МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему«Разработка модели безопасности базы данных»

Исполнитель Опря Кристина Сергеевна
(фамилия,имя,отчество)

Руководитель Бурлов Вячеслав Георгиевич
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой Лепешкин Олег Михайлович
(подпись) (фамилия,имя,отчество)

«___» _____ 2026г

Санкт–Петербург
2026

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ Лепешкин О. М

(подпись) (фамилия, имя,отчество)

« _ »_____2026 года

Задание
на выпускную квалификационную работу

студенту Опря Кристине Сергеевне

(фамилия, имя, отчество)

1. Тема Разработка модели безопасности базы данных

закреплена приказом ректора Университета от «___» _____ 2026 года, № ___

2. Срок сдачи законченной работы «___» _____ 2026 года

3. Исходные данные к выпускной квалификационной работе:

Система управления базами данных, анализ угроз и уязвимостей, проектирование и реализация системы управления безопасностью, модели и методы обеспечения безопасности, проектирование и реализация системы управления безопасностью, оценка эффективности управленческих решений

4. Перечень вопросов, подлежащих разработке (краткое содержание работы:

Введение. Актуальность темы, цели и задачи выпускной квалификационной работы.

Глава 1. Научно-технические основы построения модели обеспечения безопасности базы данных.

(наименование главы)

Глава 2.Разработка аналитической, математической модели управления безопасностью.

(наименование главы)

Глава 3. Разработка алгоритмического аппарата модели управления безопасностью базы данных.

(наименование главы)

Глава 4 Разработка предложений по совершенствованию системы обеспечения безопасности баз данных.

(наименование главы)

Заключение. Выводы по работе. Оценка степени решения поставленных задач.

(наименование главы)

5. Перечень материалов, представляемых к защите:

– Пояснительная записка;
– Листинга модулей

6. Консультанты по работы

6.1. Бурлов Вячеслав Георгиевич

7. Дата выдачи задания:«_____»_____2025 года

Руководитель выпускной квалификационной работы

профессор, д.т.н. Бурлов Вячеслав Георгиевич _____

(должность, ученая степень, ученое звание, фамилия,имя,отчество) (подпись)

Задание принял к исполнению «_____»_____2025 года

Студент Опря Кристина Сергеевна _____

(фамилия, имя, отчество, учебная группа) (подпись)

РЕФЕРАТ

Дипломная работа: ____с., __16__рис., ___16__табл., _2___ приложения, ___16__ источников литературы.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАЗ ДАННЫХ, МОДЕЛИРОВАНИЕ ПРОЦЕССОВ БЕЗОПАСНОСТИ, СЕТЕВЫЕ МОДЕЛИ,УПРАВЛЕНЧЕСКИЕ РЕШЕНИЯ, ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ

Объект исследования: база данных как компонент информационной системы, функционирующий в условиях многопользовательского и сетевого доступа и подверженный внутренним и внешним деструктивным воздействиям.

Предмет исследования: процессы обеспечения информационной безопасности базы данных, включая процессы образования угроз, их идентификации, нейтрализации и управления защитными мероприятиями.

Цель работы: разработка аналитической модели и алгоритмического аппарата управления безопасностью базы данных на основе системной интеграции целевого процесса функционирования и процессов обеспечения информационной безопасности, обеспечивающих достижение заданного уровня защищенности.

В дипломной работе проводится анализ архитектуры систем управления базами данных, актуальных угроз и уязвимостей информационной безопасности, а также современных методологий и моделей обеспечения безопасности. Обоснована необходимость применения формализованного подхода, ориентированного на решение обратной задачи проектирования системы безопасности.

Разработана аналитическая модель управления безопасностью базы данных на основе непрерывной марковской цепи, формализованной уравнениями Колмогорова–Чепмена. Для учета временных характеристик процессов идентификации и нейтрализации угроз применены сетевые модели, позволившие определить их интенсивности и критические пути. Оценен показатель эффективности реализации управленческих решений и показана возможность управления его значением путем оптимизации временных параметров процессов безопасности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 6
ГЛАВА 1. НАУЧНО-ТЕХНИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗЫ ДАННЫХ 9
1.1. Анализ угроз и уязвимостей безопасности базы данных 13
1.2. Анализ современных подходов и моделей обеспечения безопасности данных..... 20
1.3. Обоснование выбора методологии построения модели обеспечения безопасности базы данных..... 28
Выводы по первой главе 29
ГЛАВА 2. РАЗРАБОТКА АНАЛИТИЧЕСКОЙ, МАТЕМАТИЧЕСКОЙ МОДЕЛИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ. 31
2.1. Общий подход к разработке модели обеспечения безопасности систем. 31
2.3. Оценивание показателя эффективности реализации управленческих решений. 58
Выводы по второй главе: 65
ГЛАВА 3. РАЗРАБОТКА АЛГОРИТМИЧЕСКОГО АППАРАТА МОДЕЛИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ БАЗЫ ДАННЫХ..... 68
3.1. Архитектура программного комплекса управления безопасностью базы данных. . 68
3.2. Проектирование и реализация функциональных модулей 70
3.3. Реализация нейтрализации угроз и работа системы..... 76
Выводы по третьей главе: 80
ГЛАВА 4. РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ..... 82
ЗАКЛЮЧЕНИЕ 85
Приложение 1 - Исходный код сканера 90
Приложение 2 - Исходный код планировщика 95

ВВЕДЕНИЕ

Стремительное развитие вычислительной техники и информационных технологий создало уникальные возможности для широкого внедрения автоматизированных информационных систем, обеспечивающих эффективное управление, хранение и обработку больших объёмов данных. В этих условиях технологии баз данных становятся ключевым инструментом современных информационных систем, выступая основой для функционирования критически важных бизнес-процессов, корпоративных сервисов и государственных информационных ресурсов. Однако широкое и интенсивное использование баз данных сопровождается значительным ростом угроз их безопасности. Современные базы данных подвергаются множеству рисков: несанкционированному доступу, изменению или удалению данных, утечкам конфиденциальной информации, а также воздействию внутренних и внешних деструктивных факторов.

Усложнение архитектуры информационных систем и распространение многопользовательского сетевого доступа повышают вероятность деструктивных воздействий на базы данных. Реализация угроз может проявляться в форме несанкционированного доступа, утечки конфиденциальной информации, модификации или уничтожения данных, а также нарушения доступности сервисов.

В этих условиях обеспечение безопасности базы данных должно рассматриваться как управляемый процесс, включающий взаимосвязанные этапы: образование угроз, их идентификацию, принятие управленческих решений и нейтрализацию, а также оценку результата по заданному показателю защищенности. Требуется такой подход, который позволяет согласованно описывать перечисленные процессы и определять условия достижения требуемого уровня безопасности в условиях деструктивного воздействия.

Данная совокупность факторов определяет актуальность настоящей выпускной квалификационной работы, целью которой является выбор, обоснование и реализация условий обеспечения безопасности базы данных в условиях деструктивного воздействия на основе системной интеграции процессов обеспечения безопасности.

Дано:

- База данных как компонент информационной системы, функционирующий в условиях многопользовательского и сетевого доступа;
- наличие внутренних и внешних деструктивных факторов, воздействующих на процессы хранения и обработки данных;

Требуется:

Разработать модель и алгоритмический аппарат обеспечения информационной безопасности функционирования базы данных, основанные на системной интеграции целевого информационного процесса и процессов образования угроз, их идентификации и нейтрализации, обеспечивающие достижение заданного уровня защищенности.

Возникшие трудности:

- сложность формализованного описания взаимосвязей между процессами возникновения угроз и действиями механизмов защиты;
- необходимость перехода от качественного описания защищенности к количественной оценке эффективности управленческих решений.

Трудности преодолены:

- использованием системного подхода и декомпозиции задачи на подзадачи;

- применением аналитического моделирования для формализации процессов идентификации и нейтрализации угроз и введением показателя информационной безопасности.

Решение поставленной задачи требует ее декомпозиции на следующие подзадачи:

1. Проанализировать известные угрозы, уязвимости, методы и принципы обеспечения безопасности базы данных в условиях деструктивного воздействия.
2. Разработать модель системной интеграции процессов обеспечения безопасности базы данных.
3. Разработать алгоритмический аппарат управления процессами обеспечения информационной безопасности базы данных на основе выбранной модели.
4. Разработать предложения по совершенствованию системы обеспечения безопасности базы данных с учетом результатов моделирования и требований к защищенности.

Объект исследования — база данных корпоративного уровня как компонент информационной системы, подвержены деструктивному воздействию в условиях многопользовательского и сетевого доступа.

Предмет исследования — процессы обеспечения информационной безопасности базы данных и методы их формализованного описания при системной интеграции процессов образования, идентификации и нейтрализации угроз.

ГЛАВА 1. НАУЧНО-ТЕХНИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗЫ ДАННЫХ

В современных организациях обрабатываются большие массивы информации, представленной в различных формах и поступающей из множества источников. Управление такими потоками данных требует их структурирования, анализа и надежной защиты, а также обеспечения актуальности, доступности и согласованности информации.

Постепенное усложнение информационных процессов и рост требований к скорости обработки данных привели к необходимости использования специализированных инструментов для их систематизации. Файловые системы при работе с большими объемами информации оказались недостаточно эффективными в условиях, требующих упорядоченного хранения, быстрого поиска, поддержки многопользовательского доступа и обеспечения целостности данных. Указанные ограничения обусловили появление и активное развитие технологий баз данных как более структурированного способа организации информации.

В рамках технологий баз данных информация рассматривается как единое логическое хранилище, в котором данные могут быть распределены по различным носителям и вычислительным узлам, оставаясь при этом согласованными и структурированными. Такое представление информации создает предпосылки для повышения устойчивости функционирования информационных систем и формирования требований к обеспечению их безопасности.

Функционирование базы данных обеспечивается совокупностью хранимых данных и метаданных, описывающих структуру информации, ее свойства и взаимосвязи. Метаданные играют ключевую роль при реализации механизмов управления доступом, контроля целостности и

обеспечения согласованности данных, что непосредственно связано с задачами информационной безопасности.

В зависимости от модели данных, архитектуры хранения и среды функционирования базы данных классифицируются по ряду признаков. Такая классификация позволяет учитывать особенности эксплуатации различных типов баз данных и служит основой для выбора архитектурных и защитных решений, ориентированных на конкретные условия функционирования системы.

В таблице 1 представлена обобщенная структура наиболее распространенных видов баз данных:

Таблица 1 - Классификация баз данных

Признак классификации	**Вид базы данных**	**Краткая характеристика**
По модели данных	Иерархические	Древовидная структура, строгие связи «родитель–потомок»
	Сетевые	Поддержка множественных связей между элементами данных
	Реляционные	Представление данных в виде таблиц, связанных ключевыми атрибутами
	Объектно-ориентированные	Хранение данных в виде объектов с атрибутами и методами
	Гибридные (объектно-реляционные)	Совмещение реляционных таблиц и объектных структур
	NoSQL	Нереляционные модели хранения (документные, графовые, ключ–значение)
По архитектуре и среде хранения	Централизованные	Размещение базы данных на одном вычислительном узле
	Распределённые	Хранение данных на нескольких узлах вычислительной сети
	In-memory	Размещение данных в оперативной памяти
	Дисковые	Хранение на жестких дисках

Среда функционирования	Локальные	Эксплуатация в пределах одной вычислительной системы
	Клиент–серверные	Обработка данных на сервере с сетевым доступом
	Облачные	Размещение базы данных в облачной инфраструктуре

Выбор архитектуры и модели данных оказывает существенное влияние на профиль угроз информационной безопасности. Так, распределенные и облачные базы данных в большей степени подвержены рискам несанкционированного доступа и сетевых атак, тогда как для централизованных систем более характерны угрозы, связанные с внутренними нарушениями и отказами оборудования. Указанные особенности необходимо учитывать при анализе угроз и построении моделей безопасности.

Разнообразие типов баз данных формирует дополнительные требования к инструментам управления. Необходимо обеспечить единый, безопасный и согласованный доступ к информации независимо от ее физического расположения и внутренней модели. Для этих целей применяются системы управления базами данных (СУБД) - программные комплексы, обеспечивающие организацию, хранение и управление данными. СУБД предоставляет пользователю или приложению интегрированное представление информации, обрабатывает поступающие запросы, обращается к хранящимся данным и возвращает результат. При этом СУБД скрывает внутренние детали хранения и обработки данных, облегчая работу программ и пользователей. Приложения могут взаимодействовать с СУБД как через встроенные языки запросов (например, SQL), так и с помощью языков программирования высокого

уровня, таких как Python, Java или C#.

К основным функциям СУБД относятся: управление данными во внешней памяти, управление данными в оперативной памяти с использованием дискового кэша, журнализация изменений и обеспечение восстановления данных, поддержка языков определения и манипулирования данными, обеспечение безопасности и целостности данных. СУБД позволяют эффективно использовать различные виды баз данных и являются основой для построения системных моделей хранения и защиты информации [1].

Система базы данных определяет и регулирует сбор, хранение, управление и использование данных в среде баз данных. Система управления базами данных в общем виде включает пять ключевых компонентов: аппаратное обеспечение, программное обеспечение, люди, процедуры и данные.

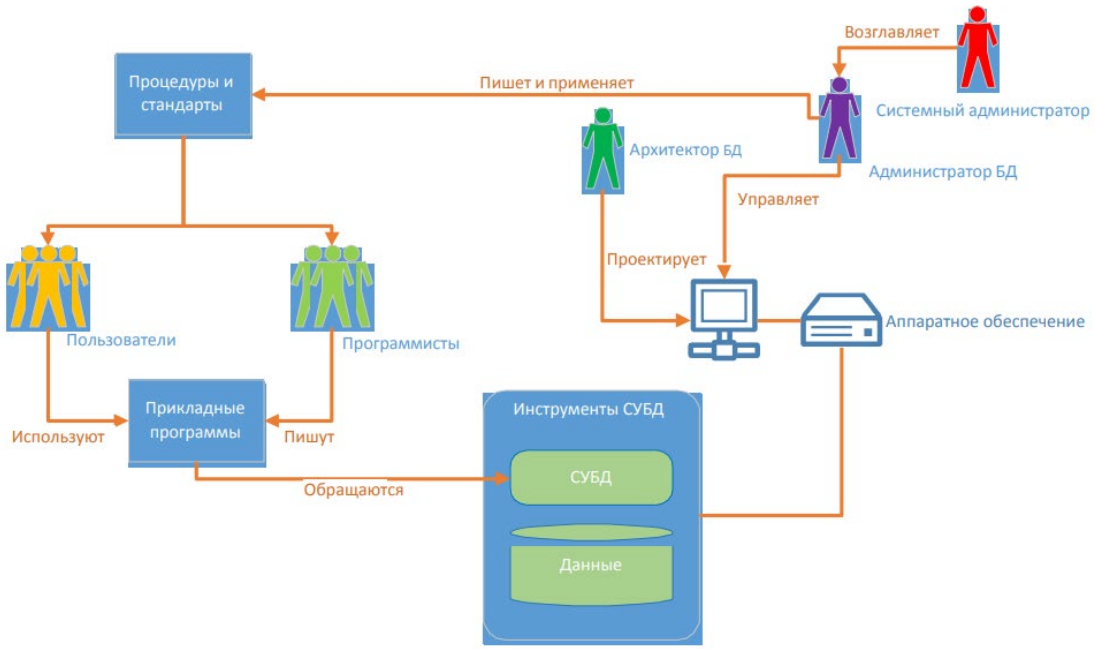

Рисунок 1 - Окружение системы базы данных

Ключевыми элементами системы баз данных являются технические средства, программное обеспечение, пользователи, регламентирующие процедуры и данные. Аппаратная и программная составляющие определяют производительность и устойчивость функционирования

системы, тогда как пользователи и процедуры формируют организационный контур её эксплуатации и безопасности. Данные выступают центральным объектом системы, вокруг которого формируется архитектура базы данных и механизмы управления доступом. Взаимосвязь указанных компонентов определяет уровень защищённости базы данных и служит основой для анализа угроз и выбора методов их нейтрализации.

1.1. Анализ угроз и уязвимостей безопасности базы данных

Под угрозой безопасности информации будем понимать действие или событие, которое может привести к нарушению достоверности, целостности или конфиденциальности хранящейся, передаваемой или обрабатываемой информации.

Дадим определение некоторым понятиям, которые часто используются, при анализе безопасности информационных систем:

Атака - попытка злоумышленником реализовать угрозу.

Злоумышленник - лицо, планирующее и осуществляющее атаку.

Источник угрозы - это потенциальный злоумышленник.

Угроза - потенциальное событие, реализация которого может привести к нарушению свойств защищаемой информации вследствие наличия уязвимостей информационной системы.

Вторжение - это злонамеренная ошибка внутреннего, но также внешнего происхождения, возникающая в результате атаки.

Процесс идентификации угроз является одним из ключевых этапов обеспечения безопасности систем баз данных. Он направлен на выявление всех потенциальных и актуальных рисков, которые могут возникнуть в пределах каждого компонента информационной системы. Каждый из представленных компонентов может стать источником уязвимостей или каналом реализации угроз.

