АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНСТИТУТ МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СВЯЗЕЙ»
INSTITUTE OF INTERNATIONAL ECONOMIC RELATIONS

Принята на заседании
Учёного совета ИМЭС
(протокол от 26 января 2022 г. № 6)

УТВЕРЖДАЮ
Ректор ИМЭС Ю.И. Богомолова
26 января 2022 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0162B6870090AF03B544352CE01F9DE4C7
Владелец: БОГОМОЛОВА ЮЛИЯ ИГОРЕВНА
Действителен: с 20.01.2023 до 20.04.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ И БАЗ ДАННЫХ

по направлению подготовки
09.03.02 Информационные системы и технологии

Направленность (профиль)
«Информационные системы и сетевые технологии»

Москва – 2022

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Безопасность операционных систем и баз данных» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 926.

Дисциплина «Безопасность операционных систем и баз данных» закрепляет и расширяет знания, умения и практический опыт в области обеспечения безопасного функционирования таких элементов информационной системы как операционные системы и базы данных. Знание и понимание уязвимостей операционных систем, угроз операционным системам, а также защитных механизмов операционных систем позволяет настроить параметры операционной системы таким образом, чтобы обеспечить оптимальный уровень защищенности. Использование встроенных механизмов защиты баз данных, а также программных и аппаратных средств защиты позволяет обеспечить оптимальное соотношение затрат на обеспечение безопасности данных и уровня их защиты.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в учебные планы по программам подготовки бакалавров по направлению подготовки 09.03.02 Информационные системы и технологии и входит в часть, формируемую участниками образовательных отношений, Блока 1.

Дисциплина изучается на 3 курсе в 5 семестре.

Цель и задачи дисциплины

Цель изучения дисциплины - формирование у обучающихся базового опыта по применению методов защиты операционных систем и баз данных, знаний различных аспектов, связанных с обеспечением безопасности операционных систем и баз данных, механизмов и сервисов безопасности компьютерных систем.

Задачи изучения дисциплины:

- сформировать знания основ операционных систем и баз данных, а также процессов создания, сопровождения, организации, управления и их модификации;
- формировать умение осуществлять выбор инструментальных программно-аппаратных средств для защиты операционных систем и баз данных;
- сформировать умение применять современные технологии описания бизнес процессов;
- формирование практического опыта проектирования, отладки, проверки работоспособности, создания (модификации), сопровождения операционных систем и баз данных, а также анализа и управления бизнес-процессами для повышения эффективности деятельности организаций.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	**Код компе-тенции**	**Код и наименование индикатора достижения компетенций**	**Перечень планируемых результатов обучения по дисциплине**			**Формы образовательной деятельности**
			выпускник должен знать	**выпускник должен уметь**	**выпускник должен иметь практический опыт**	
Способность к проектированию, отладке, проверке работоспособности, созданию (модификации) и сопровождению информационных систем (ИС), автоматизирующих задачи организационного управления и бизнес-процессы с целью повышения эффективности деятельности организаций - пользователей ИС	**ПК-2**	**ПК-2.1** Разрабатывает и верифицирует структуру программного кода и баз данных ИС, автоматизирующих задачи организационного управления и бизнес-процессы организаций	основные определения и положения безопасности ОС; основные защитные механизмы клиентских ОС	оценивать угрозы безопасности клиентским ОС; проводить анализ и осуществлять выбор программных и аппаратных средств защиты баз данных	оценки степени защищенности клиентских ОС	Контактная работа: Лекции Лабораторные практикумы Самостоятельная работа
		ПК-2.2. Согласовывает необходимость внесения изменений, обеспечивает и контролирует соответствие разработанного кода и процесса кодирования на языках программирования принятым в организации или проекте стандартам и технологиям	основные угрозы базам данных; программные и аппаратные средства защиты баз данных; основные способы защиты баз данны	устанавливать требования к длине и сложности пароля; устанавливать требования к частоте изменения и блокированию пароля	настройки политики безопасности и учетных записей ОС	
		ПК-2.3. Разрабатывает, верифицирует и модифицирует пользовательские интерфейсы с целью повышения эффективности деятельности организаций - пользователей	особенности обеспечения безопасности клиентских ОС семейств Windows и Linux	устанавливать права доступа дл различных групп пользователей; устанавливать и настраивать систему резервного копирования; проводить анализ и осуществлять выбор программных и аппаратных средств защиты баз данных	формирования, настройки и эксплуатации комплекса программно-аппаратных средств защиты баз данных	

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Безопасность клиентских операционных систем	10					14				25	Отчет по лабораторному практикуму /25
Тема 2. Безопасность серверных операционных систем	8					14				24	Отчет по лабораторному практикуму /25
Тема 3. Аппаратные и программные средства защиты баз данных	8					14				25	Отчет по лабораторному практикуму /25
Тема 4. Встроенные средства защиты баз данных	10					12				25	Отчет по лабораторному практикуму /25
Всего:	**36**					**54**				**99**	**100**
Контроль, час	**27**										**Экзамен**
Объем дисциплины (в академических часах)	**216**										
Объем дисциплины (в зачетных единицах)	**6**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Безопасность клиентских операционных систем.

