DOI 10.37882/2223-2966.2024.7.19

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ БАЗ ДАННЫХ ОТ КИБЕРАТАК

INFORMATION TECHNOLOGIES FOR PROTECTING DATABASES FROM CYBER ATTACKS

A. Kolesnikov

Summary. The article touches upon the topic related to the challenges relevant in today's digital world, which relate to the protection of databases from cyberattacks. Within the framework of the ongoing research, a comparison of the use of traditional approaches to database protection and cloud technologies is carried out. The complex of information technologies Eclipsys offered by Oracle Corporation for database protection is also described in detail. Special attention is paid to such progressive solutions as digital signatures, non-interactive knowledge argument and federated processing.

Keywords: database, defense, cyberattack, technology, cipher.

Колесников Антон Александрович
Санкт-Петербургский Политехнический университет Петра Великого
anton.kolesnikov.science@mail.ru

Аннотация. В статье затрагивается тема, связанная с актуальными для современного цифрового мира задачами, которые касаются защиты баз данных от кибератак. В рамках исследования проведено сравнение использования традиционных подходов к защите баз данных и облачных технологий. Также детально описан комплекс информационных технологий Eclipsys, предложенных корпорацией Oracle, для защиты баз данных. Отдельное внимание уделено таким прогрессивным решениям как цифровые подписи, неинтерактивный аргумент знания и федеративная обработка.

Ключевые слова: база данных, защита, кибератака, технология, шифр.

В 2023 г. произошли большие изменения, которые существенным образом повлияли на ландшафт кибербезопасности на фоне глобальных конфликтов, экономической нестабильности и появления революционных генеративных инструментов искусственного интеллекта. Год был отмечен быстро меняющейся средой и серьезными атаками на крупные корпорации и правительства по всему миру. Согласно прогнозам программы-вымогатели останутся одной из основных угроз в 2024 г., а с появлением новых инструментов и тактик можно только наблюдать рост их масштабов и сложности [1]. Семейства вредоносных программ все чаще сотрудничают на подпольных форумах, а тактика социальной инженерии становится все более изощренной и направлена на частных лиц и компании с целью компрометации устройств и личной информации.

В 2022 году организации во всем мире потеряли 2,7 миллиарда долларов из-за киберпреступности. При этом частота и стоимость утечек данных растут стабильными темпами. Однако на фоне того, что различные информационные системы и коммуникационные сети, Интернет вещей и системы промышленного управления подвергаются массированным атакам, особого внимания заслуживает уязвимость баз данных. Согласно отчету Flashpoint «Обзор года за 2022 год», в период с января по декабрь было скомпрометировано около 39 миллиардов записей [2]. В таблице 1 представлена статистика десяти крупнейших утечек данных в 2023 году в мире.

Приведенные выше данные, безусловно, впечатляют, однако они также ясно показывают необходимость принятия эффективных действий по обеспечению целостности баз данных. При этом необходимо отметить, что подходы к защите базы данных от кибератак, несколько отличаются от способов поддержки безопасности сети. Первые включают в себя физические меры, программные решения и даже обучение сотрудников. Однако, в данном перечне мер особого внимания заслуживают прогрессивные информационные технологии, которые позволяют не только защитить содержание базы, но и обеспечить безопасность самой системы управления данными, а также каждого приложения, которое обращается к ней, от неправильного использования, повреждения и вторжения.

Таким образом, научно-практическая значимость отмеченных выше вопросов предопределила выбор темы данной статьи.

Анализ источников, показывает, что проблемам защиты баз данных от кибератак на сегодняшний день уделяется очень большое внимание. Во многих отечественных и зарубежных публикациях освещается вопрос киберзащиты баз данных, конкретизируется сложность технологий обеспечения их безопасности. В частности, в данном направлении работают Кузьминых Е.С., Маслова М.А., Новоселов А.В., Шахтанов С.В., Asmaa Sallam, Daren Fadolalkarim, Elisa Bertino.

Таблица 1.

