Совершенствование системы защиты отечественных СУБД

Воробьева Диана Евгеньевна

соискатель ученой степени кандидата технических наук, АО «Невское проектно-конструкторское бюро», Санкт-Петербург, Россия, dinvor@mail.ru

АННОТАЦИЯ

Введение: В настоящее время происходит постоянное увеличение количества атак на базы данных значимых объектов информационной инфраструктуры. В то же время обеспечение защищенной работы СУБД является одной из главных задач, решаемых при обеспечении защиты критических информационных инфраструктур. **Постановка задачи:** Безопасность систем управления базами данных и самих баз данных относится к набору инструментов, элементов управления и мер, предназначенных для установления и сохранения конфиденциальности, целостности и доступности базы данных, требуется провести критический анализ существующих подходов. **Методы:** методы синтеза программных систем защиты информации. **Результаты**: методика разработки прототипа программной системы обеспечения целостности базы данных. **Практическая значимость**: обеспечение безопасной работы СУБД SQL в условиях заранее неизвестных компьютерных атак. **Обсуждение**: новизна предложенной задачи состоит в том, что предложено применение блокирующего транслятора с целью обеспечения целостности среды выполнения работ с СУБД.

КЛЮЧЕВЫЕ СЛОВА: государственная система обнаружения и предупреждения компьютерных атак целостность баз данных, защита от атак внутреннего нарушителя, программная система, блокировка опасных воздействий

Введение

Безопасность систем управления базами данных и самих баз данных относится к набору инструментов, элементов управления и мер, предназначенных для установления и сохранения конфиденциальности, целостности и доступности базы данных. Данная статья рассматривает вопросы конфиденциальности, поскольку это элемент, который скомпрометирован за счет большого количества утечек данных.

В настоящее время существует противоречие между недостаточными техническими возможностями средств защиты СУБД по выявлению и нейтрализации атак в условиях целенаправленных воздействий и высокими требованиями к защищённости и своевременности обработки данных в СУБД при проектировании кораблей на основании как ведомственных, так и общероссийских требований [1-3].

В отечественных СУБД, особенно в рамках выполнения требований Указа Президента РФ о переходе в КИИ на отечественное ПО до 2025 года, требуется обеспечение необходимой защищенности против как заранее известных, так и неизвестных компьютерных атак.

Степень разработанности темы

Анализ ранее проведенных исследований в области защиты СУБД и самих данных показал, что в известных работах были рассмотрены различные аспекты такой защиты:

- Анализ функциональной стабильности критичных информационных систем был выполнен в работах Б.В. Соколова, П.В. Сундеева, но в данных работах нет теории и нормативно-методического аппарата анализа защищенности БД от целенаправленных воздействий.
- Вопросы моделирования непрерывности функционирования ИС были разработаны в трудах В.А.Герасименко, Ю.Г.Ростовцева, П.Л.Чебышева, А.А.Маркова, А.М.Ляпунова, П.Берстейна, Ф.Найта, Т.Авена, Д.Гольмана, Д.Скотта, но в них приведена только общая теория для информационных систем в целом.
- Задачи моделирования систем защиты информации были исследованы в работах П.Д.Зегжды, А.М.Ивашко, О.И.Береснева, В.Е.Ильина, но в них нет модели защищенной обработки транзакций в БД.
- Модели и механизмы управления безопасностью рассматривались в работах В.Н.Буркова, Е.В.Грацианского, П.Н.Девянина, С.И.Дзюбко, А.В.Щепкина, Дж.Вакка, но существующие модели и механизмы управления безопасностью нацелены только на защиту данных и не включают СУБД как отдельный вид ПО.
- Выбор критериев эффективности комплексных систем безопасности был выполнен в работах В.И.Васильева, Т.А.Иванова, А.А.Бакирова, С.М.Климова, Б.П.Пальчуна, М.П.Сычева, но существующие критерии эффективности не полностью учитывают целенаправленные воздействия.