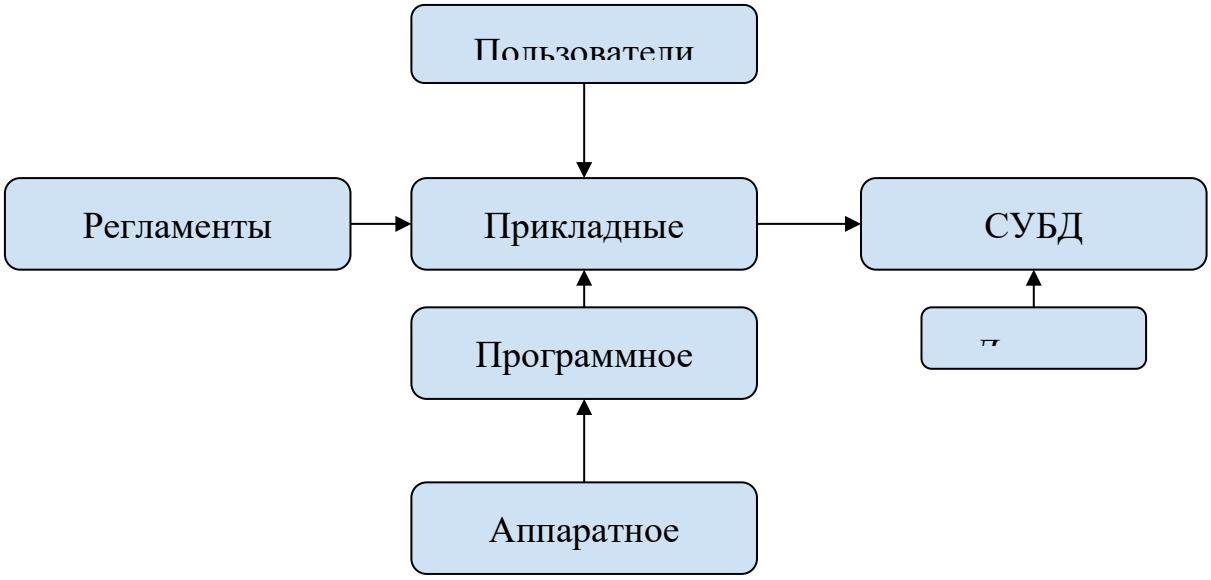

Рисунок 2 - Основные элементы функционирования систем баз данных

Систематизация угроз информационной безопасности позволяет оценить характер возможного воздействия и определить наиболее уязвимые элементы инфраструктуры системы баз данных. В процессе функционирования систем баз данных угрозы информационной безопасности могут затрагивать различные свойства информации и проявляться в виде нарушения доступности, целостности и конфиденциальности данных. Нарушения доступности приводят к ограничению или потере возможности использования базы данных вследствие отказов программных или аппаратных компонентов, ошибок конфигурирования, а также воздействия внешних деструктивных факторов.

Нарушение целостности данных выражается в их искажении, утрате или возникновении логических несоответствий, что отрицательно сказывается на достоверности информации и корректности работы прикладных процессов. Угрозы конфиденциальности связаны с несанкционированным получением доступа к данным, включая как служебные параметры безопасности и учетные данные, так и информацию, представляющую ценность для функционирования организации.

Несмотря на значительное разнообразие потенциальных уязвимостей, на практике наибольший ущерб системе наносят ограниченное число типовых угроз, реализация которых определяется особенностями архитектуры и режима эксплуатации базы данных.

В данной выпускной квалификационной работе рассматриваются наиболее распространённые на текущий момент времени угрозы безопасности, воздействующие на системы баз данных. Анализ современных инцидентов информационной безопасности и отчетов профильных организаций показывает, что указанные угрозы характеризуются различной природой возникновения, а также отличающимися временными и вероятностными параметрами их реализации. Данное обстоятельство создает предпосылки для формализации процессов обнаружения, идентификации и нейтрализации угроз, что является необходимым этапом при построении аналитической модели управления безопасностью базы данных.

В рамках работы выделены следующие ключевые уязвимости систем баз данных:

– SQL-инъекции;
– несанкционированный доступ;
– утечка данных;
– отказ в обслуживании;
– внутренние угрозы;
– уязвимости управления правами и привилегиями пользователей;
– уязвимости программного обеспечения СУБД.

1.1.1. SQL инъекции.

SQL-инъекции возникают в ситуациях, когда пользовательский ввод в SQL-запросах не проверяется и не фильтруется должным образом.

Злоумышленник может внедрять собственные SQL-конструкции, изменяя логику выполнения запросов. Вследствие этого возможно получение несанкционированного доступа к информации, ее модификация или удаление, а иногда и полный сбой работы базы данных.

Листинг 1.1 — Пример уязвимого SQL-запроса

```
$username = $_GET['username'];
$query = "SELECT * FROM users WHERE username = '$username'";
```

В данном примере пользовательский ввод напрямую вставляется в SQL-запрос без проверки. Это создает критическую уязвимость, позволяющую злоумышленнику выполнить произвольную SQL-инъекцию.

Листинг 1.2 — безопасный вариант с использованием prepared statements

```
$stmt = $pdo->prepare('SELECT * FROM users WHERE username = :username');
$stmt->execute(['username' => $username]);
```

Приведённые фрагменты кода носят иллюстративный характер и используются для демонстрации принципов возникновения и предотвращения SQL-инъекций.

Согласно аналитическому отчету компании Positive Technologies [2], в IV квартале 2024 года SQL-инъекции остаются одним из наиболее распространенных векторов атак на веб-приложения. Данные уязвимости продолжают активно эксплуатироваться злоумышленниками в рамках различных кибератак.

1.1.2. Несанкционированный доступ.

Нарушение регламентированного доступа к информационным ресурсам базы данных может происходить из-за недостаточно надежной проверки легитимности пользователей и контроля их прав. К распространенным причинам относятся использование слабых или скомпрометированных паролей, отсутствие многофакторной

аутентификации, чрезмерные привилегии и ошибки в администрировании. Реализация несанкционированного доступа приводит к утечке конфиденциальной информации, нарушению целостности данных и возможности дальнейшего развития атаки.

В соответствии с аналитическим отчетом Kaspersky Managed Detection and Response за 2024 год, целенаправленные атаки с участием человека (human-driven attacks) составляли примерно 43 % от всех инцидентов высокой критичности, что указывает на активное использование методов обхода автоматических механизмов защиты и значительный вклад действий злоумышленников в общий объем серьезных инцидентов информационной безопасности. [3]

1.1.3. Утечка данных.

Процесс утечки информации характеризуется многоаспектным воздействием на информационную безопасность организации. В зону риска попадают различные категории данных, включая персональные сведения субъектов, коммерческую тайну предприятия и служебную информацию ограниченного доступа. Последствия подобных инцидентов носят комплексный характер и проявляются в виде существенных финансовых потерь, связанных с необходимостью реагирования на инцидент, восстановления утраченных данных и компенсации ущерба пострадавшим сторонам. Согласно ежегодному отчёту IBM Security Cost of a Data Breach Report 2024, средняя стоимость утечки данных в мире составила примерно 4.88 млн долларов США — это максимальный показатель за всю историю отчетов с учетом роста затрат на восстановление после инцидентов. В исследовании также отмечается, что 42% нарушений были выявлены собственными средствами безопасности организаций, что свидетельствует о влиянии организационных и процессных факторов на управление инцидентами. [4]

1.1.4. Отказ в обслуживании.

Отказ в обслуживании (DoS/DDoS) представляет собой класс атак, направленных на нарушение доступности информационной системы за счет искусственного создания чрезмерной нагрузки на вычислительные и сетевые ресурсы, что препятствует нормальной работе сервисов и обработке запросов. В 2024 году наблюдалось значительное увеличение активности DDoS-атак: согласно отчету Cloudflare, глобальные системы защиты блокировали около 21,3 млн DDoS-атак, что на 53 % больше, чем в предыдущем году. Атаки различной интенсивности остаются одной из главных угроз доступности сервиса, при этом существенная доля таких атак значительно влияет на работу интернет-структур. [5]

1.1.5. Внутренние угрозы системы.

Внутренние угрозы связаны с действиями пользователей, обладающих легитимным доступом к системе баз данных. К данной категории относятся как преднамеренные действия инсайдеров, так и непреднамеренные ошибки персонала, возникающие вследствие недостаточной квалификации или нарушения регламентов эксплуатации.

Опасность внутренних угроз заключается в том, что такие пользователи уже обладают определенным уровнем доверия и прав доступа, что существенно упрощает реализацию деструктивных действий и затрудняет их своевременное обнаружение. Внутренние угрозы могут приводить к утечке информации, искажению данных и нарушению устойчивости функционирования системы.

1.1.6. Неправильное управление правами и привилегиями пользователей.

Уязвимости, связанные с управлением правами и привилегиями пользователей, возникают в случае, если нарушается принцип наименьших привилегий, а назначенные роли и уровни доступа не проходят регулярной актуализации и контроля. Избыточные права доступа, непоследовательное распределение ролей и отсутствие процедур по периодической ревизии

полномочий создают благоприятные условия для злоупотребления доступом, что может привести к несанкционированному использованию ресурсов базы данных и компрометации конфиденциальной информации. При реализации моделей контроля доступа важно предусмотреть механизм регулярного аудита привилегий и ограничивать права пользователей только теми операциями, которые необходимы для выполнения их служебных функций.

1.1.7. Уязвимости программного обеспечения СУБД.

Программные уязвимости в системах управления базами данных возникают вследствие ошибок реализации компонентов, эксплуатации устаревших версий программных модулей, а также некорректной настройки служб и параметров безопасности. Эксплуатация таких уязвимостей позволяет злоумышленникам обходить встроенные механизмы защиты, выполнять произвольный код с повышенными привилегиями или получать доступ к ресурсам, защищенным системой.

Особую опасность представляет отсутствие своевременного обновления СУБД и неприменение актуальных патчей, а также отсутствие мониторинга и контроля параметров безопасности. Эти факторы значительно повышают вероятность успешной атаки, поскольку затрагивают базовые механизмы функционирования системы и могут привести к комплексным нарушениям конфиденциальности, целостности и доступности данных.

Эти примеры показывают, что защита информации в современных информационных системах требует комплексного подхода, включающего как технические меры, так и организационно-методические решения.

Тем самым формирование системы защиты баз данных целесообразно рассматривать как управляемый процесс, основанный на использовании методологических подходов и моделей безопасности,

позволяющих формализовать управление рисками и оценивать уровень защищённости информационных ресурсов.

1.2. Анализ современных подходов и моделей обеспечения безопасности данных.

Современные подходы к обеспечению безопасности баз данных формировались в условиях усложнения информационных систем, роста объемов обрабатываемых данных и увеличения числа угроз, оказывающих деструктивное воздействие на работу информационных систем. В практической деятельности организации применяются как методологические подходы, так и модели безопасности, которые позволяют описывать, оценивать и контролировать уровень защищенности баз данных. Методологическая база в сфере информационной безопасности преимущественно фокусируется на регламентации организационных процессов и формировании нормативной документации.

Данные подходы устанавливают основополагающие принципы внедрения защитных механизмов, регламентируют распределение функциональных обязанностей между участниками процесса обеспечения безопасности, а также определяют механизмы контроля за исполнением установленных процедур. Для анализа применяемых в настоящее время подходов и методологий обеспечения информационной безопасности выполнено их обобщённое сравнение с точки зрения применимости к задачам защиты систем управления базами данных. Результаты сравнительного анализа представлены в таблице 2.

Таблица 2 - Сравнительный анализ существующих подходов

Методология / подход	**Основная направленность**	**Преимущества**	**Ограничения**
COBIT	Управление и контроль ИТ-	Единая терминология,	Не ориентирован непосредственно

	процессов, аудит и оценка зрелости.	формализованные метрики, поддержка управленческих решений	на данные и базы данных, требует адаптации под задачи защиты БД
ITIL	Управление ИТ-услугами	Структурированн ое управление эксплуатацией	Фокус на услугах, а не на защите данных
ISO/IEC 27000	Управление информационной безопасностью	Комплексный охват мер ИБ	Описательный характер, отсутствие количественных критериев
NIST Cybersecurity Framework (CSF)	Управление рисками ИБ	Гибкость и адаптируемость	Ограниченная применимость в рамках требований РФ
Методические документы ФСТЭК России	Соответствие национальным требованиям ИБ	Учет требований КИИ, высокий уровень формальной защищенности *КИИ - критическая информационная инфраструктура	Жесткая регламентация, низкая гибкость
Риск-ориентированные подходы	Идентификация угроз и оценка рисков	Обоснование защитных мер	Экспертный и качественный характер оценки
Формальные и математические модели			

Проведённый анализ существующих методологий и подходов обеспечения информационной безопасности показывает, что применяемые

решения ориентированы преимущественно на защиту информационных систем в целом и не в полной мере учитывают специфику систем управления базами данных [6]. Каждая из рассмотренных методологий решает определенный класс задач и обладает как преимуществами, так и ограничениями.

Методология COBIT ориентирована преимущественно на управление и контроль ИТ-процессов, а также на оценку зрелости и эффективности управления [7]. Несмотря на наличие формализованных метрик и единой терминологии, данный подход не учитывает специфику защиты данных и требует дополнительной адаптации при применении к задачам обеспечения безопасности баз данных.

Подход ITIL направлен на управление ИТ-услугами и эксплуатационными процессами, что делает его полезным в контексте организации поддержки и сопровождения информационных систем [8]. Однако основной акцент ITIL делается на качестве предоставляемых услуг, а не на защите информации и данных, что ограничивает его применимость в рамках задач информационной безопасности.

Стандарты серии ISO/IEC 27000 обеспечивают комплексный подход к управлению информационной безопасностью и охватывают широкий спектр организационных и технических мер защиты. Вместе с тем данные стандарты носят в значительной степени описательный характер и не содержат детализированных алгоритмов или количественных критериев оценки состояния безопасности [9].

Фреймворк NIST Cybersecurity Framework ориентирован на управление рисками информационной безопасности и отличается высокой гибкостью и адаптируемостью. Однако его практическое применение в условиях требований Российской Федерации может быть ограничено.

Методические документы ФСТЭК России ориентированы на соблюдение национальных требований в области информационной

безопасности, включая защиту критической информационной инфраструктуры [10]. Данные документы обеспечивают высокий уровень формальной защищенности, однако характеризуются жесткой регламентацией и низкой гибкостью.

Риск-ориентированные подходы к обеспечению информационной безопасности позволяют обосновывать выбор защитных мер на основе анализа угроз и оценки рисков, однако в большинстве случаев используют экспертные и качественные методы оценки.

Однако существенным ограничением существующих методологических решений является отсутствие четко формализованных корреляций между техническими параметрами защищаемой системы и фактическим уровнем защищенности базы данных. Это затрудняет проведение количественной оценки эффективности внедряемых мер защиты и может создавать определенные сложности при принятии управленческих решений в области информационной безопасности.

1.2.2. Анализ существующих моделей обеспечения безопасности баз данных.

В практике обеспечения информационной безопасности систем управления базами данных применяются различные модели, предназначенные для формализации процессов защиты информации, оценки уровня защищённости и управления рисками. В зависимости от степени формализации и способа применения данные модели условно можно разделить на вербальные, теоретические (формальные, математические) и экспериментальные.

Вербальные модели ориентированы на качественное описание целей и принципов информационной безопасности и не предусматривают количественной оценки уровня защищённости. Теоретические модели используют формализованный математический аппарат для анализа

свойств защищённости системы, однако их практическое применение в системах управления базами данных ограничено сложностью реализации и необходимостью адаптации к конкретной архитектуре. Экспериментальные модели основаны на имитационном моделировании и тестировании и применяются преимущественно в научно-исследовательской деятельности, что ограничивает их использование в корпоративных системах баз данных [11].

Анализ существующих моделей показывает, что большинство из них ориентировано на решение прямой задачи — оценку уровня защищенности системы при заданных параметрах архитектуры и механизмов защиты. В то же время при проектировании и управлении безопасностью систем баз данных более целесообразным является решение обратной задачи, заключающейся в определении таких параметров системы защиты, которые обеспечивают достижение требуемого уровня безопасности. Это обстоятельство обосновывает необходимость использования подходов, ориентированных на формализованное моделирование процессов информационной безопасности.

Основные используемые модели безопасности для баз данных.

Наиболее распространёнными концептуальными моделями обеспечения безопасности данных являются модели Bell–LaPadula, Biba, Take-Grant, а также модели управления доступом на основе ролей (RBAC).

Модель **Bell–LaPadula** ориентирована на формализацию требований конфиденциальности и использует иерархическую структуру уровней доступа, однако её применение в системах управления базами данных ограничено статичностью правил и отсутствием механизмов гибкого управления правами.

Модель **Biba** направлена на обеспечение целостности данных и предотвращение несанкционированного изменения информации, однако её принципы могут быть реализованы в системах управления базами данных

лишь частично.

Модель **Take-Grant** предназначена для анализа и управления передачей прав доступа между субъектами системы, но её использование на практике связано с усложнением администрирования.

Модели управления доступом на основе ролей получили наибольшее распространение благодаря простоте администрирования и масштабируемости, однако не обеспечивают детализированного контекстного контроля выполнения операций [12].

Для обобщённого сравнения наиболее распространённых моделей обеспечения безопасности баз данных выполнен их сравнительный анализ, результаты которого представлены в таблице 3.

Таблица 3 - Сравнительный анализ существующих моделей

Модель	**Преимущества**	**Ограничения**	**Область применения**
BLP	Высокая защита конфиденциальности	Сложность реализации	Государственные структуры, банки
Biba	Защита целостности	Ограниченная гибкость	Системы учета, финансы
Take-Grant	Гибкое управление правами	Сложность администрирования	Корпоративные системы, проектные команды
RBAC	Простота управления и масштабируемость	Ограниченная детализация контроля	Организации с большим числом пользователей

Проведённый анализ показывает, что каждая из рассмотренных моделей ориентирована на решение отдельных задач обеспечения безопасности, таких как защита конфиденциальности, целостности данных или управление доступом. Ни одна из моделей не обеспечивает комплексного достижения целей безопасности в условиях воздействия деструктивных факторов.

В связи с этим систему управления базами данных целесообразно рассматривать как объект, обладающий свойством обеспечивать достижение целей деятельности организации в условиях внешних и внутренних угроз. Уровень защищённости такой системы определяется не использованием отдельной модели безопасности, а совокупным применением моделей, процедур, организационных мер и технических средств защиты, согласованных между собой и ориентированных на достижение заданного уровня информационной безопасности. То есть достижение целей деятельности рассматривается как свойство защищенности системы, которое обеспечивается только комплексным применением моделей, процедур, правил и технологических средств защиты.

1.2.3 Технические средства реализации защиты баз данных.

С практической точки зрения защита баз данных реализуется с использованием совокупности технических средств, направленных на предотвращение, обнаружение и минимизацию последствий атак.

К основным направлениям технической защиты относятся средства обнаружения вредоносного программного обеспечения и аномальной активности, включая антивирусные решения, сканеры уязвимостей и системы мониторинга работы СУБД. Существенную роль играет предотвращение уязвимостей за счёт корректной настройки параметров безопасности, регулярного обновления программного обеспечения и

автоматизации контроля конфигураций.