Десять случаев утечки данных в 2023 году. [3]

Название организации	Сектор	Местонахождение	Известные нарушенные записи	Месяц публичного раскрытия информации
DarkBeam	Кибербезопасность	Великобритания	>3,800,000,000	Сентябрь
Real Estate Wealth Network	Строительство/недвижимость	США	1,523,776,691	Декабрь
Indian Council of Medical Research (ICMR)	Здравоохранение	Индия	815,000,000	Октябрь
Kid Security	ИТ-услуги/программное обеспечение	Казахстан	>300,000,000	Ноябрь
Twitter (X)	ИТ-услуги/программное обеспечение	США	>220,000,000	Январь
TuneFab	ИТ-услуги/программное обеспечение	Гонконг	>151,000,000	Декабрь
Dori Media Group	Медиа	Израиль	>100 ТВ[1]	Декабрь
Tigo	Телекоммуникации	Гонконг	>100,000,000	Июль
SAP SE Bulgaria	ИТ-услуги/программное обеспечение	Болгария	95,592,696	Ноябрь
Luxottica Group	Производство	Италия	70,000,000	Май

Обзор наиболее значимых уязвимостей, которые могут возникнуть при работе с современными базами данными в Интернете, представлен в трудах Громова Ю.Ю., Карасева П.И., Ефанова М.С., Серебряковой Т.А., Щепиловой Н.И., Masayuki Kato, Kiyohito Tanaka, Mitsuhiro Kida, Shomei Ryozawa.

Отдельное внимание вопросам защиты баз данных с точки зрения безопасности разрабатываемых приложений, которые подключаются к ним, уделяется Антошкиным К.В., Беньяшом Ю.Л., Родионовым И.Н., Бильчуком М.В., Dac-Nhuong Le, Souvik Pal, Prasant Kumar Pattnaik.

В тоже время, следует отметить, что не все ключевые аспекты в рассматриваемой предметной плоскости нашли свое полное отражение в публикациях современных авторов. В более глубокой проработке нуждаются рекомендации по администрированию баз данных, которые помогут защитить информацию и предотвратить дорогостоящие нарушения. Также уточнения и более четкой формализации требуют основные недостатки и узкие места существующих современных программных решений, которые используются для защиты базы данных от кибератак.

Таким образом, цель статьи заключается в проведении анализа современных информационных технологий защиты баз данных от кибератак.

Безопасность баз данных — это процессы, инструменты и средства управления, которые призваны поддерживать сохранность и защиту информации, хранящейся в базе, от случайных и преднамеренных угроз. Безопасность базы данных в киберпространстве должна гарантировать защиту: информации, заявок в базе данных, системы управления базами данных; виртуального сервера, аппаратного обеспечения базы данных, сетевой инфраструктуры, обеспечивающей доступ к базе [5].

Чтобы ответить на вопрос какие технологии необходимы для защиты базы данных, важно признать, что существует несколько источников рисков и угроз, в их число входят: человеческие ошибки, чрезмерные привилегии сотрудников, хакеры и инсайдеры, вредоносные программы, воздействия резервных носителей, повреждение серверов баз данных и уязвимых баз данных, таких как базы данных без исправлений или базы данных со слишком большим объемом данных в буферах.

Также представляется целесообразным обозначить требования, выдвигаемые к информационным технологиям, которые могут использоваться для защиты баз данных от кибератак.

1. Обнаружение. Для зашиты базы данных в киберпространстве необходим инструмент, который может сканировать и классифицировать уязвимости во всех базах данных, независимо от того, размещены ли они в облаке или на локальном компьютере, и предлагать рекомендации по устранению выявленных уязвимостей. Возможность обнаружения уязвимостей часто требуется для соблюдения нормативных требований.
2. Мониторинг активности данных. Решение должно обеспечивать мониторинг и аудит всех действий с данными во всех базах данных, независимо от того, где они развернуты — в локальной сети, в облаке или в контейнере. Информационная технология должна предупреждать о подозри-

[1] Для случаев, когда известен только размер файла с нарушенными данными, используется формула 1 МБ = 1 запись

тельных действиях в режиме реального времени, чтобы имелась возможность как можно скорее реагировать на угрозы. Кроме того, необходимым является решение, способное обеспечить соблюдение правил, политик и разделение обязанностей, а также предоставляющее возможность отслеживать состояние данных с помощью комплексного и унифицированного пользовательского интерфейса.

3. Возможности шифрования и токенизации. В случае утечки данных технологии шифрования обеспечат последнюю линию защиты от компрометации. Выбранный инструмент должен обладать гибкими возможностями шифрования, способными защитить данные в локальных, облачных, гибридных или мультиоблачных средах. Наиболее полезным является инструмент с возможностями шифрования файлов, томов и приложений, которые соответствуют требованиям отрасли, что может потребовать токенизации (маскировки данных) или расширенных возможностей управления ключами безопасности.
4. Оптимизация безопасности данных и анализ рисков. В данном случае речь идет об информационной технологии, способной генерировать контекстуальную информацию, объединяя сведения о безопасности данных с расширенной аналитикой, что позволит без проблем выполнять оптимизацию, анализ рисков и создавать отчеты. Наиболее эффективным является решение, способное сохранять и обобщать большие объемы исторических и актуальных данных о состоянии и безопасности базы, а также предлагающее возможности исследования данных, аудита и создания отчетов с помощью комплексной, но удобной панели самообслуживания.