Современные научно-технические направления в области обеспечения безопасности информационных технологий и систена. Дефекты обеспечения безопасности ОС. Механизмы защиты ОС. Контроль доступа к данным. Особенности обеспечения безопасности ОС Windows 7. Особенности обеспечения безопасности ОС Linux. Особенности обеспечения безопасности ОС для портативных устройств. Особенности обеспечения безопасности ОС macOS.

Тема 2. Безопасность серверных операционных систем

Выполнение требований к защите информации от НСД. Противоречия между принятыми в ОС механизмами защиты и формализованными требованиями к их безопасности. Централизованная и распределенная схемы администрирования. Основные защитные механизмы ОС семейства Unix. Недостатки защитных механизмов ОС семейства Unix. Особенности обеспечения безопасности ОС Windows NT. Сервер аутентификации Kerberos (Цербер). Обзор и статистика методов, лежащих в основе атак на современные ОС.

Тема 3. Аппаратные и программные средства защиты баз данных

Понятие защиты баз данных. Основные типы угроз безопасности баз данных. Аппаратные средства защиты баз данных. Программные средства защиты баз данных. Технологии резервного копирования и восстановления данных. Средства резервного копирования и восстановления данных.

Тема 4. Встроенные средства защиты баз данных

Защита доступа. Средства поддержки целостности данных. Средства защиты СУБД Microsoft Access. Средства защиты СУБД Oracle. Средства защиты СУБД Microsoft SQL Server. Средства защиты СУБД My SQL.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков использования профессиональной лексики, закрепление практических профессиональных компетенций, поощрение интеллектуальных

инициатив.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к экзамену.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции, обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

1. Получение задания и рекомендаций к выполнению практикума.
2. Настройка инструментальных средств, необходимых для выполнения практикума.
3. Выполнение заданий практикума.
4. Подготовка отчета в соответствии с требованиями.
5. Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14,

выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине «Безопасность операционных систем и баз данных» определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Навигация для обучающихся по самостоятельной работе в рамках изучения дисциплины

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Форма текущего контроля
Тема 1. Безопасность клиентских операционных систем.	Особенности обеспечения безопасности ОС для портативных устройств. Особенности обеспечения безопасности ОС macOS.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 2. Безопасность серверных операционных систем	Противоречия между принятыми в ОС механизмами защиты и формализованными требованиями к их безопасности. Централизованная и распределенная схемы администрирования.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 3. Аппаратные и программные средства защиты баз данных	Технологии резервного копирования и восстановления данных. Средства резервного копирования и восстановления данных.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 4. Встроенные средства защиты баз данных	Средства защиты СУБД Microsoft SQL Server. Средства защиты СУБД My SQL.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

2. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. –

Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

Дополнительная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов.
– Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

2. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

3. Смирнов, В.И. Защита информации / В.И. Смирнов ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2017. – 67 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

4. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка
1.	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
3.	Официальный сайт Institute of Electrical and Electronics Engineers (IEEE)	http://www.ieee.org/index.html
4.	Официальный сайт компании Infowatch	http://www.infowatch.ru/
5.	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
6.	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/
7.	Официальный сайт журнала «Информационная безопасность»	http://www.itsec.ru/main.php

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория (Лаборатория информационно-коммуникационных технологий), оборудованная:
комплекты специализированной учебной мебели, мультимедийный проектор, экран, доска классная, принтер, компьютер преподавателя и

компьютеры обучающихся с выходом в сеть «Интернет», доступом в электронную информационно-образовательную среду.