Для защиты конфиденциальности информации применяются криптографические методы, обеспечивающие шифрование хранимых и передаваемых данных, а также резервных копий и учетных данных пользователей. Резервное копирование данных является обязательным элементом системы защиты и позволяет восстановить работоспособность базы данных в случае реализации атак, отказов оборудования или ошибок администрирования.

Важным компонентом технической защиты является аудит событий безопасности, обеспечивающий регистрацию действий пользователей и системных процессов и позволяющий выявлять попытки несанкционированного доступа и нарушения политики безопасности.

Разграничение доступа к информационным ресурсам реализуется через комплекс мер, включающих аутентификацию, авторизацию и управление правами пользователей. В соответствии с требованиями ГОСТ Р 50739-95 и стандартов Гостехкомиссии применяются два принципа управления доступом [13]. Дискретное управление обеспечивает индивидуальное назначение прав субъектам с возможностью их передачи другим пользователям, тогда как мандатное управление основывается на использовании меток конфиденциальности информации и официальных разрешений субъектов. Комплексное применение этих методов позволяет строго контролировать доступ к данным и снижает вероятность их несанкционированного использования.

1.3. Обоснование выбора методологии построения модели обеспечения безопасности базы данных.

С учетом выявленных ограничений современных моделей для построения собственной системы защиты базы данных была выбрана методология, позволяющая решать обратную задачу: при заданном уровне

безопасности определяются оптимальные значения параметров каждого процесса системы. В связи с этим для построения модели обеспечения безопасности базы данных в данной выпускной квалификационной работе выбрана методология, основанная на естественно-научном подходе, разработанном в рамках научной школы «Системная интеграция процессов государственного управления». Данная методология ориентирована на формирование информационных процессов с наперёд заданными свойствами устойчивости и безопасности в условиях деструктивных воздействий внешней и внутренней среды.

В основе методологии лежит представление процесса обеспечения информационной безопасности как результата системной интеграции нескольких взаимосвязанных процессов, к которым относятся:

- целевой информационный процесс, реализуемый в системе баз данных;
- процесс образования угроз;
- процесс идентификации угроз;
- процесс нейтрализации угроз;
- показатель информационной безопасности.

В качестве показателя информационной безопасности используется вероятность того, что каждая актуальная угроза для данного целевого информационного процесса будет своевременно идентифицирована и нейтрализована. Такой подход позволяет перейти от качественного описания безопасности к ее количественной оценке.

Методология предполагает задание требуемого уровня информационной безопасности в виде целевого значения вероятности защищенности, а также описание целевого информационного процесса и процесса образования угроз. В результате системной интеграции указанных процессов формируется условие существования процесса обеспечения информационной безопасности, которое может быть представлено в виде

одного уравнения с двумя неизвестными: обобщенной характеристикой процесса идентификации угроз и обобщенной характеристикой процесса их нейтрализации.

Определение данных характеристик исходя из заданного уровня безопасности позволяет решить обратную задачу проектирования системы защиты — сформировать такие параметры процессов идентификации и нейтрализации угроз, которые обеспечивают достижение требуемого уровня информационной безопасности базы данных. Тем самым создаются предпосылки для разработки аналитической математической модели управления безопасностью, ориентированной на целевые показатели защищенности.

Таким образом, выбранная методология позволяет формализовать взаимосвязь между уровнем информационной безопасности базы данных и параметрами процессов идентификации и нейтрализации угроз.

Выводы по первой главе

1. В первой главе выпускной квалификационной работы выполнен анализ архитектуры систем баз данных, их основных компонентов, а также актуальных угроз и уязвимостей информационной безопасности. Проведенная классификация угроз позволила выделить наиболее значимые факторы, оказывающие влияние на устойчивость функционирования баз данных в современных условиях.
2. Анализ существующих методологий и моделей обеспечения безопасности показал, что большинство из них ориентированы на решение прямой задачи оценки защищенности и не обеспечивают формализованной связи между уровнем безопасности и параметрами процессов защиты. Это обусловило необходимость выбора

методологии, ориентированной на решение обратной задачи проектирования системы обеспечения безопасности.

3. В результате обоснован выбор методологии системной интеграции процессов, включающей целевой информационный процесс, процесс образования угроз, процессы их идентификации и нейтрализации, а также показатель информационной безопасности. Применение данной методологии позволяет перейти к количественной оценке уровня защищенности базы данных и сформировать основу для построения аналитической модели управления безопасностью, разрабатываемой в последующих главах работы.

ГЛАВА 2. РАЗРАБОТКА АНАЛИТИЧЕСКОЙ, МАТЕМАТИЧЕСКОЙ МОДЕЛИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ.

2.1. Общий подход к разработке модели обеспечения безопасности систем.

В современной методологии моделирования сложных систем выделяют два базовых подхода: на основе анализа и синтеза. Аналитический подход ориентирован на исследование уже существующих процессов и обладает ограниченной возможностью целенаправленного формирования процессов с заранее заданными характеристиками. Указанное ограничение приобретает критическое значение при моделировании процессов обеспечения информационной безопасности, поскольку в данной области требуется достижение строго определённых временных и функциональных параметров.

В отличие от аналитического, синтетический подход ориентирован на формирование модели с заранее заданными свойствами и позволяет учитывать закономерности функционирования объекта управления уже на этапе проектирования. Применение синтетического подхода обеспечивает более высокую прикладную эффективность моделей управления безопасностью и позволяет согласовать процессы функционирования системы с деятельностью системы обеспечения информационной безопасности.

Под моделью объекта в настоящей работе понимается формализованное описание объекта, позволяющее получать его количественные и качественные характеристики. Управленческое решение рассматривается как модель процесса, с которым взаимодействует субъект управления. Процесс представляет собой объект в действии при фиксированном предназначении.

Синтез модели управления безопасностью базы данных осуществляется на основе закона сохранения целостности объекта [14], представляющего собой устойчивую связь между свойствами объекта и свойствами управленческого воздействия при заданном предназначении.

Модель функционирования системы защиты информации базы данных формируется путём системной интеграции следующих процессов:

– целевого процесса функционирования системы;

– процесса образования угрозы;

– процесса идентификация угрозы;

– процесса нейтрализация угрозы.

В данной ВКР управленческое решение представлено в виде функциональной зависимости:

$$P = F\ (T_Э,\ \Delta t_{пп}\ ,\ \Delta t_{ип}\ ,\ \Delta t_{нп}\ ),$$

где

$T_Э$ – временная характеристика, используемая для прогнозирования эффективности механизмов защиты системы

$\Delta t_{пп}$ — время формирования проблемы,

$\Delta t_{ип}$ — время идентификации угрозы,

$\Delta t_{нп}$ — время нейтрализации угрозы.

Данная зависимость определяет условия существования процесса управления безопасностью системы с базой данных [15].

Графическая иллюстрация процесса формирования модели решения представлена на рисунке 3.

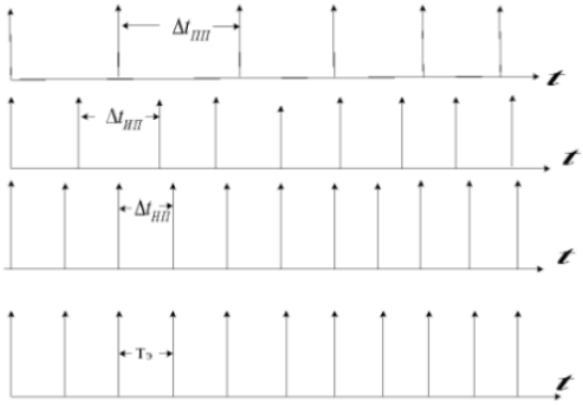

Рисунок 3 - Диаграмма проявления базовых элементов формирования модели решения.

Временная диаграмма показывает соотношение процессов возникновения угроз, их идентификации, нейтрализации и выполнения целевой функции системы и используется для обоснования параметров аналитической модели управленческого решения. Эффективность управления безопасностью при этом достигается при условии, что процессы идентификации и нейтрализации укладываются во временные ограничения, задаваемые целевым процессом функционирования системы.

Рассмотренные четыре процесса, представленные на диаграммах, описывают функционирование системы с базой данных в различных режимах ее работы.

Модель функционирования системы можно представить в виде графа:

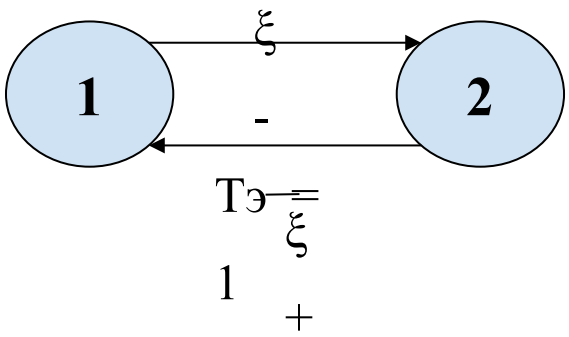

Рисунок 4 - Граф состояний

, где $Tэ = \frac{1}{\xi+}$ - среднее время выполнения запроса.

При функционировании системы существует риск неудовлетворения запроса, который описывается частотой срыва выполнения запроса ξ-. Работа базы данных характеризуется интенсивностью выполнения запросов ξ+. В условиях воздействия каких либо деструктивных факторов возникает вероятность нарушения нормального функционирования системы с базой данных.

Возникает вопрос о согласовании процесса функционирования системы с деятельностью системы обеспечения безопасности. Для решения данной задачи используется естественнонаучный подход (ЕНП), основанный на интеграции свойств мышления человека, закономерностей окружающего мира и процессов познания, реализуемый в рамках научно-педагогической школы «Системная интеграция процессов государственного управления».

При этом необходимо учитывать логику функционирования базы данных и минимизировать время, затрачиваемое специалистом по информационной безопасности - лицом, принимающим решение - на анализ выявленных уязвимостей и последствий деструктивного воздействия. Для реализации автоматизированного управления требуется определить условия существования процесса и обеспечить обратную связь, структурная схема которой представлена на рисунке *.

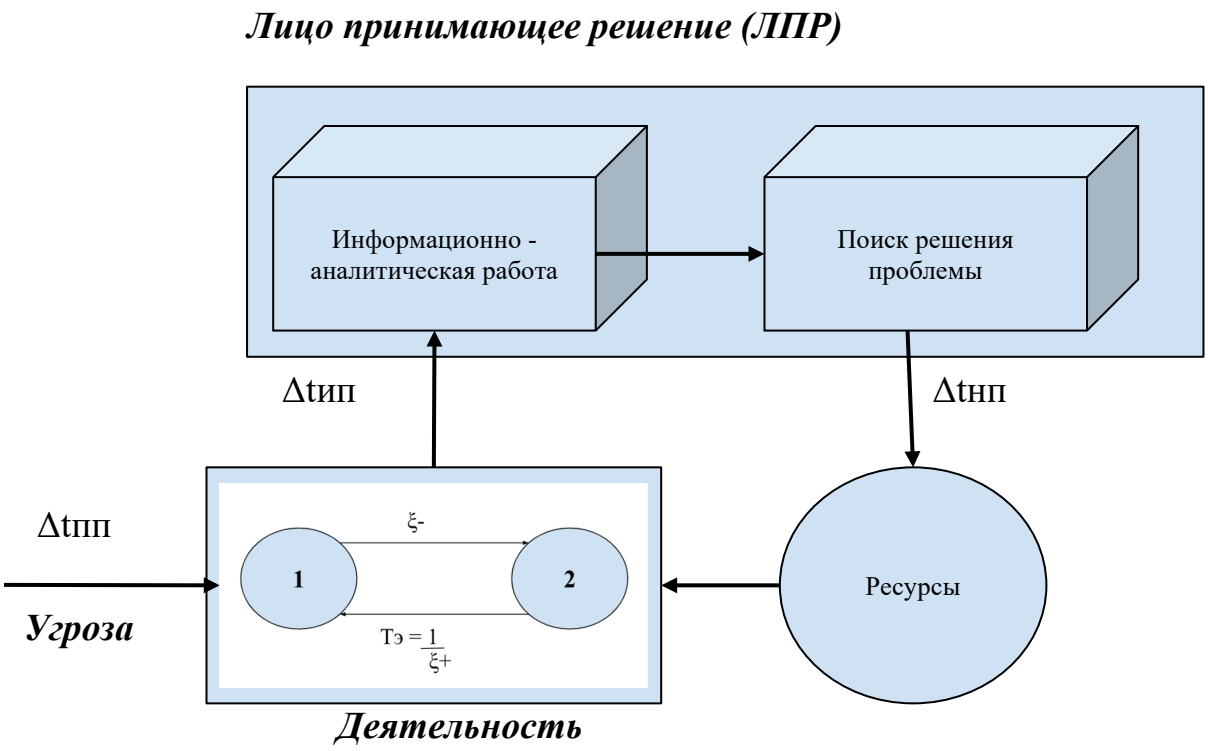

Рисунок 5 - Структурная схема функционирования базы данных на основе обратной связи.

Необходимо учесть логику функционирования системы управления безопасностью базы данных и сократить время, необходимое специалисту для принятия решения об обнаруженных уязвимостях или атаках, используя средства автоматического управления. Для реализации автоматического управления необходимо определить условия существования процесса и обеспечить обратную связь.

В результате синтеза модели управления безопасностью базы данных преобразована математическая модель управленческого решения следующего вида.

Функционирование системы описывается через последовательность состояний, образующих замкнутый цикл. В начальном состоянии (состояние 1) система находится в режиме непрерывного мониторинга, осуществляя сбор данных о состоянии объектов управления. Интенсивность поступления угроз характеризуется параметром λΔтпп -

частотой возникновения потенциальных угроз. При обнаружении воздействия угрозы система переходит в состояние 3 («Деятельность»), где специалист в течение времени Δтип осуществляет идентификацию проблемы: анализирует признаки угрозы, классифицирует её и оценивает критичность. На этом этапе формируется запрос на привлечение дополнительных ресурсов для решения проблемы.

Следующим этапом является состояние 4 (анализ и планирование нейтрализации), в рамках которого ЛПР, опираясь на результаты информационно-аналитической работы и поиска решения, определяет характер угрозы, необходимые ресурсы для её нейтрализации и стратегию устранения. Этот этап критически важен для минимизации времени реакции системы. После разработки плана система переходит в состояние 2 (нейтрализация угрозы), где реализуется разработанный план с использованием выделенных ресурсов. После успешного устранения угрозы система возвращается в исходное состояние (состояние 1), и цикл повторяется при поступлении новой угрозы.

Ключевыми параметрами, характеризующими эффективность функционирования системы, являются следующие показатели:

Параметр ξ^{+} определяет интенсивность выполнения целевого процесса и рассчитывается как величина, обратная среднему времени выполнения целевой задачи Тэ.

Параметр ξ^{-} характеризует интенсивность срыва выполнения целевой задачи и отражает вероятность нарушения нормального функционирования системы под воздействием деструктивных факторов.

$v2 = 1/\Delta tPN$ — частота перехода из состояния 4 в состояние 2, где ΔtPN — среднее время нейтрализации задачи. Параметр v2 напрямую связан с

уровнем компетентности системы в решении неизвестных (нештатных) задач: чем выше значение v2, тем эффективнее система справляется с новыми типами угроз.

Механизм функционирования системы можно описать следующим образом. При поступлении сигнала об угрозе (с интенсивностью $\lambda\Delta t_{пп}$) система фиксирует событие и переводит процесс в состояние «Деятельность» (3). В этом состоянии выполняется сбор дополнительных данных, корреляция событий, определение источника и вектора атаки, а также оценка потенциального ущерба. На этапе принятия решения ЛПР, опираясь на аналитические данные, выбирает стратегию нейтрализации с учетом критичности угрозы, доступных ресурсов и временных ограничений. Реализация решения осуществляется путём задействования необходимых ресурсов (блок «Ресурсы») и выполнения плана нейтрализации (состояние 2). После успешного устранения угрозы система возвращается в режим мониторинга (состояние 1), и цикл повторяется.

Эта логика рассуждений позволяет построить граф состояний системы, в котором выделяются следующие состояния [16]:
S1 — нормальное функционирование системы (ожидание запроса или угрозы);
S2 — целевое состояние системы;
S3 — состояние обнаруженной, но не идентифицированной угрозы;
S4 — состояние идентифицированной угрозы, ожидающей нейтрализации.

Переходы между состояниями характеризуются интенсивностями:

λ – интенсивность появления угрозы (S1→S3);

ξ^+ – интенсивность поступления запросов/перехода к целевому выполнению (S1→S2);

ξ^- - интенсивность завершения выполнения запроса и возврата к мониторингу (S2→S1);

v_1 – интенсивность идентификации угрозы (S3→S4);

v_2 – интенсивность нейтрализации угрозы (S4→S2);

v_3 – интенсивность срыва нейтрализации (S4→S1).

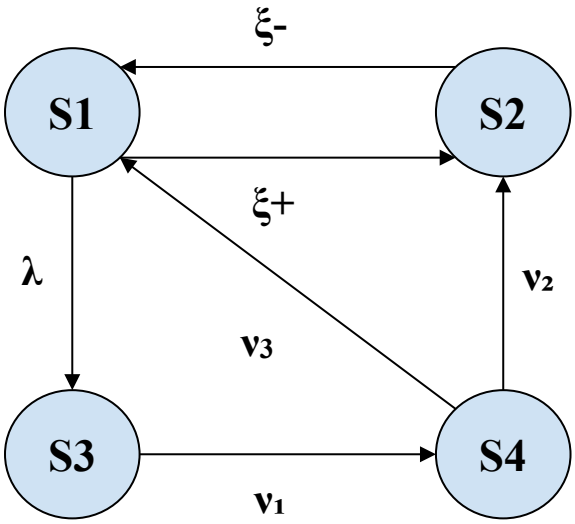

Рисунок 6 - Граф состояний процесса формирования управленческого решения.

На фоне этого может быть использована система дифференциальных уравнений Колмогорова:

$$\frac{dPi(t)}{dt} = \sum_{j=1}^{n} \lambda\, ij(t) * Pj(t) - Pi(t) * \sum_{j=1}^{n} ij(t),$$

где i = 0,1,2,...,n.