Рассматривая более детально информационные технологии, которые могут быть использованы для защиты базы данных, прежде всего, представляется целесообразным сделать акцент на том, что их состав и требуемый функционал будет зависеть от платформы базы данных. Например, если пользователь использует локальное решение, то ему необходимы такие технологии, которые позволят обеспечить все — от защиты конечных точек до физической безопасности оборудования, что является непростой задачей. Если же привлекается поставщик облачных вычислений на базе платформы как услуги (PaaS), тогда перечень необходимых информационных технологий значительно сокращается.

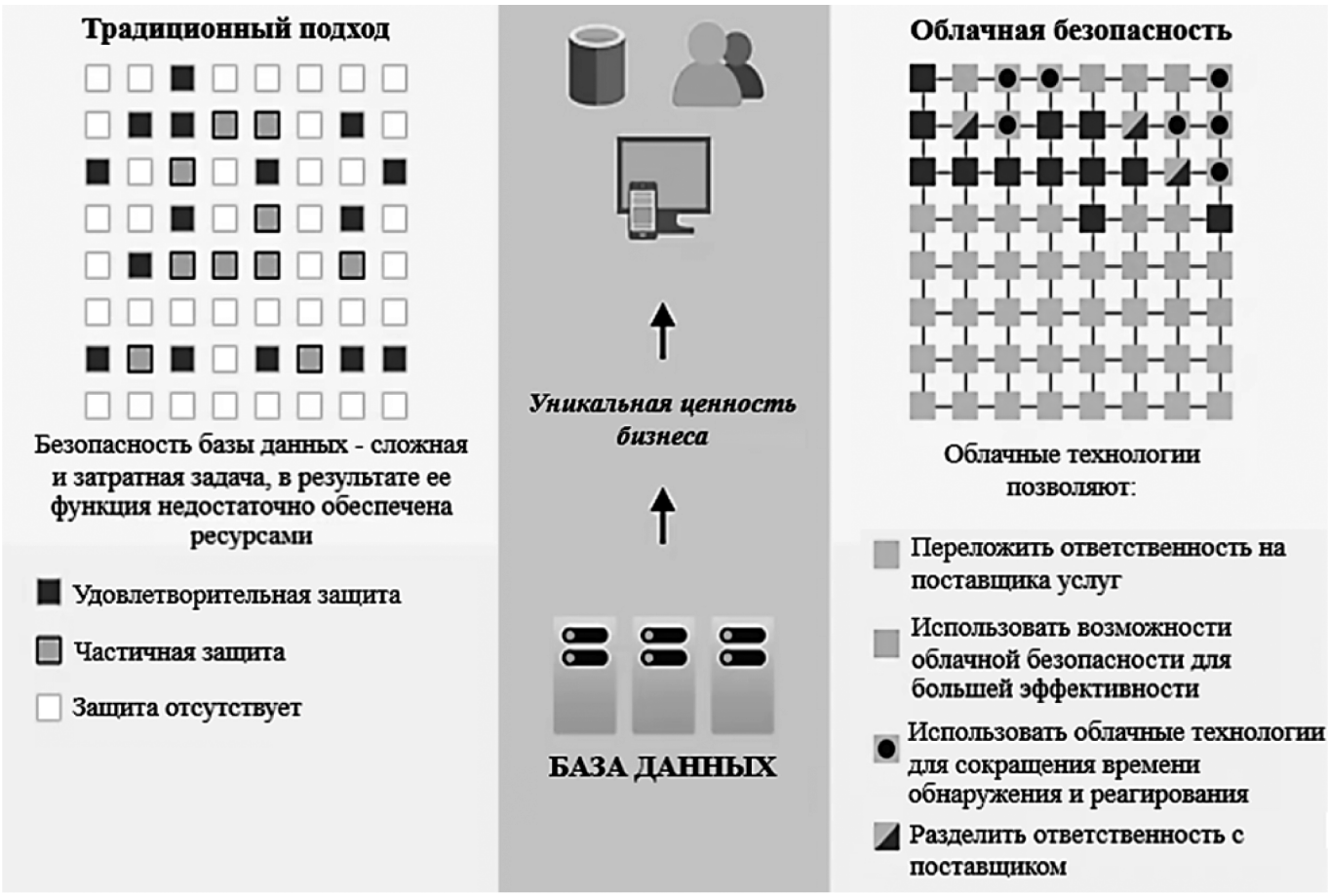

Рис. 1. Сравнение традиционного подхода и облачных технологий к обеспечению защиты баз данных от кибератак