Модель угроз и задачи обеспечения защиты баз данных в отечественных СУБД

Система безопасности баз данных в значимых объектах критической информационной инфраструктуры, в частности, в АСУ проектирования кораблей должна учитывать и защищать следующее:

- данные в базе данных;
- система управления базами данных (СУБД);
- любые связанные с процессом проектирования кораблей приложения, которые могут запускаться параллельно с работой СУБД;
- сервер базы данных и/или виртуальный сервер базы данных и базовое оборудование ЦОДа;
- вычислительная и/или сетевая инфраструктура, используемая для доступа к базе данных [4].

По определению, утечка данных — это неспособность сохранить конфиденциальность данных в базе данных [5]. Какой вред нанесет утечка данных вашему предприятию, зависит от ряда последствий или факторов:

- скомпрометированная интеллектуальная собственность;
- ущерб репутации организации;
- прерывание деятельности на длительный период;
- штрафы или пени за несоблюдение договоров;

- расходы на устранение нарушений и уведомление клиентов.

Рассмотрим наиболее распространенные типы или причины атак на безопасность баз данных и их причины [6-7].

1. Инсайдерские угрозы

Внутренняя угроза — это угроза безопасности, исходящая из любого из трех источников с привилегированным доступом к базе данных:

- злонамеренный инсайдер, намеревающийся причинить вред;
- нерадивый инсайдер, который допускает ошибки, которые делают базу данных уязвимой для атак;
- промышленный шпион — посторонний человек, который каким-то образом получает доступ к базе данных.

Внутренние угрозы являются одной из наиболее распространенных причин нарушений безопасности баз данных и часто являются результатом того, что слишком большое количество сотрудников имеют учетные данные привилегированных пользователей.

2. Человеческий фактор

Слабые пароли, совместное использование паролей и другое неразумное или неинформированное поведение пользователей по-прежнему являются причиной почти половины (49%) всех зарегистрированных утечек данных.

3. Эксплуатация уязвимостей в программном обеспечении баз данных

В настоящее время как настоящие, так и «этичные» хакеры зарабатывают на жизнь, находя и устраняя уязвимости во всех видах программного обеспечения, включая программное обеспечение для управления базами данных. Все крупные коммерческие поставщики программного обеспечения для баз данных и платформы управления базами данных с открытым исходным кодом регулярно выпускают исправления безопасности для устранения этих уязвимостей, но несвоевременное применение этих исправлений может привести к увеличению уязвимости [8-9].

4. Атаки с внедрением SQL/NoSQL

Это угрозы, специфичные для базы данных, которые включают в себя вставку произвольных строк атак SQL или не-SQL в запросы к базе данных, обслуживаемые веб-приложениями или заголовками HTTP. Организации, которые не следуют методам безопасного кодирования веб-приложений и не проводят регулярное тестирование уязвимостей, подвержены таким атакам.

5. Эксплуатация переполнения буфера

Переполнение буфера возникает, когда процесс пытается записать в блок памяти фиксированной длины больше данных, чем ему разрешено вместить. Злоумышленники могут использовать избыточные данные, хранящиеся в смежных адресах памяти, в качестве основы для запуска атак.

6. Вредоносное ПО

Вредоносное ПО — это программное обеспечение, написанное специально для использования уязвимостей или иного нанесения ущерба базе данных. Вредоносное ПО может распространяться через любое конечное устройство, подключенное к сети базы данных.

7. Атаки на резервные копии

Организации, которые не защищают данные резервных копий с помощью тех же строгих средств контроля, которые используются для защиты самой базы данных, могут быть уязвимы для атак на резервные копии [10].

Причины недостаточной эффективности системы защиты современных СУБД

Объективные причины.

Растущие объемы данных: Сбор, хранение и обработка данных продолжают расти в геометрической прогрессии почти во всех организациях. Любые инструменты или методы обеспечения безопасности данных должны обладать высокой масштабируемостью для удовлетворения потребностей ближайшего и отдаленного будущего.