Конечные вероятности состояний могут быть вычислены путем решения системы линейных алгебраических уравнений, которые получены

из дифференциальных уравнений Колмогорова. Это возможно в случае, если производные равны нулю, а вероятностные функции состояний — $P_1(t)$, …, $P_n(t)$ — в правой части уравнений переходят в неизвестные конечные вероятности — P_1, …, P_n.

Чтобы найти точные значения P_1, …, P_n, к уравнениям добавляется нормализующее условие: $P_0 + P_1 + \ldots + P_n = 1$.

Система уравнений Колмогорова для графа состояний, изображённого на рисунке , имеет следующий вид:

$$\frac{dP1(t)}{dt} = -(\xi^+ + \lambda) \cdot P_1(t) + \xi^- \cdot P_2(t)$$

$$\frac{dP2(t)}{dt} = \xi^+ \cdot P_1(t) - \xi^- \cdot P_2(t) + \nu_2 \cdot P_4(t)$$

$$\frac{dP3(t)}{dt} = \lambda \cdot P_1(t) - \nu_1 \cdot P_3(t)$$

$$\frac{dP4(t)}{dt} = \nu_1 \cdot P_3(t) - \nu_2 \cdot P_4(t)$$

Конечные вероятности могут быть вычислены путем решения системы алгебраических уравнений:

$$0 = -(\xi^+ + \lambda) \cdot P_1 + \xi^- \cdot P_2$$

$$0 = \xi^+ \cdot P_1 - \xi^- \cdot P_2 + \nu_2 \cdot P_4$$

$$0 = \lambda \cdot P_1 - \nu_1 \cdot P_3$$

$$1 = P_1 + P_2 + P_3 + P_4$$

Системное решение выглядит следующим образом:

$$P_1 = \frac{(\nu 1 \cdot \nu 2 \cdot \xi -)}{(\lambda \cdot \nu 1 \cdot \nu 2 + \lambda \cdot \nu 1 \cdot \xi^- + \lambda \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi -)}$$

$$P_2 = \frac{(\lambda \cdot \nu 1 \cdot \nu_2)}{(\lambda \cdot \nu 1 \cdot \nu 2 + \lambda \cdot \nu 1 \cdot \xi^- + \lambda \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi -)}$$

$$P_3 = \frac{(\lambda \cdot \nu 1 \cdot \xi^-)}{(\lambda \cdot \nu 1 \cdot \nu 2 + \lambda \cdot \nu 1 \cdot \xi^- + \lambda \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi -)}$$

$$P_4 = \frac{(\lambda \cdot \nu 1 \cdot \xi^-)}{(\lambda \cdot \nu 1 \cdot \nu 2 + \lambda \cdot \nu 1 \cdot \xi^- + \lambda \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot v_2 \cdot \xi -)}$$

Вероятность выявления и нейтрализации проблемы ёмкостью определяется следующей корреляцией:

$$P_2 = \frac{(\lambda \cdot \nu 1 \cdot \nu 2 + \nu 1 \cdot \nu 2 \cdot \xi^+)}{(\lambda \cdot \nu 1 \cdot \nu 2 + \lambda \cdot \nu 1 \cdot \xi - + \lambda + \nu 2 \cdot \xi - + \nu 1 \cdot \nu 2 \cdot \xi^+ + \nu 1 \cdot \nu 2 \cdot \xi -)}$$

В этом соотношении связаны три параметра. Таким образом, установлена аналитическая зависимость обобщённых характеристик появления проблемы ($\Delta t_{пп}$), идентификации проблемы ($\Delta t_{нп}$) и нейтрализации проблемы ($\Delta t_{нп}$).

Для анализа модели используются сетевые модели, которые представляют разновидность ориентированных графов. Вершины графа — это события обнаружения проблем, определяющие начало и окончание отдельных работ, а дуги в этом случае будут соответствовать работам. В данной работе используется сетевая модель, так как наглядно видно, как взаимодействуют узлы друг с другом.

α — интенсивность целевого функционирования

λ — интенсивность появления угроз

ν_1 — интенсивность идентификации угроз

ν_2 — интенсивность нейтрализации угроз

T_{pi} — раннее время наступления события

$T_{пi}$ — позднее допустимое время наступления события

R_i — резерв времени события

2.2. Проектирование сетевой модели образования угроз базы данных.

2.2.1. Сетевая модель целевого процесса функционирования системы

Перед построением сетевых графиков необходимо разработать таблицу, содержащую в себе перечень событий, которые определяют планируемый процесс и без которых он не может состояться. После этого продумываются работы, в результате которых все необходимые события должны произойти. Далее указывается, какие работы являются предшествующими по отношению к данной, а какие — последующими.

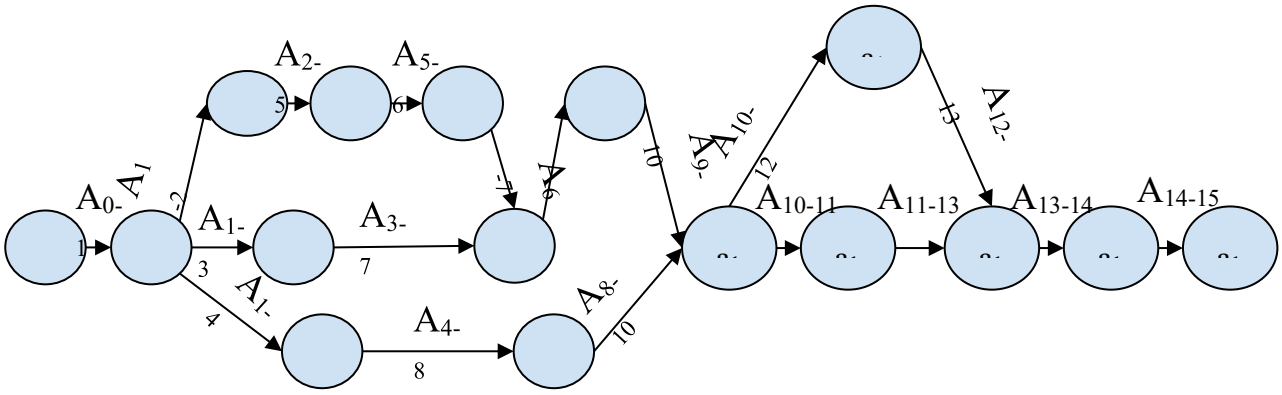

Рисунок 7 - Сетевой график целевого процесса системы

Для формализации структуры сетевого графа введен перечень событий целевого процесса, представленный в таблице 4. Каждое событие отражает завершение определённого этапа обработки пользовательского запроса и служит основой для построения временной модели функционирования системы.

Таблица 4 - События целевого процесса.

Обозначение	**Наименование i-го события**

a_0	Система находится в режиме ожидания пользовательского запроса
a_1	Пользователь инициировал формирование запроса к базе данных
a_2	Запрос передан по сетевому интерфейсу в СУБД
a_3	Выполнен синтаксический разбор структуры запроса
a_4	Выполнение аутентификации пользователя
a_5	Выполнение проверки учетных данных пользователя
a_6	Выполнение авторизации и проверки ролей пользователя
a_7	Определение типа запроса (чтение / модификация)
a_8	Выполнение проверки прав доступа к объектам БД
a_9	Выполнен анализ индексов и структуры хранения данных
a_{10}	Подготовка плана выполнения запроса
a_{11}	Выполнение операции чтения данных
a_{12}	Выполнение операции изменения данных
a_{13}	Выполнены операции изменения данных
a_{14}	Выполнение контроля целостности и согласованности данных
a_{15}	Передача запроса пользователю и фиксация в журнале

Таблица 5 - Работы целевого процесса.

Обозначение работ	Наименование работы перевода процесса от i-го события к j-му событию	tij, с	Предшествующие работы	Последующие работы	rni,j, с
A_{0-1}	Инициация пользовательск	2	-	A_{1-2} A_{1-3}	0

	ого взаимодействия			A_{1-4}	
A_{1-2}	Передача запроса в СУБД	2	A_{0-1}	A_{2-5}	0
A_{1-3}	Передача запроса в подсистему управления БД	2	A_{0-1}	A_{3-7}	9
A_{1-4}	Запуск процедур контроля безопасности	2	A_{0-1}	A_{4-8}	7
A_{2-5}	Аутентификация пользователя	4	A_{1-2}	A_{5-6}	0
A_{5-6}	Авторизация доступа	4	A_{2-5}	A_{6-9}	0
A_{3-7}	Анализ структуры запроса	3	A_{1-3}	A_{7-9}	9
A_{4-8}	Контроль допустимости операций	3	A_{1-4}	A_{8-10}	7
A_{6-9}	Формирование логического плана	5	A_{5-6}	A_{9-10}	0
A_{7-9}	Передача данных анализа запроса	1	A_{3-7}	A_{9-10}	9
A_{8-10}	Формирование физического плана	5	A_{4-8}	A_{10-11} A_{10-12}	7

$A_{9\text{-}10}$	Согласование плана выполнения	2	$A_{6\text{-}9}$ $A_{7\text{-}9}$	$A_{10\text{-}11}$ $A_{10\text{-}12}$	0
$A_{10\text{-}11}$	Выполнение операций чтения	6	$A_{8\text{-}10}$ $A_{9\text{-}10}$	$A_{11\text{-}13}$	0
$A_{10\text{-}12}$	Выполнение операций модификации	6	$A_{8\text{-}10}$ $A_{9\text{-}10}$	$A_{12\text{-}13}$	0
$A_{11\text{-}13}$	Контроль целостности передаваемых данных	4	$A_{10\text{-}11}$	$A_{13\text{-}14}$	0
$A_{12\text{-}13}$	Контроль согласованности данных	4	$A_{10\text{-}12}$	$A_{13\text{-}14}$	0
$A_{13\text{-}14}$	Формирование результата обработки	4	$A_{11\text{-}13}$ $A_{12\text{-}13}$	$A_{14\text{-}15}$	0
$A_{14\text{-}15}$	Передача результата пользователю	3	$A_{13\text{-}14}$	-	0

Анализ сетевого графика целевого функционирования системы с базой данных

Наиболее раннее время наступления j-го события $T_p(j)$ вычисляется по формуле:

$$Tp(j) = \frac{max}{i \subset j}(Tp(i) + tij),$$

где

i и j — номера предшествующего и последующего событий;

t_{ij} — продолжительность работы между событиями i и j.

Самое позднее допустимое время наступления i-го события $T_п$ (i) вычисляется по формуле: $T_п$ (j) = $\frac{min}{i \supset j}$ $(Tn\,(i) - tij)$

Резервное время (R_i) и полное резервное время ($r_п$ (i,j)) вычисляются по формуле:

$r_п$ (i,j) = ($T_п$ (j) - T_p(i) - t_{ij})

R_i = ($T_п$ (i) - T_p (i))

<u>Расчет ранних сроков идентификации угрозы:</u>

T_p (a_0) = 0	T_p (a_6) =8+4=12	T_p (a_{12}) = 19+6=25
T_p (a_1)=0+2=2	T_p (a_7) =4+7=3	T_p (a_{13})= 29
T_p (a_2) =2+2=4	T_p (a_8) =4+3=7	T_p (a_{14})=29+4=33
T_p (a_3) =2+2=4	T_p (a_9) = 17	T_p (a_{15})=33+3=36
T_p (a_4) =2+2=4	T_p (a_{10}) = 19	
T_p (a_5) =4+4=8	T_p (a_{11}) = 19+6=25	

<u>Расчет поздних сроков идентификации угрозы:</u>

$T_п$ (a_0) = 2-2=0	$T_п$ (a_6) = 17-5=12	$T_п$ (a_{12}) = 29-4=25
$T_п$ (a_1) = 2	$T_п$ (a_7) = 17-1=16	$T_п$ (a_{13}) = 33-4=29
$T_п$ (a_2) = 8-4=4	$T_п$ (a_8) = 19-5=14	$T_п$ (a_{14}) = 36-3=33
$T_п$ (a_3) =16-3=13	$T_п$ (a_9) = 19-2=17	$T_п$ (a_{15}) = 36
$T_п$ (a_4) = 14-3=11	$T_п$ (a_{10}) = 19	
$T_п$ (a_5) = 12-4=8	$T_п$ (a_{11}) = 29-4=25	

<u>Резервы событий Ri идентификации угрозы:</u>

R_0 = 0-0=0	R_8 = 14-7=7
R_1 = 2-2=4	R_9 = 17-17=0
R_2 = 4−4=0	R_{10}= 19−19=0

R_3 = 13−4=9	R_{11}= 25-25=0
R_4 = 11−4=7	R_{12} = 25-25=0
R_5 = 8-8=0	R_{13} = 29−29=0
R_6 = 12−12=0	R_{14} =33-33=0
R_7 = 16−7=9	R_{15} = 36-36=0

Полные резервы работ rp(i,j) появление угрозы:

$r_п$(0,1)= 5-0-5=0	$r_п$(5,8)= 37-29-8=0	$r_п$(12,13)= 62-52-10=0
$r_п$(1,2)= 17-5-12=0	$r_п$(6,9)= 37-25-10=2	$r_п$(13,14)= 67-62-5=0
$r_п$(1,3)= 17-5-10=2	$r_п$(7,10)= 37-23-9=5	$r_п$(14,15)= 72-67-5=0
$r_п$(1,4)= 19-5-9=5	$r_п$(8,11)= 42-37-5=0	
$r_п$(2,5)= 29-17-12=0	$r_п$(9,11)= 42-35-5=2	
$r_п$(3,6)= 27-15-10=2	$r_п$(10,11)= 42-32-5=5	
$r_п$(4,7)= 28-14-9=5	$r_п$(11,12)= 52-42-10=0	

2.1.2. Сетевая модель процесса появления угрозы

Интенсивность **λ** процесса появления угрозы

Это процесс, переводящий систему из S1 в S3 (Обнаруженная, но не идентифицированная угроза).

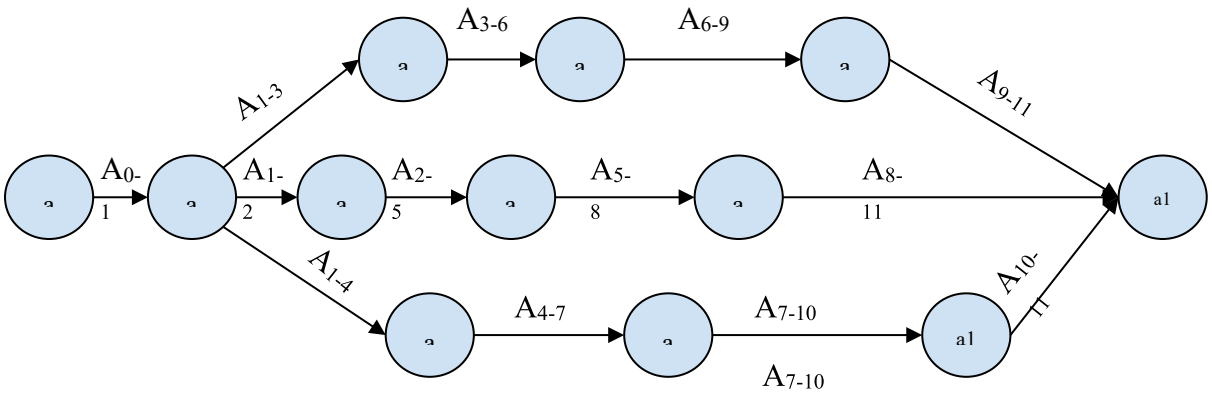

Рисунок 8 - Сетевой график процесса появления угрозы

Обозначение	**Наименование i-го события**
a_0	Нормальное функционирование системы базы данных (отсутствие активных угроз)
a_1	Инициация деструктивного воздействия на систему
a_2	Формирование угрозы программного обеспечения
a_3	Формирование угрозы аппаратного обеспечения
a_4	Формирование угрозы несанкционированного доступа к данным
a_5	Нарушение функционирования СУБД вследствие программной угрозы
a_6	Отказ аппаратных ресурсов системы хранения и обработки данных
a_7	Попытка обхода механизмов защиты доступа к базе данных
a_8	Нарушение целостности данных базы данных
a_9	Потеря доступности базы данных
a_{10}	Утечка конфиденциальной информации из базы данных
a_{11}	Фиксация инцидента информационной безопасности
a_{12}	Сформированная угроза безопасности базы данных

Таблица 6 - События появления угроз.

Таблица 7 - Работы процесса появления угроз.

Обозначение работ	Наименование работы перевода процесса от i-го события к j-му событию	tij, с	Предшествующие работы	Последующие работы	rni,j, с

A_{0-1}	Инициация деструктивного воздействия	10	-	A_{1-2} A_{1-3} A_{1-4}	0
A_{1-2}	Развитие программной угрозы	15	A_{0-1}	A_{2-5}	0
A_{1-3}	Развитие аппаратной угрозы	20	A_{0-1}	A_{3-6}	0
A_{1-4}	Формирование угрозы несанкционированного доступа	15	A_{0-1}	A_{4-7}	5
A_{2-5}	Нарушение логики функционирования СУБД	15	A_{1-2}	A_{5-8}	0
A_{3-6}	Отказ аппаратных компонентов системы	20	A_{1-3}	A_{6-9}	0
A_{4-7}	Реализация обхода механизмов защиты	15	A_{1-4}	A_{7-10}	5
A_{5-8}	Искажение и повреждение данных	20	A_{2-5}	A_{8-11}	0
A_{6-9}	Потеря доступа к базе данных	10	A_{3-6}	A_{9-11}	0
A_{7-10}	Несанкционированное	15	A_{4-7}	A_{10-11}	5

	извлечение информации				
A_{8-11}	Фиксация нарушения целостности данных	5	A_{5-8}	A_{11-12}	0
A_{9-11}	Фиксация отказа аппаратных ресурсов	5	A_{6-9}	A_{11-12}	0
A_{10-11}	Фиксация отказа аппаратных ресурсов	5	A_{7-10}	A_{11-12}	5
A_{11-12}	Завершение формирования угрозы	5	A_{8-11} A_{9-11} A_{10-11}	-	

2.2.3. Сетевая модель процесса идентификации угрозы

Это процесс перехода системы из состояния S3 в S4, когда угроза идентифицирована, но ожидает нейтрализации.