Помещение для самостоятельной работы обучающихся –, оборудованная:
комплекты специализированной учебной мебели, мультимедийный проектор, экран, доска классная, компьютеры с выходом в сеть «Интернет» и доступом в электронную информационно-образовательную среду.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

- Windows (зарубежное, возмездное);
- MS Office (зарубежное, возмездное);
- Adobe Acrobat Reader (зарубежное, свободно распространяемое);
- КонсультантПлюс: «КонсультантПлюс: Студент» (российское, свободно распространяемое);
- 7-zip – архиватор (зарубежное, свободно распространяемое);
- Comodo Internet Security (зарубежное, свободно распространяемое);
- MySQL for Windows – реляционная система управления базами данных (зарубежное, свободно распространяемое);
- Apache NetBeans – свободная интегрированная среда разработки приложений (IDE) на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада и ряда других (зарубежное, свободно распространяемое);
- Android Studio – разработка мобильных приложений (зарубежное, свободно распространяемое)

электронно-библиотечная система:

- Электронная библиотечная система (ЭБС) «Университетская библиотека ONLINE» http://biblioclub.ru/.
- Образовательная платформа «Юрайт». Для вузов и ссузов. Электронная библиотечная система (ЭБС) https://urait.ru/

современные профессиональные баз данных:

- Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.
- Портал Единое окно доступа к образовательным ресурсам http://window.edu.ru/

информационные справочные системы:

- Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
- Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/).

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	25-20 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 19-15 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 14- 6 – работа и отчет выполнены в срок, в основном самостоятельно, использованы соответствующие формулы; определены соответствующие спецификации, имеются ошибки в расчетах; выбраны совместимые комплектующие необходимые, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 5 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

<u>Типовые задания к лабораторным практикумам</u>

Лабораторный практикум № 1. Безопасность клиентских операционных систем.

Задание 1

1. Выбрать клиентские операционные системы, отвечающие интересам компании.
2. Спланировать и описать области проверки безопасности операционных систем, используемых в компании.
3. Провести проверку безопасности операционных систем, используемых в компании.
4. Сформировать отчет по результатам протоколирования и аудита операционных систем.

Задание 2

1. Сформулировать потенциальные угрозы безопасности операционным системам компании.
2. Дать характеристику и оценку следующим технологиям защиты от программ-шпионов и вирусов, предлагаемых компанией Microsoft:

- Защитник Windows (Windows Defender)
- Windows Live Safety Center
- Средство удаления вредоносных программ (Malicious Software Removal Tool)
- Windows Live OneCare
- Microsoft Client Protection

Задание 3

В операционной системе Windows 7 и выше настроить политику паролей и учетных записей.

Лабораторный практикум № 2. Безопасность серверных операционных систем

Задание 1

1. Выбрать серверные операционные системы, отвечающие интересам компании.
2. Спланировать и описать области проверки безопасности операционных систем, используемых в компании.
3. Провести проверку безопасности операционных систем, используемых в компании.
4. Сформировать отчет по результатам протоколирования и аудита операционных систем.

Задание 2

1. Провести анализ имеющихся на рынке услуг программно-

технических средств используемых для протоколирования и аудита информационной безопасности операционных систем.

2. Оценить возможности предлагаемых средств и варианты их использования в компании.

Задание 3

В операционной системе семейства Unix - Debian произвести настройку протокола безопасных соединений – SSH.

Задание 4

В операционной системе семейства Windows NT - Windows Server 2008 R2 и выше настроить аудит доменных служб Active Directory

Лабораторный практикум № 3. Аппаратные и программные средства защиты баз данных

Задание 1

Разработать модель безопасности компании с рассмотрением вопросов стоимости внедряемых средств защиты и соотношения затрат на защиту и получаемого эффекта, на основе современных стандартов в области информационной безопасности, в частности используя критерии оценки безопасности информационных технологий ISO/IEC 15408.

Задание 2

1. Провести анализ имеющихся на рынке услуг программно-технических средств используемых для протоколирования и аудита информационной безопасности операционных систем.

2. Оценить возможности предлагаемых средств и варианты их использования в компании.

3. Провести анализ предлагаемых средств на предмет устойчивости системы аудита к несанкционированному изменению параметров системы и собственно данных аудита, а также избирательности средств аудита.

Задание 3

1. Выбрать СУБД нескольких производителей (не менее 2-х).

2. Используя модель потенциальных угроз оценить степень безопасности каждой из выбранных СУБД и провести сравнительный анализ.

Задание 4

Провести настройку RAID массива с целью повышения безопасности данных посредством одновременной записи на два разных диска.

Лабораторный практикум № 4. Встроенные средства защиты баз данных

Задание 1

1. Выбрать СУБД, отвечающие интересам компании.

2. Спланировать и описать области проверки безопасности СУБД, используемых в компании.

3. Провести проверку безопасности СУБД, используемых в компании.

4. Сформировать отчет по результатам протоколирования и аудита СУБД.

Задание 2

1. Выбрать СУБД, отвечающие интересам компании.