Разрастание инфраструктуры: сетевые среды становятся все более сложными, особенно по мере того, как компании перемещают рабочие нагрузки в мульти облако или гибридное облако архитектуры, что делает выбор, развертывание и управление решениями безопасности еще более сложными [11-12].

Все более строгие нормативные требования РФ: Ситуация с соблюдением нормативных требований в РФ продолжает усложняться, что усложняет соблюдение всех требований.

Нехватка специалистов в области кибербезопасности: эксперты прогнозируют, что к 2024 году может остаться до 9 миллионов вакансий в сфере кибербезопасности.

Субъективные причины и изменение модели нарушителя

Приблизительно семь лет назад попадание в Интернет в свободном доступе материалов методологии EcCouncil по «этичному хакингу» привело к настоящему времени к беспрецедентной ситуации, когда оснащенность нарушителя для хакерских атак гарантируется наличием в Интернете постоянно обновляющихся операционных систем для пентестинга в которых предустановлено до 1500 специальных утилит [13-20].

Это означает, что при разработке модели нарушителя в организации можно сразу ставить высшую ступень для нарушителя Н1. При этом в действующих нормативных документах совершенно не учитывается тот факт, что основная масса атак в настоящее время во все мире реализуется школьниками и студентами младших курсов, многие из которых даже открывают лаборатории по пентестингу.

В российском сегменте Интернета существуют специальные сайты для тренировки «этичных хакеров», где имитируется сеть банка, промышленного предприятия, исследовательского института, постоянно подогревается интерес к олимпиадам и соревнованиям CTF (в хакерских технологиях).

Все это означает, что система безопасности современных отечественных СУБД должна быть модифицирована с учетом реалий настоящего времени.

Предложения по системе защиты баз данных предприятия

1. Защищенность от атак типа «отказ в обслуживании» (DoS/DDoS)

При атаке типа «отказ в обслуживании» (DoS) злоумышленник перегружает целевой сервер (в данном случае сервер базы данных) таким количеством запросов, что сервер больше не может выполнять законные запросы от реальных пользователей, и во многих случаях сервер становится нестабильным или выходит из строя.

Поскольку базы данных почти всегда доступны по сети, любая угроза безопасности для любого компонента в сетевой инфраструктуре или ее части также является угрозой для базы данных, а любая атака, затрагивающая устройство или рабочую станцию пользователя, может угрожать базе данных. Таким образом, безопасность базы данных должна выходить далеко за пределы одной только базы данных.

Любая атака такого типа на физический сервер базы данных будет эффективна, поэтому единственным способом защиты может служить работа АРМ с «витринной базой данных» которая имеет воздушный зазор с настоящей. При этом реализуется как защита от атак извне периметра, так и от внутренних атак.

2. Физическая охрана

Независимо от того, находится ли сервер базы данных локально или в облачном центре обработки данных, он должен быть расположен в безопасной зоне. Одним из современных вариантов обеспечения физической безопасности является вариант, если сервер базы данных находится в облачном центре обработки данных.

3. Безопасность учетной записи конечного пользователя/устройства

Решения для мониторинга данных могут предупредить, если действия с данными являются необычными или опасными. Все пользовательские устройства, подключающиеся к сети, в которой размещена база данных, должны быть физически защищены (только в руках соответствующего пользователя) и постоянно подвергаться контролю безопасности.

4. Шифрование

Все данные, включая данные в базе данных и учетные данные, должны быть защищены с помощью лучшего в своем классе отечественного протокола шифрования при хранении и передаче. Все ключи шифрования должны обрабатываться в соответствии с рекомендациями.

5. Безопасность программного обеспечения баз данных

Поскольку нет никакой гарантии, что программное обеспечение как СУБД, так и прикладного характера не имеет программных закладок, требуется разработка внешних блокираторов опасной функциональности.

6. Безопасность приложений/веб-серверов.