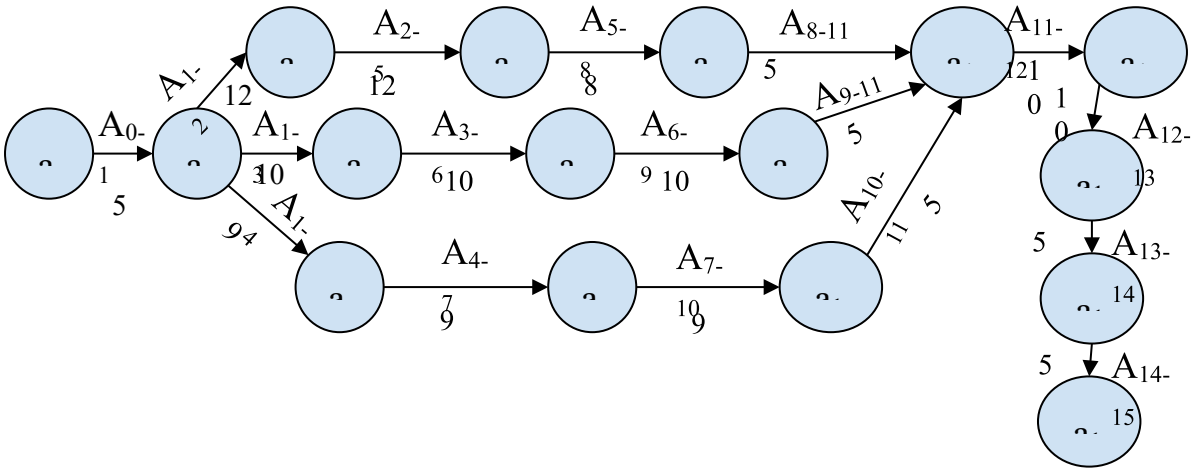

Рисунок 9 - Сетевой график процесса идентификации угрозы

Таблица 8 - События процесса идентификации угрозы.

Обозначение	Наименование i-го события
A_0	Сбор журналов сетевой активности
A_1	Инициация процедуры идентификации угрозы
A_2	Сбор журналов сетевой активности
A_3	Сбор журналов СУБД
A_4	Сбор журналов систем управления доступом
A_5	Анализ сетевой активности
A_6	Анализ журналов базы данных
A_7	Анализ прав и политик доступа
A_8	Выявление аномалий сетевого поведения
A_9	Выявление нарушений целостности данных
A_{10}	Выявление нарушений разграничения доступа
A_{11}	Корреляция событий безопасности
A_{12}	Определение источника и типа угрозы
A_{13}	Оценка уровня критичности угрозы
A_{14}	Подготовка решения по реагированию
A_{15}	Угроза идентифицирована

Таблица 9 - Работы процесса идентификации угрозы.

Обозначение работ	Наименование работы перевода процесса от i-го события к j-му событию	tij, с	Предшествующие работы	Последующие работы	rni,j, с
A_{0-1}	Запуск процедуры идентификации	5	-	A_{1-2} A_{1-3}	0

				A_{1-4}	
A_{1-2}	Анализ сетевых событий	12	A_{0-1}	A_{2-5}	0
A_{1-3}	Сбор журналов СУБД	10	A_{0-1}	A_{3-6}	2
A_{1-4}	Сбор журналов доступа	9	A_{0-1}	A_{4-7}	5
A_{2-5}	Анализ сетевой активности	12	A_{1-2}	A_{5-8}	0
A_{3-6}	Анализ журналов БД	10	A_{1-3}	A_{6-9}	2
A_{4-7}	Анализ прав доступа	9	A_{1-4}	A_{7-10}	5
A_{5-8}	Выявление сетевых аномалий	8	A_{2-5}	A_{8-11}	0
A_{6-9}	Выявление нарушений целостности	10	A_{3-6}	A_{9-11}	2
A_{7-10}	Выявление нарушений доступа	9	A_{4-7}	A_{10-11}	5
A_{8-11}	Передача сетевых инцидентов на корреляцию	5	A_{5-8}	A_{11-12}	0
A_{9-11}	Передача инцидентов БД на корреляцию	5	A_{6-9}	A_{11-12}	2
A_{10-11}	Передача инцидентов доступа на корреляцию	5	A_{7-10}	A_{11-12}	5
A_{11-12}	Корреляция событий безопасности	10	A_{8-11} A_{9-11} A_{10-11}	A_{12-13}	0
A_{12-13}	Оценка	10	A_{11-12}	A_{13-14}	0

	критичности угрозы				
A_{13-14}	Формирование решения реагирования	5	A_{12-13}	A_{14-15}	0
A_{14-15}	Завершение идентификации угрозы	5	A_{13-14}	-	0

Расчет ранних сроков идентификации угрозы:

$T_р(a_0) = 0$	$T_р(a_6) = 15+10=25$	$T_р(a_{12}) = 42+10=52$
$T_р(a_1) = 0+5=5$	$T_р(a_7) = 14+9=23$	$T_р(a_{13}) = 52+10=62$
$T_р(a_2) = 5+12=17$	$T_р(a_8) = 29+8=37$	$T_р(a_{14}) = 62+5=67$
$T_р(a_3) = 5+10=15$	$T_р(a_9) = 25+10=35$	$T_р(a_{15}) = 67+5=72$
$T_р(a_4) = 5+9=14$	$T_р(a_{10}) = 23+9=32$	
$T_р(a_5) = 17+12=29$	$T_р(a_{11}) = 42$	

Расчет поздних сроков идентификации угрозы:

$T_п(a_0) = 5-5=0$	$T_п(a_6) = 37-10=27$	$T_п(a_{12}) = 62-10=52$
$T_п(a_1) = 5$	$T_п(a_7) = 37-9=28$	$T_п(a_{13}) = 67-5=62$
$T_п(a_2) = 29-12=17$	$T_п(a_8) = 42-5=37$	$T_п(a_{14}) = 72-5=67$
$T_п(a_3) = 27-10=17$	$T_п(a_9) = 42-5=37$	$T_п(a_{15}) = 72$
$T_п(a_4) = 28-9=19$	$T_п(a_{10}) = 42-5=37$	
$T_п(a_5) = 37-8=29$	$T_п(a_{11}) = 52-10=42$	

Резервы событий Ri идентификации угрозы:

$R_0 = 0-0=0$	$R_8 = 37-37=0$
$R_1 = 5-5= 0$	$R_9 = 37-35=2$

R_2 = 17-17=0	R_{10}= 37-32=5
R_3 = 17-15=2	R_{11}= 42-42=0
R_4 = 19-14=5	R_{12} = 52-52=0
R_5 = 29-29=0	R_{13} = 62-62=0
R_6 = 27-25=2	R_{14} = 67-67=0
R_7 = 28-23=5	R_{15} = 72-72=0

Полные резервы работ rp(i,j) появление угрозы:

$r_п$(0,1)= 5-0-5=0	$r_п$(5,8)= 37-29-8=0	$r_п$(12,13)= 62-52-10=0
$r_п$(1,2)= 17-5-12=0	$r_п$(6,9)= 37-25-10=2	$r_п$(13,14)= 67-62-5=0
$r_п$(1,3)= 17-5-10=2	$r_п$(7,10)= 37-23-9=5	$r_п$(14,15)= 72-67-5=0
$r_п$(1,4)= 19-5-9=5	$r_п$(8,11)= 42-37-5=0	
$r_п$(2,5)= 29-17-12=0	$r_п$(9,11)= 42-35-5=2	
$r_п$(3,6)= 27-15-10=2	$r_п$(10,11)= 42-32-5=5	
$r_п$(4,7)= 28-14-9=5	$r_п$(11,12)= 52-42-10=0	

Критический путь:

$A_{0\text{-}1} \rightarrow A_{1\text{-}2} \rightarrow A_{2\text{-}5} \rightarrow A_{5\text{-}8} \rightarrow A_{8\text{-}11} \rightarrow A_{11\text{-}12} \rightarrow A_{12\text{-}13} \rightarrow A_{13\text{-}14} \rightarrow A_{14\text{-}15}$

Ткр = 5+12+12+8+5+10+10+5+5=72 с

Интенсивность:

$$\nu_1 = \frac{1}{Tкр}$$

$$_1 = \frac{1}{72} = 0,0139 \text{ с}^{(-1)} \approx 1{,}2 \cdot 103 \text{ сут}^{-1}$$

2.2.4. Сетевая модель процесса нейтрализации угрозы

Это процесс перехода системы из состояния S4 в состояние S2 (Угроза нейтрализована, система вернулась к работе).

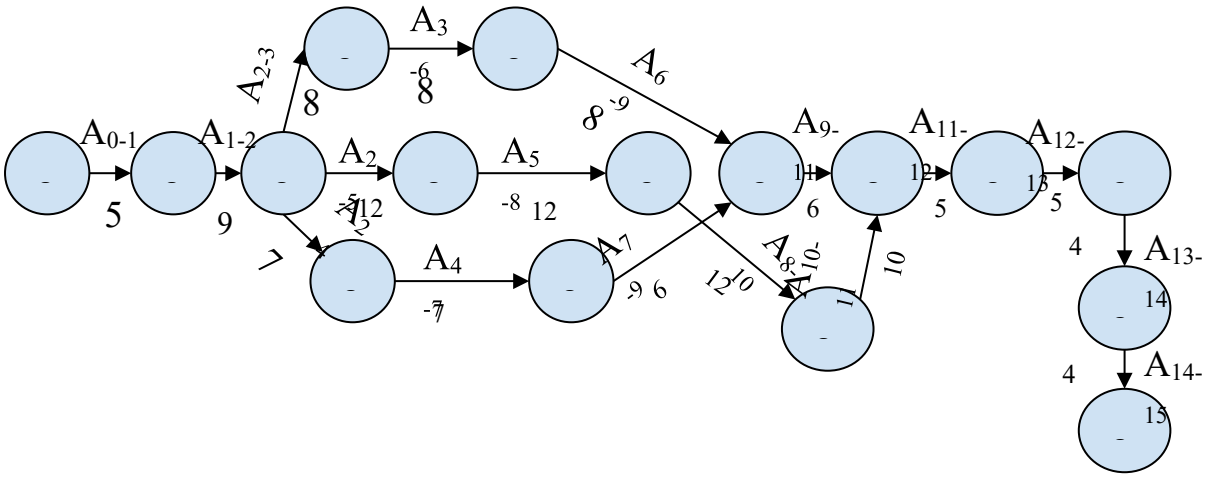

Рисунок 10 - Сетевой график нейтрализации угроз системы

Таблица 10 - События процесса нейтрализации угрозы.

Обозначение	Наименование i-го события
A_0	Подтверждённая идентифицированная угроза
A_1	Инициация процедуры нейтрализации угрозы
A_2	Выбор стратегии реагирования
A_3	Подготовка программных мер защиты
A_4	Подготовка организационных мер реагирования
A_5	Контроль функционирования
A_6	Ограничение доступа к ресурсам БД
A_7	Блокировка подозрительных учетных записей
A_8	Изоляция скомпрометированных компонентов
A_9	Восстановление целостности данных
A_{10}	Восстановление конфигурации безопасности
A_{11}	Проверка корректности функционирования БД

A_{12}	Тестирование защитных механизмов
A_{13}	Контроль отсутствия повторной угрозы
A_{14}	Подтверждение устранения угрозы
A_{15}	Восстановленное штатное функционирование системы

Таблица 11 - Работы процесса нейтрализации угрозы.

Обозначение работ	Наименование работы перевода процесса от i-го события к j-му событию	tij, с	Предшествующие работы	Последующие работы	rпi,j, с
A_{0-1}	Запуск процедуры нейтрализации	5	-	A_{1-2}	0
A_{1-2}	Анализ доступных стратегий реагирования	9	A_{0-1}	A_{2-3} A_{2-4} A_{2-5}	0
A_{2-3}	Формирование программных мер защиты	8	A_{1-2}	A_{3-6}	16
A_{2-4}	Формирование организационных мер реагирования	7	A_{1-2}	A_{4-7}	20
A_{2-5}	Формирование аппаратных мер защиты	12	A_{1-2}	A_{5-8}	0

A_{3-6}	Реализация ограничений доступа	8	A_{2-3}	A_{6-9}	16
A_{4-7}	Блокировка учетных записей	7	A_{2-4}	A_{7-9}	20
A_{5-8}	Изоляция компонентов системы	12	A_{2-5}	A_{8-10}	0
A_{6-9}	Восстановление целостности данных	8	A_{3-6}	A_{9-11}	16
A_{7-9}	Контроль последствий блокировки	6	A_{4-7}	A_{9-11}	20
A_{8-10}	Коррекция параметров безопасности	12	A_{5-8}	A_{10-11}	0
A_{9-11}	Проверка функционирования БД	6	A_{6-9} A_{7-9}	A_{11-12}	16
A_{10-11}	Проверка конфигурации безопасности	10	A_{8-10}	A_{11-12}	0
A_{11-12}	Тестирование системы защиты	5	A_{9-11} A_{10-11}	A_{12-13}	0
A_{12-13}	Контроль повторных проявлений угроз	5	A_{11-12}	A_{13-14}	0
A_{13-14}	Подтверждение нейтрализаци	4	A_{12-13}	A_{14-15}	0

	и угрозы				
A_{14-15}	Возврат системы к штатной работе	4	A_{13-14}	-	0

Расчет ранних сроков нейтрализации угрозы:

$T_p(a_0) = 0$	$T_p(a_6) = 22+8=30$	$T_p(a_{12}) = 60+5=65$
$T_p(a_1) = 0+5=5$	$T_p(a_7) = 21+7=28$	$T_p(a_{13}) = 65+5=70$
$T_p(a_2) = 5+9=14$	$T_p(a_8) = 26+12=38$	$T_p(a_{14}) = 70+4=74$
$T_p(a_3) = 14+8=22$	$T_p(a_9) = 38$	$T_p(a_{15}) = 74+4=78$
$T_p(a_4) = 14+7=21$	$T_p(a_{10}) = 38+12=50$	
$T_p(a_5) = 14+12=26$	$T_p(a_{11}) = 60$	

Расчет поздних сроков нейтрализации угрозы:

$T_п(a_0) = 5-5=0$	$T_п(a_6) = 54-8=46$	$T_п(a_{12}) = 70-5=65$
$T_п(a_1) = 14-9=5$	$T_п(a_7) = 54-6=48$	$T_п(a_{13}) = 74-4=70$
$T_п(a_2) = 14$	$T_п(a_8) = 50-12=38$	$T_п(a_{14}) = 78-4=74$
$T_п(a_3) = 46-8=38$	$T_п(a_9) = 60-6=54$	$T_п(a_{15}) = 78$
$T_п(a_4) = 48-7=41$	$T_п(a_{10}) = 60-10=50$	
$T_п(a_5) = 38-12=26$	$T_п(a_{11}) = 65-5=60$	

Резервы событий Ri нейтрализации угрозы:

$R_0 = 0-0=0$	$R_8 = 38-38=0$
$R_1 = 5-5=0$	$R_9 = 54-38=16$
$R_2 = 14-14=0$	$R_{10} = 50-50=0$
$R_3 = 38-22=16$	$R_{11} = 60-60=0$
$R_4 = 41-21=20$	$R_{12} = 65-65=0$
$R_5 = 26-26=0$	$R_{13} = 70-70=0$

R_6 = 46-30=16	R_{14} = 74-74=0
R_7 = 48-28=20	R_{15} = 78-78=0

Полные резервы работ rp(i,j) нейтрализации угрозы:

$r_п(0,1)$= 5-0-5=0	$r_п(5,8)$= 38-26-12=0	$r_п(12,13)$= 70-65-5=0
$r_п(1,2)$= 14-5-9=0	$r_п(6,9)$= 54-30-8=16	$r_п(13,14)$= 74-70-4=0
$r_п(2,3)$= 38-14-8=16	$r_п(7,9)$= 54-28-6=20	$r_п(14,15)$= 78-74-4=0
$r_п(2,4)$= 41-14-7=20	$r_п(8,10)$= 50-38-12=0	
$r_п(2,5)$= 26-14-12=0	$r_п(9,11)$= 60-38-6=16	
$r_п(3,6)$= 46-22-8=16	$r_п(10,11)$= 60-50-10=0	
$r_п(4,7)$= 48-21-7=20	$r_п(11,12)$= 65-60-5=0	

Расчет интенсивности нейтрализации угрозы

Критический путь:

$A_{0-1} \rightarrow A_{1-2} \rightarrow A_{2-5} \rightarrow A_{5-8} \rightarrow A_{8-10} \rightarrow A_{10-11} \rightarrow A_{11-12} \rightarrow A_{12-13} \rightarrow A_{13-14} \rightarrow A_{14-15}$

Ткр = 5+9+12+12+12+10+5+5+4+4=78 с

Интенсивность:

$$\nu_2 = \frac{1}{Tкр}$$

$\nu_2 = \frac{1}{78} = 0{,}0129$ с$^{(-1)}$ $\approx 1{,}1 \cdot 103$ сут$^{-1}$.

Время выполнения всех работ: 70 работ в стуки. Для составления перечня работ, ведущих к образованию угрозы, выносим следующие предположения: система мониторинга системы спроектирована и смонтирована без ошибок. Критическое время/среднее время проявления проблемы - **8** часов. Устранение проблемы - **7** часов. Работа системы - 1 сутки (24 часа)

2.3. Оценивание показателя эффективности реализации управленческих решений.

Условие, при котором функционирование объекта является достоверным событием, соответствует значению показателя эффективности P_2=1. Однако в реальных условиях функционирования системы управления безопасностью базы данных наличие случайных факторов и возмущений приводит к доказуемо меньшим значениям показателя эффективности.

Эффективность - это свойство, которое характеризует степень достижения цели или степень реализации возможностей системы, заложенных в неё разработчиком, в рамках определенных ограничений, и оценивается определенным показателем.