2. Выявить и проанализировать встроенные механизмы защиты, обеспечивающие:

- *конфиденциальность:* обеспечение пользователям доступа только к тем данным, для которых пользователь имеет явное или неявное разрешение на доступ;
- *целостность:* обеспечение защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки;
- *доступность:* обеспечение возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией.

3. Оценить эффективность встроенных средств защиты с точки зрения противодействия потенциальным угрозам.

Задание 3

Разработайте таблицы определения идентификаторов 3-4 пользователей с заданными вариантами прав. Для практической реализации можно использовать СУБД Access, My SQL или SQL Server.

Задание 4

Для созданного или готового набора таблиц БД (не менее 3-х) Сформулируйте и разработайте не менее 3-х запросов, содержащих выборку из всех таблиц и отражающих только информацию, необходимую пользователю в соответствии с его правами. Для практической реализации можно использовать СУБД Access, My SQL или SQL Server.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Процедура оценивания	Шкала и критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета, включающего в себя: Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающимся	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые формулы, использована профессиональная

Процедура оценивания	Шкала и критерии оценки, балл
принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними; Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности; Задание №3 – задание на проверку умений и навыков, полученных в результате освоения дисциплины	лексика. Задача решена правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо)–** ответ в целом правильный, логически выстроен, приведены необходимые формулы, использована профессиональная лексика. Ход решения задачи правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно)–** ответ в основном правильный, логически выстроен, приведены не все необходимые формулы, использована профессиональная лексика. Задача решена частично. **-Менее 50 (неудовлетворительно)**– ответы на теоретическую часть неправильные или неполные. Задача не решена

Типовые задания для проведения промежуточной аттестации обучающихся

Задания на знания

1. Перечень и содержание типовых функциональных дефектов обеспечения безопасности ОС.
2. Встроенные средства защиты ОС и порядок их функционирования. Способы реализации средств защиты ОС. Средства мониторинга. Средства профилактического контроля.
3. Организация процесса и средства обеспечения контроля доступа к данным.
4. Встроенные средства обеспечения безопасности клиентской части ОС Windows 7 и выше.
5. Назначение, возможности и практическое применение технологии шифрования диска BitLocker.
6. Встроенные средства обеспечения безопасности клиентской части ОС Linux (на примере Ubuntu 14 и выше, Debian 8.0 и выше или другой ОС семейства Linux).
7. Формальные требования и практическая реализация механизмов защиты ОС.
8. Встроенные средства обеспечения безопасности серверной части ОС семейства Unix (на примере Solaris 5.11 и выше, AIX 6 и выше, FreeBSD 10 и выше или другой ОС семейства Unix).
9. Недостатки реализации системы защиты ОС семейства Unix (на примере Solaris 5.11 и выше, AIX 6 и выше, FreeBSD 10 и выше или другой ОС семейства Unix).
10. Встроенные средства обеспечения безопасности серверной части ОС семейства Windows NT (на примере Windows Server 2012 и

выше).

11. Назначение, возможности и практическое использование сервера аутентификации Kerberos (Цербер). Протокол аутентификации Kerberos (назначение, функции, интеграция с системой безопасности). Поддержка Kerberos открытых ключей.

12. Перечень, частота использования и способы реализации атак на современные ОС.

13. Назначение, функции, интеграция с системой безопасности протокола безопасных соединений SSH.

14. Определение, основные направления и области применения (оборудование, программное обеспечение, персонал и так далее) защиты баз данных.

15. Перечень, основные источники и способы реализации угроз безопасности базам данных.

16. Перечень, назначение, возможности и порядок функционирования аппаратных средства защиты баз данных.

17. Перечень, назначение, возможности и порядок функционирования программных средств защиты баз данных.

18. Реализация трехуровневой архитектуры защиты баз данных в Web (передача, хранение, доступ). Задачи и способы реализации защиты на каждом из уровней.

19. Назначение, возможности, характеристики и способы реализации прокси-сервера как средства защиты баз данных.

20. Назначение, возможности, характеристики и способы реализации брандмауэра как средства защиты баз данных.

21. Назначение, возможности, характеристики и способы реализации цифрового сертификата как средства защиты баз данных.

22. Обеспечение защиты доступа к базам данных (организационные, административные, аппаратные и программные аспекты).

23. Назначение, возможности, характеристики и способы реализации средств поддержки целостности данных.

24. Встроенные средства защиты СУБД Microsoft Access 2010 и выше (перечень, назначение, возможности, практика применения).

25. Встроенные средства защиты СУБД Oracle 10g и выше (перечень, назначение, возможности, практика применения).

