В., доцент кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Рабочая программа учебной дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии общепрофессионального цикла

Протокол от 28.10.2026 г. №1

Председатель предметной (цикловой) комиссии общепрофессионального цикла  Е.Е. Кукина

1. Кодификатор фонда оценочных средств

Наименование учебной дисциплины: «Основы информационной безопасности»

Планируемые результаты освоения учебной дисциплины:

Код общих и профессиональных компетенций	Умения	Знания
ОК 02 ОК 03 ОК 04 ОК 06 ОК 07 ПК 2.1 ПК 2.2 ПК 2.3	- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации; -применять нормативные правовые акты и нормативные методические документы в области защиты информации; -контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники; -проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; -оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; -защищать свои права в соответствии с трудовым законодательством.	-Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; - правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны информации; - нормативные документы в области обеспечениязащиты информации ограниченного доступа; - организацию ремонтного обслуживания аппаратуры и средств защиты информации; - принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации информации; -принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; -основные принципы действия и характеристики, порядок технического обслуживания,

		устранение неисправностей и организацию ремонта технических средств защиты информации; -правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); -нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе; -законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

2. Оценочные материалы

ОК 02: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

1. Какой официальный интернет-ресурс содержит нормативные документы по информационной безопасности в РФ?

А) Википедия
Б) сайт ФСТЭК России (fstec.ru)
В) социальные сети

2. Для анализа защищённости информационной системы наиболее достоверным источником информации является:

А) форумы
Б) официальная документация производителей и базы уязвимостей (CVE, БДУ ФСТЭК)
В) рекламные сайты

3. Какой инструмент позволяет автоматизировать поиск уязвимостей в информационной системе?

А) сканеры уязвимостей (OpenVAS, Nessus, MaxPatrol)
Б) текстовый редактор
В) графический редактор

4. Как называется база данных уязвимостей, поддерживаемая ФСТЭК России (аббревиатура)?

ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях

5. Какой федеральный закон регулирует защиту персональных данных в РФ?

А) Федеральный закон № 152-ФЗ «О персональных данных»

Б) Трудовой кодекс

В) Гражданский кодекс

6. Какой федеральный закон регулирует отношения в области обеспечения информационной безопасности?

А) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Б) Налоговый кодекс

В) Уголовный кодекс

7. Для повышения квалификации в области информационной безопасности наиболее эффективным способом является:

А) прохождение курсов, сертификаций (CISSP, CISM) и изучение нормативных документов

Б) игнорирование новых угроз

В) работа без обучения

8. Как называется документ, определяющий политику организации в области информационной безопасности?

ОК 04: Эффективно взаимодействовать и работать в коллективе и команде

9. При командной работе над обеспечением информационной безопасности наиболее эффективным способом взаимодействия является:

А) распределение ролей: администратор безопасности, аналитик, аудитор

Б) работа без обсуждения

В) выполнение всей работы одним человеком

10. Для оперативного оповещения команды об инцидентах информационной безопасности удобнее всего использовать:

А) системы оповещения и тикет-системы (Jira, ServiceDesk)

Б) бумажные носители

В) устные договорённости без фиксации

11. При возникновении разногласий в команде по поводу мер защиты информации необходимо:

А) принять решение большинством голосов без обсуждения

Б) выслушать аргументы и выбрать решение на основе нормативных требований и оценки рисков

В) прекратить обсуждение

12. Как называется процесс обучения сотрудников правилам информационной безопасности?

ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

13. Что является проявлением антикоррупционного поведения специалиста по информационной безопасности?

А) отказ от использования служебного доступа к данным в личных целях
Б) передача паролей коллегам для удобства
В) использование служебного положения для получения выгоды

14. Какой федеральный закон регулирует основы противодействия коррупции в РФ?

А) Федеральный закон № 273-ФЗ «О противодействии коррупции»
Б) Трудовой кодекс
В) Гражданский кодекс

15. Что является нарушением этических норм при работе с информацией ограниченного доступа?

А) разглашение конфиденциальных данных третьим лицам
Б) соблюдение режима конфиденциальности
В) работа с данными в рамках должностных обязанностей

16. Как называется преступление, заключающееся в получении должностным лицом денег за незаконные действия?

ОК 07: Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

17. При организации работы серверного оборудования для снижения энергопотребления наиболее эффективным способом является:

А) виртуализация и оптимизация загрузки серверов
Б) работа всех серверов на максимальной мощности
В) отказ от охлаждения

18. Какой принцип бережливого производства применим к обработке данных?