Показателем эффективности разработанной модели управления безопасностью базы данных является вероятность реализации управленческих решений P_2, определяемая следующей аналитической зависимостью:

$$P_2 = f\left(\lambda, \nu_1, \nu_2, \nu_3, \zeta^+, \zeta^-\right),$$

где λ - есть величина , где $\left(\lambda = \frac{1}{\Delta t_{ПП}}\right)$ $\Delta t_{ПП}$ - среднее время проявление проблемы;

ν_1 - есть величина , где $\left(\nu_1 = \frac{1}{\Delta t_{ИП}}\right)$ $\Delta t_{ИП}$ - среднее время идентификации проблемы;

ν_2 - есть величина , где $\left(\nu_2 = \frac{1}{\Delta t_{НП}}\right)$ $\Delta t_{НП}$ - среднее время нейтрализации проблемы;

ν_3 - частота срыва нейтрализации проблемы ЛПР, по причине невозможности распознать ситуацию (показатель квалификации ЛПР);

ζ^+ - есть величина $\left(\zeta^+ = \frac{1}{T_Э}\right)$, где $T_Э$ - длительность решения задачи;

ζ^- - частота срыва плана;

P_2 - показатель эффективности реализации управленческих решений.

Исходные параметры.

Общее время управления - 12,5 часов в сутки.

Количество срывов - 1 шт в сутки

Количество задач - 70 шт в сутки

Среднее время проявления проблемы - 8 часов в сутки.

Среднее время идентификации проблем - 1 час в сутки

Среднее время нейтрализации проблем - 6 часов в сутки

$\lambda = \frac{1}{8} = 0{,}125$

$\nu_1 = \frac{1}{1} = 1$

$\nu_2 = \frac{1}{6} = 0{,}1667$

$\zeta^+ = \frac{1}{12{,}5} = 0{,}08;\ \zeta^- = \frac{2}{70} = 0{,}0286$

Зададим условие правильности функционирования процессов идентификации и нейтрализации угрозы:

$$\frac{\Delta t_{ип} + \Delta t_{нп}}{\Delta t_{пп}} < 1 \Rightarrow \frac{1+6}{8} = 0{,}875 < 1,$$

что подтверждает допустимость выбранных параметров.

Сценарная проверка влияния возмущений

Найдем вероятность выполнения задачи P_2 с учетом:

- частоты ν_3 ,которая характеризует частоту срыва нейтрализации проблемы ЛПР, по причине невозможности распознать ситуацию, что является основой показателя квалификации ЛПР;
- частоты ζ^- ,которая характеризует среднее количество срыва выполнения плана прохождения пользователей, что показывает успешность выполнения функционирования сайта.

1. Если $\nu_3 = \frac{\nu_1}{1000}$, ζ^- = 0,0143, то P_2 = 0,8516

$$P_1 = \frac{\nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_2 = \frac{\lambda \cdot \nu_1 \cdot \nu_2 + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \zeta^+ \cdot \nu_3}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_3 = \frac{\lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_4 = \frac{\lambda \cdot \nu_1 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

Подставив значения получим:

P_1 = 0,0596, P_2 = 0,8516, P_3 = 0,0444, P_4 = 0,0444.

Проверим: $P_1 + P_2 + P_3 + P_4$ = 0,0596 + 0,8516 + 0,0444 +0,0444 = 1

2. Если $\nu_3 = \frac{\nu_1}{100}$, ζ^- = 0,0143, то P_2 = 0,8514

$$P_1 = \frac{\nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_2 = \frac{\lambda \cdot \nu_1 \cdot \nu_2 + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \zeta^+ \cdot \nu_3}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_3 = \frac{\lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_4 = \frac{\lambda \cdot \nu_1 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

Подставив значения получим:

P_1 = 0,0614, P_2 = 0,8512, P_3 = 0,0439, P_4 = 0,0435.

Проверим: $P_1 + P_2 + P_3 + P_4 = 0{,}0614 + 0{,}8512 + 0{,}0439 + 0{,}0435 = 1$

3. Если $\nu_3 = \frac{\nu_1}{1000}$, $\zeta^- = \frac{2}{70} = 0{,}0285$, то $P_2 = 0{,}7415$

$$P_1 = \frac{\nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_2 = \frac{\lambda \cdot \nu_1 \cdot \nu_2 + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \zeta^+ \cdot \nu_3}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_3 = \frac{\lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

$$P_4 = \frac{\lambda \cdot \nu_1 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-}$$

Подставив значения получим:

$P_1 = 0{,}1037$, $P_2 = 0{,}7415$, $P_3 = 0{,}0774$, $P_4 = 0{,}0773$.

Проверим: $P_1 + P_2 + P_3 + P_4 = 0{,}1037 + 0{,}7415 + 0{,}0774 + 0{,}0773 = 1$

4. Если $\nu_3 = \frac{\nu_1}{100}$, $\zeta^- = \frac{2}{70} = 0{,}0285$, то $P_2 = 0{,}7409$

$$P_1 = \frac{\nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-} =$$

$$P_2 = \frac{\lambda \cdot \nu_1 \cdot \nu_2 + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \zeta^+ \cdot \nu_3}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-} =$$

$$P_3 = \frac{\lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-} =$$

$$P_4 = \frac{\lambda \cdot \nu_1 \cdot \zeta^-}{\lambda \cdot \nu_1 \cdot \nu_2 + \lambda \cdot \nu_1 \cdot \zeta^- + \lambda \cdot \nu_3 \cdot \zeta^- + \nu_1 \cdot \nu_2 \cdot \zeta^+ + \nu_1 \cdot \nu_2 \cdot \zeta^- + \nu_1 \cdot \zeta^+ \cdot \nu_3 + \nu_1 \cdot \nu_2 \cdot \zeta^-} =$$

Подставив значения получим:

$P1 = 0{,}1070$, $P2 = 0{,}7409$, $P3 = 0{,}0764$, $P4 = 0{,}0757$.

Проверим: $P1 + P2 + P3 + P4 = 0{,}1070 + 0{,}7409 + 0{,}0774 + 0{,}0757 = 1$

Разработка модели обеспечения безопасности базы данных на основе решения задачи при **заданной** вероятности реализации управленческих решений.

Разработка модели обеспечения безопасности базы данных на основе решения задачи при заданной вероятности реализации управленческих решений при управлении безопасностью БД P_2=0,8, при общем времени решения задачи ζ^+, при количестве срывов ζ^-, частоте срыва нейтрализации ЛПР ν_3=0,001 и заданной угрозе λ=0,125:

$$P_2 = 0{,}8$$

Так как при исходном числе срывов $N_{срыв}$= 2 получено $P_2 \approx 0{,}74 < 0{,}8$, в рамках решения обратной задачи принимаем управленческое решение снизить число срывов выполнения плана до $N_{срыв}$=1, то есть:

$$\zeta^- = \frac{1}{70} = 0{,}0143$$

Далее:

$$T_э = 12{,}5 \rightarrow \zeta^+ = \frac{1}{12{,}5} = 0{,}08$$

$$\Delta t_{пп} = 8 \rightarrow \lambda = \frac{1}{8} = 0{,}125$$

ν_3=0,001

$$P_2 = \frac{\lambda\nu_1\nu_2 + \lambda\nu_1\zeta^- + \lambda\nu_3\zeta^- + \nu_1\nu_2\zeta^+ + 2\nu_1\nu_2\zeta^- + \nu_1\zeta^+\nu_3 + \nu_1\nu_3\zeta^-}{\lambda\nu_1\nu_2 + \nu_1\nu_2\zeta^+ + \nu_1\zeta^+\nu_3} = 0{,}8$$

$$\nu_1 = 2 \rightarrow \Delta t_{ип} = \frac{1}{\nu 1} = \frac{1}{2} = 0{,}5$$

$$\nu_2 = 0{,}5 \rightarrow \Delta t_{ип} = \frac{1}{\nu 2} = \frac{1}{0{,}5} = 2$$

$$P_2 = f\left(\lambda, \nu_1, \nu_2, \nu_3, \zeta^+, \zeta^-\right)$$

$P_2 = f(0{,}125; 2; 0{,}5; 0{,}001; 0{,}057; 0{,}02)$

Следовательно, для обеспечения P_2 необходимо сократить длительности работ на критических путях процессов идентификации и нейтрализации угрозы.

1. При расчете графиков идентификации все данные уменьшаются в **2** раза:

Обозначение работ	**Время выполнения работ, с**	**Измененное время выполнения работ, с**
A_{0-1}	5	2,5
A_{1-2}	12	6
A_{1-3}	10	5
A_{1-4}	9	4,5
A_{2-5}	12	6
A_{3-6}	10	5
A_{4-7}	9	4,5
A_{5-8}	8	4
A_{6-9}	10	5
A_{7-10}	9	4,5
A_{8-11}	5	2,5
A_{9-11}	5	2,5
A_{10-11}	5	2,5
A_{11-12}	10	5
A_{12-13}	10	5
A_{13-14}	5	2,5
A_{14-15}	5	2,5

Таблица 12 - Изменение времени в перечне работ процесса идентификации угрозы.

2. При расчете графиков нейтрализации все данные уменьшаются в **3** раза:

Обозначение работ	**Время выполнения работ, с**	**Измененное время выполнения работ, с**
A_{0-1}	5	1,666
A_{1-2}	9	3
A_{1-3}	8	2,666
A_{1-4}	7	2,333
A_{2-5}	12	4
A_{3-6}	8	2,666
A_{4-7}	7	2,333
A_{5-8}	12	4
A_{6-9}	8	2,666
A_{7-10}	6	2
A_{8-11}	12	4
A_{9-11}	6	2
A_{10-11}	10	3,333
A_{11-12}	5	1,666
A_{12-13}	5	1,666
A_{13-14}	4	1,333
A_{14-15}	4	1,333

Таблица 13- Изменение времени в перечне работ процесса нейтрализации угрозы

Выводы по второй главе:

1. Для обеспечения безопасности базы данных в условиях деструктивных воздействий внешней и внутренней среды в работе был использован естественно-научный подход. В рамках данного подхода разработана аналитическая модель процесса управления безопасностью базы данных. Построенная модель позволила получить условие существования процесса обеспечения безопасности базы данных и формализовать процесс принятия управленческих решений.

Для обеспечения требуемого уровня безопасности базы данных необходимо осуществлять системную интеграцию следующих процессов:

- проявления угрозы безопасности;
- идентификации угрозы;
- нейтрализации угрозы;
- реализации управленческих решений по обеспечению безопасности базы данных.

Интеграция указанных процессов позволяет анализировать уровень безопасности базы данных, основанный на своевременной идентификации и устранении угроз.

2. Установлено, что обеспечение требуемого уровня безопасности базы данных возможно за счет:

- сокращения времени идентификации и нейтрализации угроз, в том числе за счет оптимизации критических путей соответствующих процессов;
- внедрения современных технических средств защиты информации и специализированного программного обеспечения;

- совершенствования организационных мер, включая регламентацию действий персонала и повышение уровня квалификации лиц, принимающих решения, в части обеспечения безопасности базы данных.

3. Система алгебраических уравнений позволила получить условие существования процесса обеспечения безопасности базы данных. На основе данного условия сформировано аналитическое уравнение, которое увязывает показатель эффективности реализации управленческих решений с характеристиками четырех основных процессов: проявления угрозы, идентификации угрозы, нейтрализации угрозы и функционирования системы управления безопасностью базы данных.

4. Показано, что условие существования процесса обеспечения безопасности базы данных формируется из временных характеристик деятельности по обеспечению безопасности. Установлено, что данные временные характеристики зависят от состояний четырех указанных процессов.

Для этого в работе решена задача увязывания временных характеристик процессов с их состояниями, перечнем работ, необходимых для достижения этих состояний, а также с временными ресурсами, затрачиваемыми на выполнение указанных работ. В качестве математического аппарата использованы сетевые модели, которые при расчете критических путей обеспечили количественное формирование элементов условия существования процесса обеспечения безопасности базы данных. Это, в свою очередь, позволило обосновать достижение требуемого уровня безопасности базы данных.

Разработанная аналитическая математическая модель управления безопасностью базы данных создала основу для дальнейшего проектирования и разработки технологии обеспечения безопасности базы данных, а также для обоснования управленческих решений, направленных на повышение устойчивости функционирования системы в условиях воздействия угроз.

ГЛАВА 3. РАЗРАБОТКА АЛГОРИТМИЧЕСКОГО АППАРАТА МОДЕЛИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ БАЗЫ ДАННЫХ.

3.1. Архитектура программного комплекса управления безопасностью базы данных.

В процессе разработки алгоритмического аппарата модели управления безопасностью базы данных, представленного во второй главе выпускной квалификационной работы, был реализован программный комплекс мониторинга и управления защитными мероприятиями, ориентированный на функционирование в среде СУБД MariaDB. Разработанная архитектура программного комплекса обеспечивает практическую реализацию алгоритмов мониторинга, анализа и планирования защитных мероприятий, тем самым осуществляя переход от теоретической модели к ее прикладному применению.

Архитектура программного комплекса построена по модульному принципу и включает в себя следующие основные компоненты:

- модуль мониторинга и идентификации угроз, реализованный в виде программного скрипта scanner.py;
- модуль планирования и управления заданиями мониторинга, реализованный в виде программного скрипта planner.py
- СУБД MariaDB, используемую в качестве централизованного хранилища данных;
- журнал событий безопасности, реализованный в виде совокупности реляционных таблиц базы данных.

Модули мониторинга и планирования взаимодействуют между собой через базу данных, что обеспечивает логическое разделение функций, устойчивость системы и возможность дальнейшего расширения программного комплекса без изменения его архитектуры. Обобщенная

архитектура программного комплекса управления безопасностью базы данных представлена на рисунке 7.

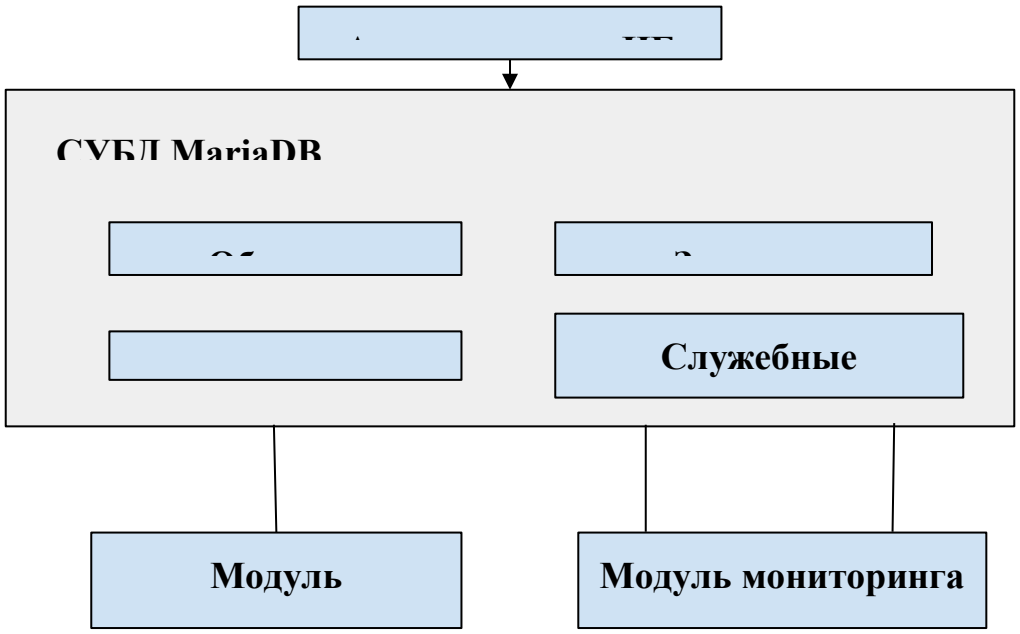

Рисунок 11 - Архитектура программного комплекса управления безопасностью базы данных

Взаимодействие компонентов осуществляется с использованием отдельной учетной записи базы данных, обладающей ограниченным набором прав доступа. Данный подход соответствует принципу минимально необходимых привилегий и снижает риск несанкционированного воздействия на данные базы данных со стороны программных модулей.

В качестве инструментальных средств реализации программного комплекса были выбраны язык программирования Python и система управления базами данных MariaDB.

Выбор языка Python обусловлен его универсальностью, высокой скоростью разработки и наличием развитой экосистемы библиотек для работы с сетевыми протоколами, многопоточностью и базами данных.

Использование Python позволило реализовать алгоритмы

мониторинга и планирования в виде независимых программных модулей, а также обеспечить наглядность и воспроизводимость логики функционирования системы, что особенно важно на этапе апробации модели управления безопасностью.

В качестве СУБД была выбрана MariaDB, что связано с её высокой производительностью, устойчивостью к нагрузкам и поддержкой развитых механизмов разграничения прав доступа. Использование MariaDB позволило реализовать централизованное хранилище данных для фиксации результатов мониторинга, заданий и событий нейтрализации угроз, а также обеспечить согласованность информации между функциональными модулями системы.

Совместное использование Python и MariaDB обеспечило практическую реализуемость разработанной модели управления безопасностью базы данных, а также возможность дальнейшего расширения системы без изменения её архитектурных принципов.

3.2. Проектирование и реализация функциональных модулей

3.2.1. Модуль мониторинга и идентификации угроз

Модуль мониторинга и идентификации угроз является ключевым компонентом программного комплекса, так как именно он обеспечивает получение первичной информации о состоянии сетевой инфраструктуры доступа к базе данных и формирование данных для последующего анализа.

Модуль реализован на языке Python и выполняет следующие основные функции:

- инициализацию процедуры мониторинга;
- активное сканирование заданного набора сетевых портов;
- выявление доступных сетевых сервисов;

- сбор дополнительной информации (в том числе HTTP-заголовков при наличии веб-сервисов);
- предварительную классификацию уровня потенциальной угрозы;
- фиксацию результатов мониторинга в базе данных.

Алгоритм работы модуля мониторинга реализует процесс идентификации угроз, описанный во второй главе, и включает следующие этапы:

1. Получение идентификатора объекта мониторинга и сетевого адреса;
2. Выполнение сетевого сканирования;
3. Анализ полученных данных;
4. Определение уровня угрозы;
5. Фиксацию временных характеристик идентификации угрозы.

Результаты мониторинга сохраняются в таблицу scan_results базы данных MariaDB. В таблице фиксируются моменты начала и окончания идентификации угрозы, что позволяет определить значение времени идентификации $\Delta t_{ип}$, используемое далее при расчёте показателя эффективности $P2$.

Алгоритм работы модуля мониторинга и идентификации угроз представлен на рисунке 12.