Задания на умения

1. Какие существуют основные типы угроз безопасности ОС? Обоснуйте ответ.

2. В чем заключается разница между необратимыми и обратимыми технологиями шифрования? Обоснуйте ответ.

3. Что общего и в чем разница механизмов защиты СУБД Microsoft Access 2010 и выше и Oracle 10g и выше? Обоснуйте ответ.

4. В чем заключается разница защитных механизмов клиентских

ОС семейства Windows 7 и выше и Linux (на примере Ubuntu 14 и выше, Debian 8.0 и выше или другой ОС семейства Linux)? Обоснуйте ответ.

5. В чем заключается разница защитных механизмов серверных ОС семейства Windows Server 2012 и выше и Unix (на примере Solaris 5.11 и выше, AIX 6 и выше, FreeBSD 10 и выше или другой ОС семейства Unix)? Обоснуйте ответ.

6. Для чего необходимы и как применяются средства профилактического контроля безопасности операционные системы? Обоснуйте ответ.

7. В чем заключается разница между матрицей и списками доступа? Обоснуйте ответ.

8. Какие требования предъявляются к параметрам пароля для ОС семейства Linux (на примере Ubuntu 14 и выше, Debian 8.0 и выше или другой ОС семейства Linux) и Windows 7 и выше? Обоснуйте ответ.

9. Какие существуют технологии и средства аутентификации на основе ключей? Приведите 2-3 примера практического применения средств аутентификации на основе ключей. Обоснуйте ответ.

10. В чем состоят противоречия между реализованными в ОС механизмами защиты и принятыми формализованными требованиями? Обоснуйте ответ.

11. В чем, с точки зрения обеспечения информационной безопасности, состоит отличие между централизованной и распределенной схемой администрирования? Обоснуйте ответ.

12. Для чего предназначена служба Active Directory и какие она предоставляет возможности администрирования? Обоснуйте ответ.

13. Каким образом система Kerberos реализует попарную проверку подлинности субъектов? Обоснуйте ответ.

14. Какие выделяют группы методов, позволяющие несанкционированно вмешаться в работу системы? Обоснуйте ответ.

15. Какие основные недостатки механизма защиты ОС используют средства несанкционированного доступа? Обоснуйте ответ.

16. В чем заключается разница структур прав доступа серверных ОС семейства Windows Server 2012 и выше и Unix (на примере Solaris 5.11 и выше, AIX 6 и выше, FreeBSD 10 и выше или другой ОС семейства Unix)? Обоснуйте ответ.

17. Чем отличаются преднамеренные и не преднамеренные угрозы базе данных? Обоснуйте ответ.

18. В чем заключается применение технологии RAID массивов? Какие существуют уровни RAID массивов? Обоснуйте ответ.

19. Какие существуют технологии и средства резервного копирования? Приведите 2-3 примера практического применения резервного копирования для обеспечения безопасности базы данных.

20. Какие компоненты должны использовать системы шифрования для организации защищенной передачи данных по незащищенным сетям? Обоснуйте ответ.

21. Какие основные механизмы защиты доступа к данным реализованы в СУБД? Обоснуйте ответ.

22. Какие выделяют категории целостности данных? Обоснуйте ответ.

23. Какие компоненты СУБД Access 2010 и выше могут быть небезопасны? Обоснуйте ответ.

24. Какие основные средства и инструменты, необходимы для построения защищенных систем СУБД Oracle 10g и выше? Обоснуйте ответ.

25. Какие категории привилегий предусмотрены в СУБД Oracle 10g и выше? Обоснуйте ответ.

Задания на навыки

Задание № 1.

По представленному описанию компании определить угрозы безопасности клиентским ОС, выбрать клиентские ОС, отвечающие интересам компании и описать процесс организации их защиты.

Задание № 2.

По представленному описанию компании определить угрозы безопасности серверным ОС, выбрать серверные ОС, отвечающие интересам компании и описать процесс организации их защиты.

Задание № 3.

По представленному описанию компании определить угрозы безопасности базам данных, выбрать СУБД, отвечающую интересам компании и описать процесс организации защиты баз данных.

Задание № 4.

В операционной системе Windows 7 и выше настроить политику паролей и учетных записей.

Задание № 5.

В операционной системе семейства Unix - Debian произвести настройку протокола безопасных соединений – SSH.

Задание № 6.

В операционной системе семейства Windows NT - Windows Server 2012 R2 и выше настроить аудит доменных служб Active Directory.

Задание № 7.

К предложенным таблицам разработать три SQL запроса на выборку данных в соответствии с заданными критериями.