Любое приложение или веб-сервер, взаимодействующий с базой данных, может быть каналом для атаки и должен подвергаться постоянному тестированию безопасности и управлению передовыми методами.

7. Безопасность резервного копирования

Все резервные копии, копии или образы базы данных должны подвергаться тем же (или столь же строгим) средствам контроля безопасности, что и сама база данных.

8. Аудит: запись всех входов на сервер базы данных и в операционную систему, а также регистрация всех операций, выполняемых с конфиденциальными данными. Аудит безопасности баз данных должен проводиться регулярно.

9. Для значимых объектов КИИ, требуется автоматическое определение причин нештатного функционирования рабочих мест операторов, работающих с СУБД, как и самой базы данных и автоматическое информирование в систему ГосСОПКА.

Заключение

Представленный в статье анализ современного состояния дел в области модели угроз и нарушителя для баз данных показывает, что при модернизации системы защиты отечественных СУБД требуется учитывать ряд новых факторов.

Фактически в настоящее время существует только одна защищенная отечественная СУБД – «Линтер-ВС», в которой не выполняются все перечисленные выше требования, что делает актуальной ее модернизацию.

Применение блокирующего транслятора позволит в реальных системах отказаться от сигнатурного анализа команд управления СУБД, а с другой стороны увеличить защищенность благодаря возможности блокирования запуска опасных процессов в памяти АРМ как при внешнем, так и внутреннем их вызове.

Литература

1. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / *А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов* // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.

2. *Белов А. С.* Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / *А. С. Белов, М. М. Добрышин, Д. Е. Шугуров* // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.

3. *Васильев В. И.* Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / *В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова* // Вопросы кибербезопасности. - 2022. - № 2. - С. 27-38.

4. *Гладких А. В.* Методы защиты от DDoS –атак в интеллектуальных сетях / *А. В. Гладких* // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 3-5.

5. *Гладков А. Н.* Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности = Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the field of Information Security / А. Н. Гладков, С. Н. Горячев, Н. С. Кобяков // Защита информации. Инсайд. - 2023. - № 1. - С. 32-37.

6. *Голубев Г. Д.* Обзор безопасности маломощных глобальных сетей: угрозы, проблемы и потенциальные решения / Г. Д. Голубев // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 5-11.

7. *Горбунов Д.Д.* Криптовалюта и блокчейн: перспективы развития с точки зрения информационной безопасности / Д. Д. Горбунов // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 11-17.

8. *Догучаева С. М.* Анализ современных проблем информационной безопасности в российских компаниях / *С. М. Догучаева* // Риск: ресурсы, информация, снабжение, конкуренция. - 2022. - № 2. - С. 65-68.

9. *Долганов К. А.* Технология блокчейн с точки зрения информационной безопасности / *К. А. Долганов* // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 14-17.

10. *Смирнова Н.А.* Формирование оценочной модели устойчивости с использованием дискриминантного анализа. — Нижний Новгород: Вестник нижегородского университета им. Н.И.Лобачевского, 2013, №3, с.235-238.

11. *Andress, J.* The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2019. — 240 p. — ISBN 9780128008126.

12. *Stewart, James Michael.* CISSP® : Certified Information Systems Security Professional Study Guide : [англ.] / James Michael Stewart, Mike Chapple, Darril Gibson. — Seventh Edition. — Canada : John Wiley & Sons, Inc., 2021. — 1023 p. — ISBN 978-1-119-04271-6.

13. *Moore, Robert.* Cybercrime : Investigating High Technology Computer Crime : [англ.]. — 2nd ed. — Boston : Anderson Publ., 2022. — 318 p. — ISBN 9781437755824.

14. Phishing attacks and countermeasures / *Ramzan, Zulfikar* // Handbook of Information and Communication Security : [англ.] / Peter Stavroulakis, Mark Stamp. — L. : Springer Science & Business Media, 2020. — 867 p. — ISBN 978-3-642-04117-4.