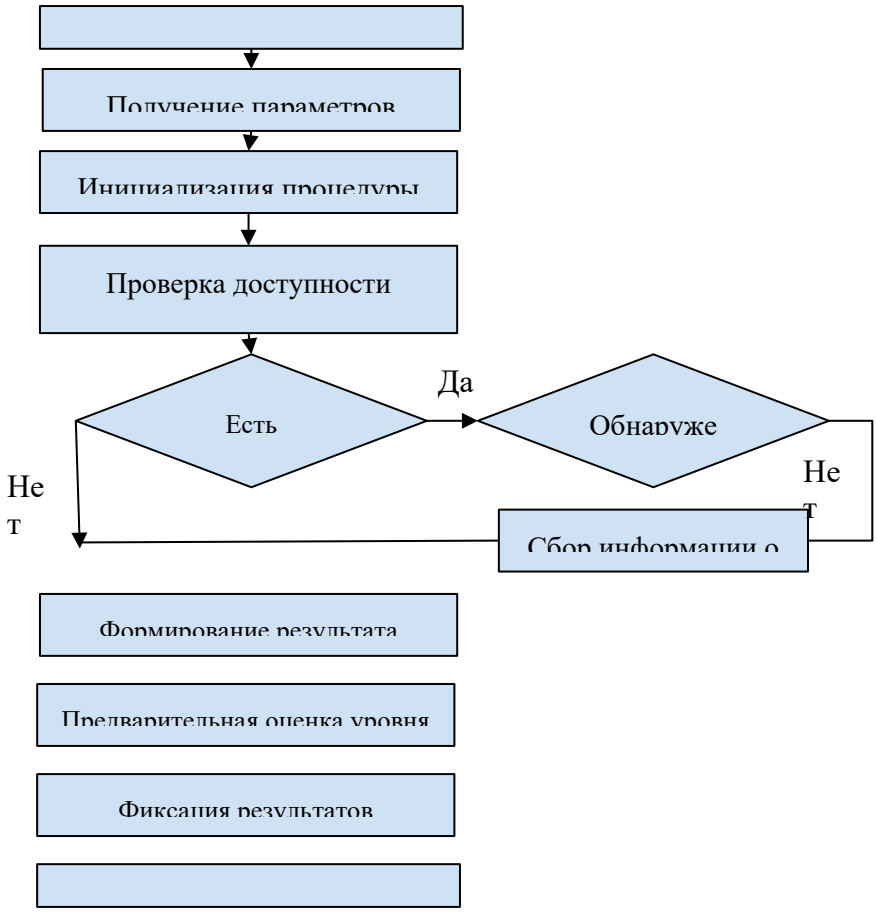

Рисунок 12 – Блок-схема алгоритма мониторинга и выявления угроз

Пример записи результатов мониторинга в базе данных представлен на рисунке 13.

scan_results (223r × 14c)

#	1 id	2 target_id	3 job_id	4 scan_time	5 scan_started_at	6 scan_finished_at	7 identify_started_at	8 identify_finished_at	9 t_identify_sec	10 open_ports_js...	11 http_headers_js...
1	1	1	(NULL)	2026-01-28 09:56:55	2026-01-28 09:56:50	2026-01-28 09:56:55	2026-01-28 09:56:55	2026-01-28 09:56:55	0,000011	[3306]	{}
2	2	1	(NULL)	2026-01-28 10:09:40	2026-01-28 10:09:35	2026-01-28 10:09:40	2026-01-28 10:09:40	2026-01-28 10:09:40	0,000011	[3306]	{}
3	3	1	(NULL)	2026-01-28 10:09:46	2026-01-28 10:09:41	2026-01-28 10:09:46	2026-01-28 10:09:46	2026-01-28 10:09:46	0,000011	[3306]	{}
4	4	1	(NULL)	2026-01-28 10:09:51	2026-01-28 10:09:46	2026-01-28 10:09:51	2026-01-28 10:09:51	2026-01-28 10:09:51	0,000003	[3306]	{}
5	5	1	(NULL)	2026-01-28 10:09:56	2026-01-28 10:09:51	2026-01-28 10:09:56	2026-01-28 10:09:56	2026-01-28 10:09:56	0,000009	[3306]	{}
6	6	1	(NULL)	2026-01-28 10:10:02	2026-01-28 10:09:57	2026-01-28 10:10:02	2026-01-28 10:10:02	2026-01-28 10:10:02	0,000006	[3306]	{}
7	7	1	(NULL)	2026-01-28 10:10:07	2026-01-28 10:10:02	2026-01-28 10:10:07	2026-01-28 10:10:07	2026-01-28 10:10:07	0,000008	[3306]	{}
8	8	1	(NULL)	2026-01-28 10:10:12	2026-01-28 10:10:07	2026-01-28 10:10:12	2026-01-28 10:10:12	2026-01-28 10:10:12	0,000011	[3306]	{}
9	9	1	(NULL)	2026-01-28 10:10:18	2026-01-28 10:10:12	2026-01-28 10:10:17	2026-01-28 10:10:17	2026-01-28 10:10:17	0,000008	[3306]	{}
10	10	1	(NULL)	2026-01-28 10:10:23	2026-01-28 10:10:18	2026-01-28 10:10:23	2026-01-28 10:10:23	2026-01-28 10:10:23	0,000011	[3306]	{}
11	11	1	(NULL)	2026-01-28 10:10:28	2026-01-28 10:10:23	2026-01-28 10:10:28	2026-01-28 10:10:28	2026-01-28 10:10:28	0,000012	[3306]	{}
12	12	1	(NULL)	2026-01-28 10:21:42	2026-01-28 10:21:37	2026-01-28 10:21:42	2026-01-28 10:21:42	2026-01-28 10:21:42	0,000029	[3306]	{}
13	13	2	(NULL)	2026-01-28 10:26:10	2026-01-28 10:26:03	2026-01-28 10:26:09	2026-01-28 10:26:09	2026-01-28 10:26:09	0,000009	[]	{}

Рисунок 13 - Запись результата мониторинга

3.2.2. Модуль планирования и управления заданиями мониторинга

Модуль планирования и управления заданиями предназначен для автоматизации запуска процедур мониторинга и координации работы системы в режиме непрерывного функционирования. Модуль реализован в виде программного скрипта planner.py.

Основными функциями модуля являются:

- формирование и обработка заданий мониторинга;
- определение условий запуска процедур сканирования;
- передача параметров в модуль мониторинга;
- контроль выполнения заданий;
- инициирование процедур нейтрализации угроз.

Модуль планирования использует информацию, хранящуюся в таблице scan_jobs, где задаются параметры периодичности мониторинга и состояния активности заданий. Использование идентификаторов заданий обеспечивает логическую связь между процессами мониторинга и результатами их выполнения.

Запуск процедур мониторинга осуществляется в асинхронном режиме, что позволяет выполнять несколько заданий без блокировки работы системы. Такой подход обеспечивает сокращение времени реакции системы и повышает эффективность управления безопасностью базы данных.

Пример хранения заданий мониторинга в базе данных представлен на рисунке 14.

scan_jobs (16r × 6c)

#	1 id	2 target_id	3 schedule_minutes	4 enabled	5 last_run	6 created_at
1	1	1	5	1	2026-01-28 12:36:42	2026-01-28 12:33:04
2	2	1	5	1	2026-01-28 12:36:42	2026-01-28 12:38:31
3	3	1	5	1	2026-01-28 12:36:42	2026-01-28 12:38:45
4	4	1	5	1	2026-01-28 12:36:42	2026-01-28 12:39:00
5	5	1	5	1	2026-01-28 12:36:42	2026-01-28 12:40:15
6	6	1	5	1	2026-01-28 12:36:42	2026-01-28 12:45:27
7	7	1	5	1	2026-01-28 12:36:42	2026-01-28 12:56:30
8	8	1	5	1	2026-01-28 12:36:42	2026-01-28 12:57:22
9	9	1	5	1	2026-01-28 12:36:42	2026-01-28 13:04:47
10	10	1	5	1	2026-01-28 12:36:42	2026-01-28 13:11:55
11	11	1	5	1	2026-01-28 12:36:42	2026-01-28 13:12:35
12	12	1	5	1	2026-01-28 12:36:42	2026-01-28 13:16:22
13	13	1	5	1	2026-01-28 12:36:42	2026-01-28 13:40:10
14	14	1	5	1	2026-01-28 12:36:42	2026-01-28 13:41:30

Рисунок 14 - Хранения заданий мониторинга в базе данных

Связь заданий мониторинга с результатами сканирования представлена на рисунке 15.

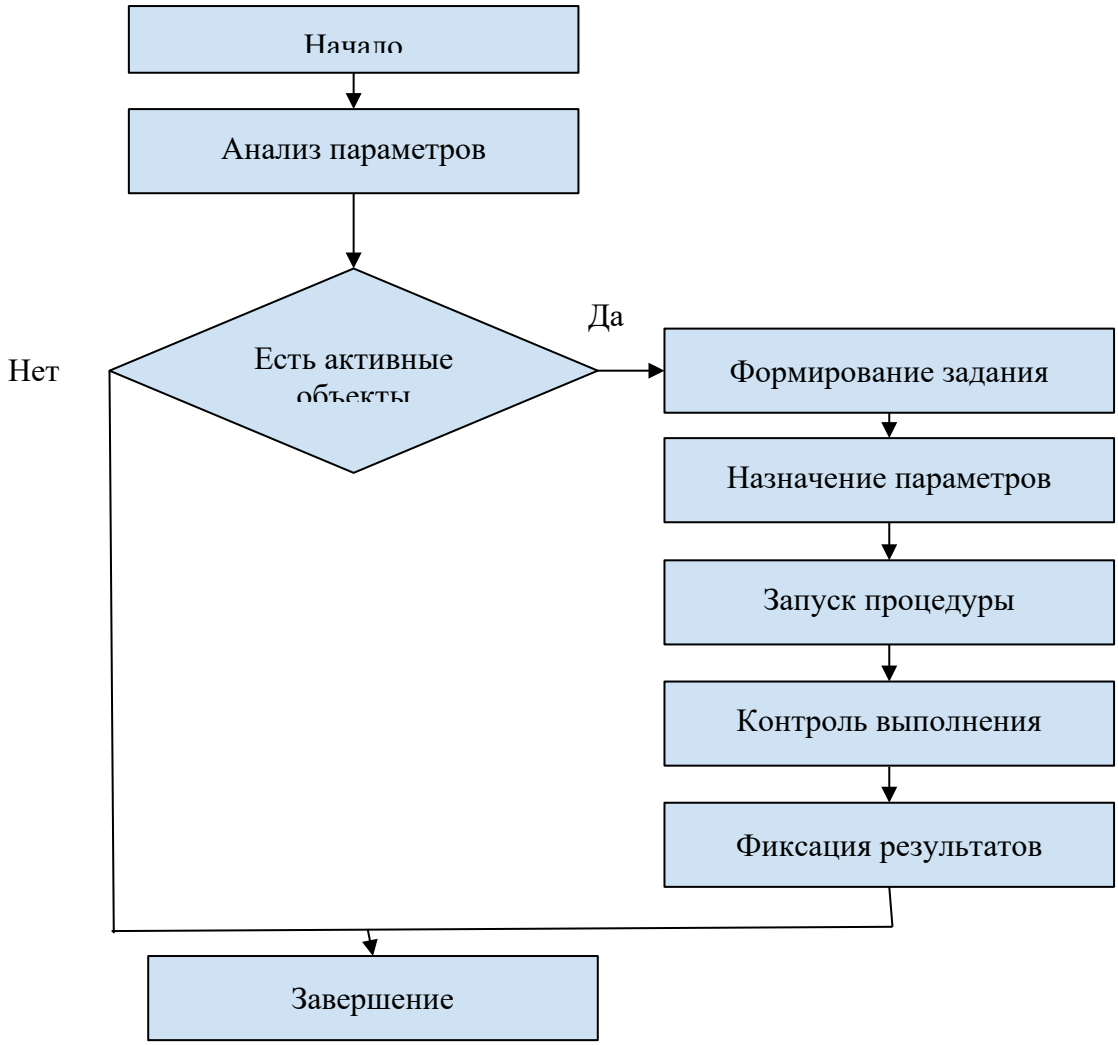

Рисунок 15– Схема взаимодействия модуля планирования и управления заданиями с компонентами системы

Модуль планирования реализует алгоритм управления заданиями, обеспечивающий переход от непрерывного мониторинга к управляемому циклу сканирования.

Таким образом, спроектированный модуль планирования и управления заданиями обеспечивает координацию процессов мониторинга, повышает управляемость системы и способствует реализации целостной модели управления безопасностью базы данных.

3.3. Реализация нейтрализации угроз и работа системы

В случае выявления потенциальной угрозы модуль планирования инициирует процесс нейтрализации. Информация о выполнении защитных мероприятий фиксируется в таблице **mitigations** базы данных.

В таблице записываются данные:

- момент начала нейтрализации угрозы;
- момент завершения нейтрализации;
- время нейтрализации Δt_нп;
- тип выполненного защитного действия;
- статус выполнения мероприятия.

Таким образом обеспечивается практическая реализация процесса перехода системы из состояния S4 (угроза идентифицирована) в состояние S2 (угроза нейтрализована), описанного во второй главе.

Пример записи данных о нейтрализации угрозы представлен на рисунке 16.

mitigations (226r × 11c)

#	1 id	2 target_id	3 scan_result_id	4 job_id	5 started_at	6 finished_at	7 t_neutralize_sec	8 action	9 comment	10 st...	11 created_at
1	1	1	11	(NULL)	2026-01-28 10:10:28	2026-01-28 10:10:31	3,950612	restrict_access	Ограничение доступа, аудит БД, по...	done	2026-01-28 13:10:28
2	2	1	12	(NULL)	2026-01-28 10:21:58	2026-01-28 10:22:01	3,689682	restrict_access	Ограничение доступа, аудит БД, по...	done	2026-01-28 13:21:58
3	3	1	31	4	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
4	4	1	31	3	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
5	5	1	31	13	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
6	6	1	29	11	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
7	7	1	31	5	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
8	8	1	31	15	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
9	9	1	31	10	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
10	10	1	29	1	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
11	11	1	31	2	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
12	12	1	31	14	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
13	13	1	31	12	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31
14	14	1	31	16	2026-01-28 11:07:25	2026-01-28 11:07:31	6	restrict_access	Ограничение доступа и аудит БД	done	2026-01-28 14:07:31

Рисунок 16 - Запись данных в таблице mitigations.

3.4. Оценка эффективности разработанной системы

Оценка эффективности разработанной системы управления безопасностью базы данных выполнена на основе аналитической модели,

представленной во второй главе выпускной квалификационной работы. В качестве основного критерия эффективности использовался показатель **P_2**, характеризующий качество управленческого решения за счёт временных характеристик процессов идентификации и нейтрализации угроз.

Таблица 14 – События процесса идентификации угрозы

Обозначение	**Наименование i-го события**	**Источник фиксации**
a_0	Запуск процедуры мониторинга объекта	planner.py
a_1	Начало сетевого сканирования	scanner.py
a_2	Обнаружение активных сетевых сервисов	scanner.py
a_3	Анализ результатов сканирования	scanner.py
a_4	Начало идентификации угрозы	scan_results
a_5	Завершение идентификации угрозы	scan_results

Таблица 15 - Работы процесса идентификации угрозы

Обозначение	**Наименование i-го события**	**Источник фиксации**
a_{0-1}	Инициация процедуры мониторинга	planner.py
a_{1-2}	Выполнение сетевого сканирования	scanner.py
a_{2-3}	Анализ полученных данных	scanner.py
a_{3-4}	Классификация уровня угрозы	scanner.py
a_{4-5}	Идентификация угрозы	scan_results

Таблица 16 - События процесса нейтрализации угрозы

Обозначение	Наименование i-го события	Источник фиксации
a_0	Угроза идентифицирована	scan_results
a_1	Инициация нейтрализации угрозы	planner.py
a_2	Выбор защитного воздействия	planner.py
a_3	Начало выполнения защитных мероприятий	mitigations
a_4	Завершение нейтрализации угрозы	mitigations
a_5	Возврат системы в штатное состояние	mitigations

Таблица 17 - События процесса нейтрализации угрозы

Обозначение	Наименование i-го события	Источник фиксации
a_{0-1}	Формирование решения реагирования	planner.py
a_{1-2}	Выбор стратегии нейтрализации	planner.py
a_{2-3}	Реализация защитных мероприятий	planner.py
a_{3-4}	Выбор стратегии нейтрализации	mitigations
a_{4-5}	Идентификация угрозы	mitigations

Таблица 18 - Используемые временные параметры для расчета эффективности

Параметр	Обозначение	Значение

Среднее время появления угрозы	$\Delta t_{\text{пп}}$	8ч
Среднее время идентификации угрозы	$\Delta t_{\text{ип}}$	4,6 с = 786,2 ч$^{(-1)}$
Среднее время нейтрализации угрозы	$\Delta t_{\text{нп}}$	6,8 с = 529,4 ч$^{(-1)}$
Частота срыва нейтрализации	ν_3	0,001
Время решения задачи	$T_э$	12,5 часов = 0,08 ч$^{(-1)}$

ν_1 = 0,217

ν_2 = 0,147

Для оценки возможности устойчивого функционирования системы управления безопасностью предварительно проверяется выполнение условия допустимости временных характеристик процессов идентификации и нейтрализации угроз. Условие имеет вид:

$$\frac{\Delta tип + \Delta tнп}{\Delta tпп} < 1$$

В ходе экспериментальной апробации программного комплекса были получены следующие значения временных параметров:

Δtип=4,6 с,Δtнп=6,8 с,Δtпп=8 ч.

Приведя значения к одной размерности и подставив в выражение, получаем:

$$\frac{4{,}6 + 6{,}8}{8 * 3600} = \frac{11{,}4}{28800} < 1$$

Таким образом, условие допустимости выполняется, что свидетельствует о возможности применения разработанной модели для оценки эффективности управленческих решений.