А) минимизация избыточности данных и оптимизация хранения
Б) хранение всех данных без ограничений
В) дублирование всех данных

19. При чрезвычайной ситуации (например, отключении электричества) для сохранности данных необходимо:
А) использовать источники бесперебойного питания (ИБП) и резервное копирование
Б) отключить все системы
В) продолжить работу без защиты

20. Как называется процесс повторного использования компонентов компьютерной техники (например, серверов)?

ПК 2.1: Выявлять проблемы, возникающие в процессе эксплуатации баз данных.
21. Как называется проблема, возникающая при дублировании данных в нескольких таблицах?
А) избыточность данных
Б) целостность данных
В) индексация

22. При медленной работе запросов к базе данных наиболее вероятной причиной является:
А) отсутствие индексов на часто используемых полях
Б) слишком много таблиц
В) мало данных

23. Как называется ситуация, когда запись в подчинённой таблице ссылается на несуществующую запись в главной таблице?
А) нарушение целостности данных
Б) нормализация
В) индексация

24. Как называется процесс проверки базы данных на наличие ошибок и проблем?

ПК 2.2: Осуществлять процедуры администрирования баз данных.
25. Для обеспечения сохранности данных при сбое оборудования необходимо регулярно выполнять:
А) резервное копирование (бэкап)
Б) удаление старых записей
В) изменение структуры таблиц

26. Какой инструмент позволяет управлять правами доступа пользователей к базе данных?
А) СУБД (например, MySQL, PostgreSQL, MS SQL)
Б) текстовый редактор
В) графический редактор

27. Как называется процедура восстановления базы данных из резервной копии?
А) восстановление (restore)
Б) удаление
В) архивация

28. Как называется учётная запись с максимальными правами доступа в базе данных?

ПК 2.3: Проводить аудит систем безопасности баз данных с использованием регламентов по защите информации
29. При аудите безопасности базы данных в первую очередь проверяют:
А) права доступа пользователей и наличие шифрования данных
Б) цвет интерфейса
В) скорость набора текста

30. Какой нормативный документ регламентирует защиту информации в информационных системах?
А) Приказы ФСТЭК России
Б) рекламные буклеты
В) инструкции по охране труда

31. Что является результатом аудита системы безопасности базы данных?
А) отчёт с выявленными уязвимостями и рекомендациями по их устранению
Б) удаление всех данных
В) отказ от дальнейшей работы

32. Как называется процесс проверки соответствия системы безопасности базы данных установленным требованиям?

3.Критерии оценки

Объем выполнения	Оценка	Критерии оценки
от 61 до 70	«отлично»	- теоретическое содержание дисциплины освоено полностью, сформированы необходимые практические навыки и умения, выполнены все задания.
от 49 до 60	«хорошо»	теоретическое содержание дисциплины освоено полностью, сформированы необходимые практические навыки и умения не в полном объеме, выполнены все задания, при выполнении которых были обнаружены ошибки и недочеты.

от 35 до 48	«Удовлетворительно»	теоретическое содержание дисциплины освоено частично, но пробелы не носят существенного характера, сформированы в основном необходимые практические навыки и умения, выполнено большинство заданий, при выполнении которых были обнаружены ошибки и недочеты.
от 0 до 34	«Неудовлетворительно»	теоретическое содержание дисциплины не освоено, не сформированы необходимые практические навыки и умения, выполненные учебные задания содержат ошибки и недочеты.

4. Ключ (правильные ответы)

ОК 02: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

1. Ответ: Б
2. Ответ: Б
3. Ответ: А
4. Ответ: БДУ

ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях

5. Ответ: А
6. Ответ: А
7. Ответ: А
8. Ответ: Политика

ОК 04: Эффективно взаимодействовать и работать в коллективе и команде

9. Ответ: А
10. Ответ: А
11. Ответ: Б
12. Ответ: Инструктаж

ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

13. Ответ: А
14. Ответ: А
15. Ответ: А
16. Ответ: Взятка

ОК 07: Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

17. Ответ: А
18. Ответ: А
19. Ответ: А
20. Ответ: Рециклинг

ПК 2.1: Выявлять проблемы, возникающие в процессе эксплуатации баз данных

21. Ответ: А
22. Ответ: А
23. Ответ: А
24. Ответ: Диагностика

ПК 2.2: Осуществлять процедуры администрирования баз данных

25. Ответ: А
26. Ответ: А
27. Ответ: А
28. Ответ: Администратор

ПК 2.3: Проводить аудит систем безопасности баз данных с использованием регламентов по защите информации

29. Ответ: А
30. Ответ: А
31. Ответ: А
32. Ответ: Аудит