15. *Johnson, John.* The Evolution of British Sigint : 1653–1939 : [англ.]. — Her Majesty's Stationary Office, 2018. — 58 p.

16. *Staff, Gary.* Information security in DBMS. — Barnsley: Pen & Sword Books, 2021. — 224 p. — ISBN 978-1848841826.

17. Official Secrets Act (1889; New 1911; Amended 1920, 1939, 1989) // Spies, Wiretaps, and Secret Operations : An Encyclopedia of American Espionage / editor Hastedt, G. P.. — Santa Barbara, CA, USA : ABC-CLIO, LLC, 2021. — Vol. 2. — ISBN 978-1-85109-807-1.

18. Sebag–Montefiore, Hugh. Enigma : The Battle for the Code. — Orion, 2022. — 576 p. — ISBN 9781780221236.

19. *Pipkin, Donald L.* Information Security : Protecting the Global Enterprise : [англ.]. — N. Y. : Prentice Hall PTR, 2020. — 364 p. — ISBN 9780130173232.

20. Official (ISC)²® Guide to the CISSP® CBK® : Fourth Edition : [англ.] / Adam Gordon, Editor. — Boca Raton, FL, USA : CRC Press, 2019. — 1278 p. — ISBN 978-1-4822-6275-9.

IMPROVEMENT OF THE SYSTEM OF PROTECTION OF DOMESTIC DBMS

DIANA E. VOROBIEVA
JSC "Nevskoye Design Bureau",
St Petersburg, Russia dinvor@mail.ru

ABSTRACT

Introduction: At present, there is a constant increase in the number of attacks on the databases of significant information infrastructure objects. At the same time, ensuring the secure operation of the DBMS is one of the main tasks to be solved when ensuring the protection of critical information infrastructures. **Problem Statement:** The security of database management systems and databases itself refers to a set of tools, controls and measures designed to establish and maintain the confidentiality, integrity and availability of a database, and a critical analysis of existing approaches is required. **Methods:** methods of synthesis of information security software systems. **Results:** methodology for developing a prototype of a software system for ensuring the integrity of the database. **Practical significance:** ensuring the safe operation of the SQL DBMS in the face of previously unknown computer attacks.

Keywords: the novelty of the proposed task lies in the fact that a mechanism for proactively blocking dangerous impacts on significant objects of critical information infrastructure is proposed.

REFERENCES

1. Puchkov A. Yu., Sokolov A. M., Shirokov S. S., Prokimnov N. N. Algorithm for identifying information security threats in distributed multiservice networks of public administration bodies / A. Yu. - 2023. - Vol. 18, No. 2. - P. 85-102.
2. Belov A. S., Dobryshin M. M., Shugurov D. E. Modernization of the Information Security System: The Approach to Determining the Frequency: Approach to Determining the Frequency: Approach to Determining the Periodicity / A. S. Belov, M. M. Dobryshin, D. E. Shugurov // Information Protection. Inside. - 2022. - № 4. - P. 76-80.
3. Vasil'ev V. I., Vulfin A. M., Kuchkarova N. V. Otsenka aktual'nykh ugroz bezopasnosti informatsii s pomoshchi tekhnologii transformerov [Assessment of actual threats to information security with the help of transformers technology] / V. I. Vasil'ev, A. M. Vulfin, N. V. Kuchkarova // Voprosy cyberbezopasnost'. - 2022. - № 2. - P. 27-38.
4. Gladkikh A. V. Metody zashchita ot DDoS –atak v intellektual'nykh seti [Methods of protection against DDoS –attacks in intellectual networks] / A. V. Gladkikh // Digital transformation of society and information security: materials of the All-Russian Federation. Sci.-Prakt. Conf. (Yekaterinburg, May 18, 2022) - Yekaterinburg, 2022. - P. 3-5.
5. Gladkov A. N., Goryachev S. N., Kobyakov N. S. Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the Field of Information Security = Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the Field of Information Security / A. N. Gladkov, S. N. Goryachev, N. S. Kobyakov // Information Protection. Inside. - 2023. - № 1. - P. 32-37.
6. Golubev G. D. Obzor bezopasnosti malomoshchnykh global'nykh seti: ugrozy, problemy i potentsionnykh resheniya [Review of the security of low-power global networks: threats, problems and potential solutions] / G. D. Golubev // Digital transformation of society and information security: materials of Vseross. Sci.-Prakt. Conf. (Yekaterinburg, May 18, 2022) - Yekaterinburg, 2022. - P. 5-11.