На данном этапе реализации решения $\mathbf{P_2 = 0{,}877.}$

Выводы по третьей главе:

В ходе третьей главы был разработан и реализован программный комплекс управления безопасностью базы данных, обеспечивающий автоматизированный мониторинг состояния сетевой инфраструктуры и выявление потенциальных угроз безопасности. Сформирована модульная архитектура системы, включающая модуль мониторинга и выявления угроз, модуль планирования и управления заданиями, а также централизованное хранилище данных на основе СУБД MariaDB. Реализованы алгоритмы активного сетевого сканирования, предварительной классификации уровня угроз и фиксации результатов мониторинга в базе данных.

Данные результаты были получены вследствие реализации алгоритмического аппарата модели управления безопасностью, разработанной во второй главе работы.

Использование модульного подхода и прямой интеграции функциональных компонентов с системой управления базами данных позволило обеспечить согласованность данных, устойчивость функционирования программного комплекса и возможность непрерывного мониторинга. Применение эвристических правил оценки уровня угрозы и формата JSON для хранения результатов мониторинга обеспечило гибкость алгоритмов и возможность их расширения без изменения структуры базы данных. Асинхронная организация выполнения заданий мониторинга

позволила оптимизировать временные характеристики процессов идентификации угроз, что соответствует требованиям к показателю эффективности управленческих решений P_2.

Полученные результаты могут быть использованы на практике для повышения уровня безопасности систем управления базами данных. Разработанный программный комплекс может применяться для мониторинга состояния сетевой инфраструктуры доступа к СУБД, выявления потенциально опасных конфигураций и анализа динамики изменения уровня угроз. Архитектурные и алгоритмические решения, реализованные в рамках работы, создают основу для дальнейшего развития системы, включая расширение перечня анализируемых параметров, внедрение механизмов автоматического реагирования на события безопасности и применение методов аналитической обработки данных в задачах управления информационной безопасностью.

ГЛАВА 4. РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ.

На основе разработанной аналитической модели управления безопасностью базы данных и результатов сценарного моделирования были сформированы предложения по совершенствованию системы обеспечения информационной безопасности систем с базами данных

Предлагаемые меры направлены на сокращение времени идентификации и нейтрализации угроз, снижение вероятности реализации уязвимостей и повышение значения показателя эффективности реализации управленческих решений P_2.

Реализация предложенных мероприятий позволяет повысить уровень защищенности базы данных, сократить временные характеристики процессов идентификации и нейтрализации угроз и обеспечить достижение заданного значения показателя эффективности реализации управленческих решений. Предлагаемые меры по обеспечению информационной безопасности базы данных представлены в таблице 16.

Таблица 16 - Предложения по совершенствованию системы обеспечения информационной безопасности базы данных

Уязвимый элемент / процесс	**Предложения по совершенствованию системы**
Аутентификация пользователей БД	● Использовать уникальные учетные записи для каждого пользователя СУБД ● Реализовать политику сложных паролей и их периодической смены ● Ограничить количество неуспешных попыток подключения

Авторизация и управление правами доступа	• Применять ролевую модель разграничения доступа (RBAC) • Регулярно проводить аудит назначенных ролей и привилегий • Удалять неактуальные и избыточные права доступа
Мониторинг и управление инцидентами	• Вести централизованный журнал событий СУБД • Автоматизировать сбор и анализ журналов безопасности • Защитить журналы от несанкционированного изменения
Защита серверной инфраструктуры БД	• Ограничить доступ к интерфейсам администрирования СУБД • Своевременно устанавливать обновления и патчи безопасности • Контролировать сетевой доступ к серверу базы данных
Обеспечение целостности и доступности данных	• Регулярно выполнять резервное копирование базы данных • Хранить резервные копии в защищённой среде • Проводить тестирование процедур восстановления
Криптографическая защита данных	• Использовать встроенные средства шифрования СУБД • Обеспечить защиту криптографических ключей • Применять защищённые каналы передачи данных

Реализация предложенных мероприятий позволяет повысить уровень защищенности базы данных, сократить временные характеристики процессов идентификации и нейтрализации угроз и обеспечить достижение заданного значения показателя эффективности реализации управленческих решений.

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе рассмотрена задача обеспечения информационной безопасности базы данных корпоративного уровня, функционирующей в условиях многопользовательского и сетевого доступа при наличии внутренних и внешних деструктивных воздействий. Актуальность исследования обусловлена ростом сложности архитектур информационных систем и увеличением числа угроз безопасности систем управления базами данных.

Целью работы являлась разработка модели и алгоритмического аппарата обеспечения безопасности базы данных на основе системной интеграции процессов целевого функционирования, образования угроз, их идентификации и нейтрализации. Для достижения поставленной цели были решены задачи анализа угроз и уязвимостей, выбора методологии моделирования, построения аналитической модели управления безопасностью, разработки алгоритмического аппарата и формирования практических рекомендаций.

В первой главе выполнен анализ архитектуры систем баз данных и актуальных угроз информационной безопасности. Показано, что существующие методологии и модели ориентированы преимущественно на качественное описание процессов или решение прямой задачи оценки защищенности, что обосновало необходимость выбора методологии, ориентированной на решение обратной задачи проектирования системы обеспечения безопасности.

Во второй главе на основе естественно-научного подхода разработана аналитическая математическая модель управления безопасностью базы данных, основанная на системной интеграции процессов функционирования, образования угроз, их идентификации и нейтрализации. С использованием сетевых моделей определены временные

характеристики процессов, критические пути и интенсивности, а также выполнено оценивание показателя эффективности реализации управленческих решений P_2.

В третьей главе разработан и реализован алгоритмический аппарат модели управления безопасностью базы данных. Создан программный комплекс мониторинга и управления защитными мероприятиями, проведена его экспериментальная апробация, подтвердившая корректность функционирования алгоритмов и соответствие реализованных процессов аналитической модели.

В четвертой главе сформулированы рекомендации по совершенствованию системы обеспечения информационной безопасности базы данных, направленные на сокращение времени идентификации и нейтрализации угроз и повышение значения показателя эффективности P_2. Реализация предложенных мер позволяет обеспечить требуемый уровень защищенности и повысить устойчивость функционирования системы в условиях деструктивного воздействия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Мамедли Р. Э. Базы данных [Электронный ресурс] // Официальный сайт Северного (Арктического) федерального университета имени М. В. Ломоносова. – URL: https://nvsu.ru/ru/Intellekt/2316/Mamedli_R.EH._Bazy_dannykh.pdf (дата обращения: 31.08.2025).
2. Актуальные киберугрозы: IV квартал 2024 года и I квартал 2025 года [Электронный ресурс] / Positive Technologies. – URL:https://ptsecurity.com/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 05.09.2025).
3. Kaspersky Managed Detection and Response Report 2024 [Электронный ресурс] / Securelist (Лаборатория Касперского). – URL:https://securelist.com/kaspersky-managed-detection-and-response-report-2024/115635/ (дата обращения: 06.09.2025).
4. IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs [Электронный ресурс]. – IBM Newsroom, 30 July 2024. – URL: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs (дата обращения: 09.09.2025).
5. DDoS threat report for 2024 Q4 [Электронный ресурс] / Cloudflare Radar. – San Francisco: Cloudflare, 2025. – URL: https://radar.cloudflare.com/reports/ddos-2024-q4 (дата обращения: 10.09.2025).
6. Обзор и анализ методов обеспечения безопасности в различных СУБД [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/obzor-i-analiz-metodov-obespecheniya-bezopasnosti-v-razlichnyh-subd (дата обращения: 11.11.2025).

7. Применение системы показателей для совершенствования процесса управления поддержкой пользователей на основе методологии COBIT [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/primenenie-sistemy-pokazateley-dlya-sovershenstvovaniya-protsessa-upravleniya-podderzhkoy-polzovateley-na-osnove-metodologii-cobit (дата обращения: 15.11.2025).
8. Дешко И. П. Управление IT-услугами по ITIL 4 : учеб. пособие [Электронный ресурс]. – URL: https://www.litres.ru/book/igor-petrovich-deshk/upravlenie-it-uslugami-po-itil-4-uchebnoe-posobie-dly-69544897/ (дата обращения: 01.12.2025).
9. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary [Электронный ресурс]. – URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2018.pdf (дата обращения: 07.12.2025).
10. Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России) [Электронный ресурс]. – URL: https://fstec.ru/ (дата обращения: 15.12.2025).
11. Учебно-методические материалы по защите информации [Электронный ресурс]. – URL: https://www.vavilovsar.ru/files/pages/26368/14702169075.pdf (дата обращения: 28.12.2025).
12. Рабочая программа дисциплины «Защита информации в информационных системах» [Электронный ресурс]. – URL: https://bgu.ru/repository/edu/mag/2024/09.04.03/progs/РП_Защита%20информации%20в%20информационных%20системах_МИС-24.pdf (дата обращения: 12.01.2026).

13. ГОСТ Р 50739–95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие требования. – М.: Госстандарт России, 1995.
14. Оценивание эффективности принятия управленческих решений в социально-экономических системах [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/otsenivanie-effektivnosti-prinyatiya-upravlencheskih-resheniy-v-sotsialno-ekonomicheskih-sistemah-na-primere-uchebnogo-zavedeniya (дата обращения: 14.01.2026).
15. Управление безопасностью объекта техносферы на основе закона сохранения целостности объекта [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/upravlenie-bezopasnostyu-obekta-tehnosfery-na-osnove-zakona-sohraneniya-tselostnosti-obekta (дата обращения: 15.01.2026).
16. Бурлов В. Г., Попов Н. Н., Гарсия Эскалона Х. А. Управление процессом применения космической геоинформационной системы в интересах обеспечения экологической безопасности региона [Электронный ресурс]. — URL: https://rshu.ru/university/notes/archive/issue50/UZ-50-el-118-129.pdf (дата обращения: 16.01.2026).

Приложение 1 - Исходный код сканера

```
# scanner.py
import sys
import json
import time
import socket
import logging
from datetime import datetime, timezone
import mysql.connector
import http.client

DB_CONFIG = {
    "host": "127.0.0.1",
    "user": "scanner_user",
    "password": "scanner_pass",
    "database": "security_monitor",
    "port": 3306,
}

logging.basicConfig(level=logging.INFO,                format='[%(asctime)s]
%(levelname)s: %(message)s')

DEFAULT_PORTS = [22, 80, 443, 3306, 5432, 8080]

def utcnow_naive():

    return datetime.now(timezone.utc).replace(tzinfo=None, microsecond=0)
```

```
def db_conn():
    return mysql.connector.connect(**DB_CONFIG)

def simple_port_scan(host, ports=DEFAULT_PORTS):
    open_ports = []
    for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(1.0)
        try:
            s.connect((host, port))
            open_ports.append(port)
        except Exception:
            pass
        finally:
            s.close()
    return open_ports

def fetch_http_headers(host):
    try:
        conn = http.client.HTTPConnection(host, timeout=3)
        conn.request("HEAD", "/")
        resp = conn.getresponse()
        headers = dict(resp.getheaders())
        conn.close()
        return headers
    except Exception as e:
        return {"error": str(e)}
```

```
def calculate_severity(open_ports):
    # как у тебя: наличие 3306 -> warning
    if 3306 in open_ports:
        return "warning"
    if open_ports:
        return "low"
    return "info"

def save_scan_result(target_id, job_id, scan_started_at, scan_finished_at,
                     identify_started_at, identify_finished_at, t_identify_sec,
                     open_ports, http_headers, severity):

    result_obj = {
        "host": None,  # можно не заполнять, у тебя host хранится в targets
        "open_ports": open_ports,
        "http_headers": http_headers,
        "severity": severity,
    }

    conn = db_conn()
    cur = conn.cursor()

    scan_time = utcnow_naive()
    cur.execute("""
        INSERT INTO scan_results (
            target_id,
            job_id,
            scan_time,
            scan_started_at,
```

```
        scan_finished_at,
        identify_started_at,
        identify_finished_at,
        t_identify_sec,
        open_ports_json,
        http_headers_json,
        result_json,
        severity
    )
    VALUES (%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s)
""", (
    target_id,
    job_id,
    scan_time,
    scan_started_at,
    scan_finished_at,
    identify_started_at,
    identify_finished_at,
    t_identify_sec,
    json.dumps(open_ports),
    json.dumps(http_headers),
    json.dumps(result_obj, ensure_ascii=False),
    severity
))

conn.commit()
cur.close()
conn.close()
```

```
def run_scan(target_id, host, job_id=None, identify_delay_sec=4):
    logging.info("Start scan host=%s target_id=%s job_id=%s", host, target_id,
job_id)

    scan_started_at = utcnow_naive()

    open_ports = simple_port_scan(host)

    http_headers = {}
    if any(p in open_ports for p in (80, 443, 8080)):
        http_headers = fetch_http_headers(host)

    scan_finished_at = utcnow_naive()

    # --- Идентификация угрозы (моделирование времени анализа) ---
    identify_started_at = utcnow_naive()
    time.sleep(float(identify_delay_sec))  # <-- Δтип = 4 секунды
    severity = calculate_severity(open_ports)
    identify_finished_at = utcnow_naive()

    t_identify_sec = (identify_finished_at - identify_started_at).total_seconds()

    save_scan_result(
        target_id=target_id,
        job_id=job_id,
        scan_started_at=scan_started_at,
        scan_finished_at=scan_finished_at,
        identify_started_at=identify_started_at,
        identify_finished_at=identify_finished_at,
```

```
        t_identify_sec=t_identify_sec,
        open_ports=open_ports,
        http_headers=http_headers,
        severity=severity
    )

    logging.info("Done host=%s severity=%s t_identify_sec=%.2f", host, severity, t_identify_sec)
    return severity

if __name__ == "__main__":
    if len(sys.argv) < 3:
        print("Usage: python scanner.py <target_id> <host> [job_id]")
        sys.exit(1)

    target_id = int(sys.argv[1])
    host = sys.argv[2]
    job_id = int(sys.argv[3]) if len(sys.argv) >= 4 else None

    run_scan(target_id, host, job_id=job_id)
```

Приложение 2 - Исходный код планировщика

```
# scanner.py
import sys
```

```
import json
import time
import socket
import logging
from datetime import datetime, timezone
import mysql.connector
import http.client

DB_CONFIG = {
    "host": "127.0.0.1",
    "user": "scanner_user",
    "password": "scanner_pass",
    "database": "security_monitor",
    "port": 3306,
}

logging.basicConfig(level=logging.INFO, format='[%(asctime)s]
%(levelname)s: %(message)s')

DEFAULT_PORTS = [22, 80, 443, 3306, 5432, 8080]

def utcnow_naive():
    # Python 3.13: utcnow() deprecated \
    return datetime.now(timezone.utc).replace(tzinfo=None, microsecond=0)

def db_conn():
    return mysql.connector.connect(**DB_CONFIG)

def simple_port_scan(host, ports=DEFAULT_PORTS):
```

```
    open_ports = []
    for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(1.0)
        try:
            s.connect((host, port))
            open_ports.append(port)
        except Exception:
            pass
        finally:
            s.close()
    return open_ports

def fetch_http_headers(host):
    try:
        conn = http.client.HTTPConnection(host, timeout=3)
        conn.request("HEAD", "/")
        resp = conn.getresponse()
        headers = dict(resp.getheaders())
        conn.close()
        return headers
    except Exception as e:
        return {"error": str(e)}

def calculate_severity(open_ports):

    if 3306 in open_ports:
        return "warning"
    if open_ports:
```

```
        return "low"
    return "info"

def save_scan_result(target_id, job_id, scan_started_at, scan_finished_at,
                     identify_started_at, identify_finished_at, t_identify_sec,
                     open_ports, http_headers, severity):

    result_obj = {
        "host": None,  # можно не заполнять, у тебя host хранится в targets
        "open_ports": open_ports,
        "http_headers": http_headers,
        "severity": severity,
    }

    conn = db_conn()
    cur = conn.cursor()

    # ВАЖНО: scan_time есть в таблице и по умолчанию current_timestamp(),
    # поэтому его можно не вставлять. Но чтобы было одинаково и наглядно
— вставим явно.
    scan_time = utcnow_naive()

    cur.execute("""
        INSERT INTO scan_results (
            target_id,
            job_id,
            scan_time,
            scan_started_at,
            scan_finished_at,
```

```
            identify_started_at,
            identify_finished_at,
            t_identify_sec,
            open_ports_json,
            http_headers_json,
            result_json,
            severity
        )
        VALUES (%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s)
    """, (
        target_id,
        job_id,
        scan_time,
        scan_started_at,
        scan_finished_at,
        identify_started_at,
        identify_finished_at,
        t_identify_sec,
        json.dumps(open_ports),
        json.dumps(http_headers),
        json.dumps(result_obj, ensure_ascii=False),
        severity
    ))

    conn.commit()
    cur.close()
    conn.close()

def run_scan(target_id, host, job_id=None, identify_delay_sec=4):
```

```
    logging.info("Start scan host=%s target_id=%s job_id=%s", host, target_id, job_id)

    scan_started_at = utcnow_naive()

    open_ports = simple_port_scan(host)

    http_headers = {}
    if any(p in open_ports for p in (80, 443, 8080)):
        http_headers = fetch_http_headers(host)

    scan_finished_at = utcnow_naive()

    # --- Идентификация угрозы (моделирование времени анализа) ---
    identify_started_at = utcnow_naive()
    time.sleep(float(identify_delay_sec))  # <-- Δтип = 4 секунды
    severity = calculate_severity(open_ports)
    identify_finished_at = utcnow_naive()

    t_identify_sec = (identify_finished_at - identify_started_at).total_seconds()

    save_scan_result(
        target_id=target_id,
        job_id=job_id,
        scan_started_at=scan_started_at,
        scan_finished_at=scan_finished_at,
        identify_started_at=identify_started_at,
        identify_finished_at=identify_finished_at,
        t_identify_sec=t_identify_sec,
```

```
        open_ports=open_ports,
        http_headers=http_headers,
        severity=severity
    )

    logging.info("Done host=%s severity=%s t_identify_sec=%.2f", host, severity, t_identify_sec)
    return severity

if __name__ == "__main__":
    if len(sys.argv) < 3:
        print("Usage: python scanner.py <target_id> <host> [job_id]")
        sys.exit(1)

    target_id = int(sys.argv[1])
    host = sys.argv[2]
    job_id = int(sys.argv[3]) if len(sys.argv) >= 4 else None

    run_scan(target_id, host, job_id=job_id)
```