Облачные технологии хранения информации предлагают значительные преимущества для решения проблем безопасности баз данных от киберугроз. В локальном окружении у компаний, в большинстве своем, есть невыполненные обязанности и ограниченные ресурсы для инвестиций в прогрессивные информационные технологии, обеспечивающие безопасность, что создает среду, в которой злоумышленники могут использовать уязвимости на всех уровнях [6]. На рис. 1 показан традиционный подход, для которого характерным является широкий перечень уязвимых мест в системе защиты базы данных, образовавшихся в результате ограниченности ресурсов. При использовании облачных технологий ряд задач по обеспечению безопасности базы делегируется облачному провайдеру, в результате чего формируется более расширенный и надежный защитный контур.

На рис. 2 представлен пример использования информационных технологий Eclipsys от компании Oracle для защиты базы данных от кибератак.

Рассмотрим более подробно возможности технологий Eclipsys

Аудит/оценка безопасности базы данных. Технологии позволяют проводить аудит требований безопасности в соответствии с текущей средой и спецификой развертывания базы данных, чтобы предоставить пользователю отчет, в котором определяются уязвимые области и проблемы соответствия. На основании этого разрабатываются рекомендации по улучшению инфраструктуры и устранению выявленных узких мест.

Исправления базы данных и веб-логика. Базы данных могут подвергаться дополнительному риску, поскольку не применены к системам последние обновления безопасности. Технологии дают возможность оценить актуальность набора исправления в инфраструктуре, а также спланировать и выполнить необходимые загрузки.

Развертывание продуктов безопасности баз данных.

Eclipsys может повысить безопасность базы данных внедрив следующие передовые продукты:

— расширенная безопасность/шифрование данных (TDE) — позволяет защитить хранящие данные путем их шифрования;
— аудит хранилища — предоставляет платформу для мониторинга и аудита корпоративной безопасности, а также определяет ее соответствие принятым стандартам;
— брандмауэр базы данных — создает внутренний защитный периметр, который отслеживает и обеспечивает безаварийное функционирование приложений, помогая предотвратить SQL-инъекцию,