7. Gorbunov D.D. Cryptocurrency and Blockchain: Development Prospects from the Point of View of Information Security / D. D. Gorbunov // Digital Transformation of Society and Information Security: Materials of Vseross. Sci.-Prakt. Conf. (Yekaterinburg, May 18, 2022) - Yekaterinburg, 2022. - P. 11-17.
8. Doguchaeva S. M. Analiz sovremennykh problemy informatsionnogo bezopasnosti v rossiyskikh kompanii [Analysis of modern problems of information security in Russian companies] / S. M. Doguchaeva // Risk: resources, information, supply, competition. - 2022. - № 2. - P. 65-68.
9. Dolganov K. A. Tekhnologiya blockchain s vzremennosti informatsionnogo bezopasnosti [Blockchain technology from the point of view of information security] / K. A. Dolganov // Digital transformation of society and information security: materials of Vseross. Sci.-Prakt. Conf. (Yekaterinburg, May 18, 2022) - Yekaterinburg, 2022. - P. 14-17.
10. Smirnova N.A. Formation of an Evaluation Model of Stability Using Discriminant Analysis. - Nizhny Novgorod: Vestnik Nizhny Novgorod University named after N.I. Lobachevsky, 2013, No. 3, pp. 235-238.
11. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2019. — 240 p. — ISBN 9780128008126.
12. Stewart, James Michael. CISSP® : Certified Information Systems Security Professional Study Guide : [англ.] / James Michael Stewart, Mike Chapple, Darril Gibson. — Seventh Edition. — Canada : John Wiley & Sons, Inc., 2021. — 1023 p. — ISBN 978-1-119-04271-6.
13. Moore, Robert. Cybercrime : Investigating High Technology Computer Crime : [англ.]. — 2nd ed. — Boston : Anderson Publ., 2022. — 318 p. — ISBN 9781437755824.
14. Phishing attacks and countermeasures / Ramzan, Zulfikar // Handbook of Information and Communication Security : [англ.] / Peter Stavroulakis, Mark Stamp. — L. : Springer Science & Business Media, 2020. — 867 p. — ISBN 978-3-642-04117-4.
15. Johnson, John. The Evolution of British Sigint : 1653–1939 : [англ.]. — Her Majesty's Stationary Office, 2018. — 58 p.
16. Staff, Gary. Information security in DBMS. — Barnsley: Pen & Sword Books, 2021. — 224 p. — ISBN 978-1848841826.
17. Official Secrets Act (1889; New 1911; Amended 1920, 1939, 1989) // Spies, Wiretaps, and Secret Operations : An Encyclopedia of American Espionage / editor Hastedt, G. P.. — Santa Barbara, CA, USA : ABC-CLIO, LLC, 2021. — Vol. 2. — ISBN 978-1-85109-807-1.
18. Sebag–Montefiore, Hugh. Enigma : The Battle for the Code. — Orion, 2022. — 576 p. — ISBN 9781780221236.
19. Pipkin, Donald L. Information Security : Protecting the Global Enterprise : [англ.]. — N. Y. : Prentice Hall PTR, 2020. — 364 p. — ISBN 9780130173232.
20. Official (ISC)²® Guide to the CISSP® CBK® : Fourth Edition : [англ.] / Adam Gordon, Editor. — Boca Raton, FL, USA : CRC Press, 2019. — 1278 p. — ISBN 978-1-4822-6275-9.