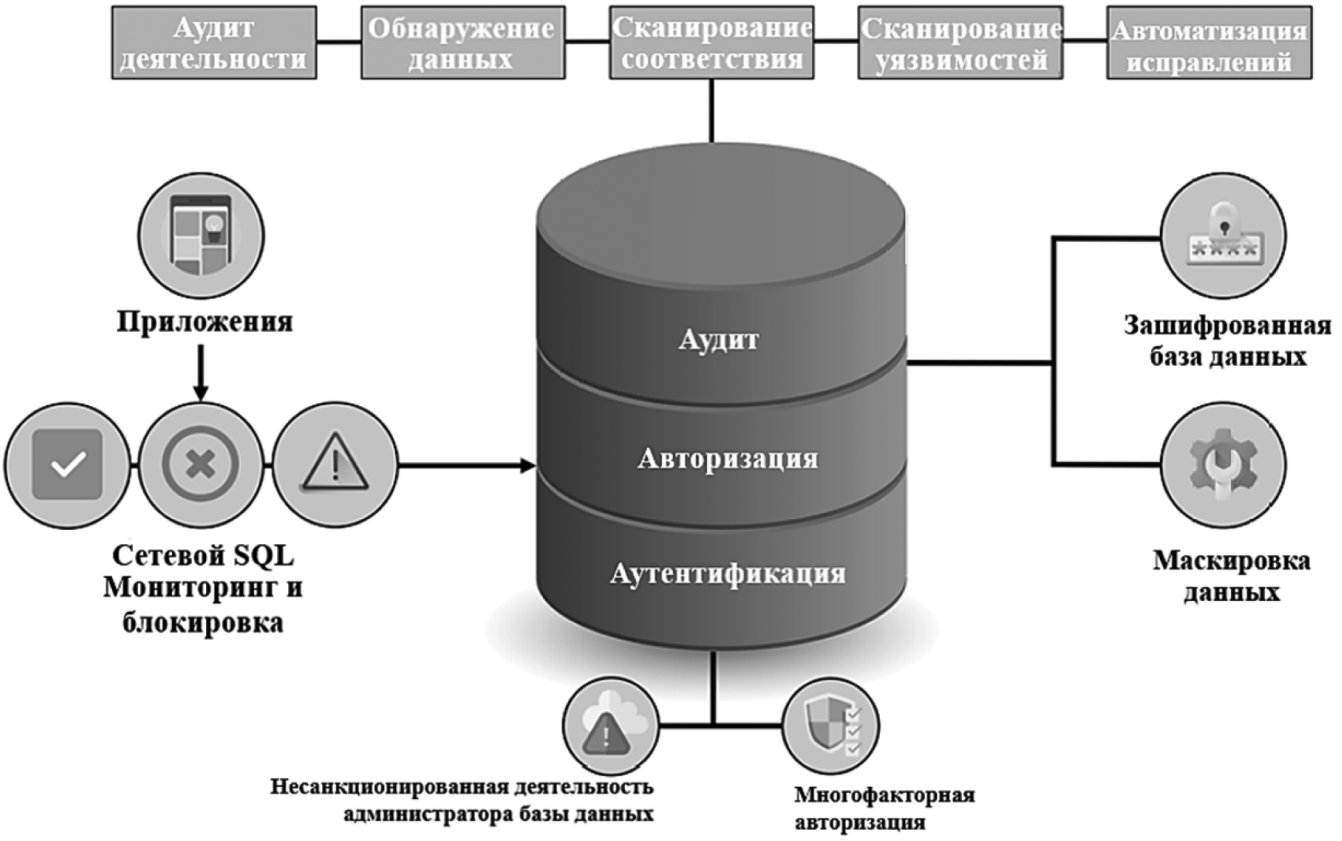

Рис. 2. Комплекс информационных технологий Eclipsys для защиты базы данных от кибератак

обход приложений и другие вредоносные действия;
- маскировка данных — обеспечивает конфиденциальность, предотвращая раскрытие секретных частей информации неавторизированным лицам;
- хранилище базы данных — реализует превентивный контроль за привилегированными пользователями для предотвращения внутренних атак.

Также отдельно можно выделить ряд передовых информационных технологий, которые способны внести существенный вклад в защиту базы данных от кибератак.

Цифровые подписи. Алгоритмы цифровой подписи, такие как RSA или DSA, представляют собой более сложные вычисления, в которых сочетаются свойства хэш-функций по обнаружению несанкционированного доступа и указание конкретного лица или учреждения, которое заверяет информацию. Они опираются на секретный ключ, который знает только ответственная сторона. Базы данных, отслеживающие персональную ответственность, могут включать цифровые подписи, подтверждающие конкретные транзакции.

SNARKs. Лаконичный неинтерактивный аргумент знания (SNARK) — это более сложная версия цифровых подписей, которая может подтвердить личную информацию, не раскрывая саму информацию. Эта информационная технология опирается на математику, которую иногда называют «доказательством с нулевым знанием» (ZKP). Базы данных, использующие SNARK и другие подобные технологии, могут защищать конфиденциальность пользователей, обеспечивая при этом соблюдение нормативных требований.

Федеративная обработка. Некоторые разработчики разбивают набор данных на более мелкие части, иногда значительно более мелкие, и затем распределяют их по множеству независимых компьютеров. Иногда места расположения данных зашифрованы, поэтому бывает невозможно предсказать, на каком компьютере будет храниться та или иная запись. Такие решения часто строятся на основе программных пакетов, призванных ускорить работу с так называемыми большими данными за счет параллельного запуска алгоритмов поиска или анализа. Изначально целью была скорость, но побочным эффектом может быть повышенная устойчивость к атакам.

Таким образом, поскольку киберпространство сегодня стремительно развивается и существенным образом усложняется, количество нарушений целостности и надежности баз данных увеличивается многократно. В данном контексте для защиты баз данных решающее значение имеют современные информационные технологии, которые обладают широкими возможностями обеспечения непрерывной комплексной защиты с соблюдением нормативных требований.

ЛИТЕРАТУРА

1. Афанасьева С.В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации // Вестник Самарского университета. Экономика и управление. 2023. № 2. С. 7–16.
2. Ali Alqahtani, Surbhi Bhatia Khan An optimal hybrid cascade regional convolutional network for cyberattack detection // International Journal of Network Management. 2023. № 176. P. 81–94.
3. He Wen, Faisal Khan Cybersecurity and process safety synergy: An analytical exploration of cyberattack-induced incidents // The Canadian Journal of Chemical Engineering. 2023. № 09. P. 67–73.
4. Белевитин В.А. Оценка эффективности защиты информации на основе нечетких рисков // Вопросы науки. 2022. № 3. С. 100–105.
5. Зубков В.О. Подходы к управлению информационной безопасностью на базе современных технологий // Автоматизация и информатизация ТЭК. 2024. № 1 (606). С. 28–35.

Журнал «Современная наука: актуальные проблемы теории и практики»