УДК 004.056

ПРОБЛЕМНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ БАЗ ДАННЫХ В ТАМОЖЕННЫХ ОРГАНАХ

Павлова Я.В., Самойленко О.Р.
Санкт-Петербургский имени В.Б.Бобкова филиал Российской таможенной академии

PROBLEM ASPECTS OF ENSURING INFORMATION SECURITY OF DATABASE FUNCTIONING IN CUSTOMS AUTHORITIES

Pavlova Y.V., Samoilenko O.R.
St. Petersburg named after V.B. Bobkov branch of the Russian Customs Academy

Аннотация
В процессе деятельности таможенных органов Российской Федерации используется огромное количество информации, которая для удобства и оперативности применения структурирована в виде баз данных. В статье рассмотрены самые значимые и опасные уязвимости, возникающие при использовании баз данных на практике. Проанализированы основные проблемы в области обеспечения безопасности баз данных. Представлены возможные пути устранения.

Ключевые слова: информация, база данных, система управления базами данных, защита информации, уязвимость.

Abstract
In the process of activity of the customs authorities of the Russian Federation, a huge amount of information is used, which is structured in the form of databases for the convenience and speed of use. The article considers the most significant and dangerous vulnerabilities that arise when using databases in practice. The main problems in the field of database security are analyzed. Possible solutions are presented.

Keywords: information, database, database management system, information protection, vulnerability.

На современном этапе в результате стремительного развития технологических процессов в сфере информационных таможенных технологий, которые формируют непрерывность пополнения архивов разнородной информации, роль данных модернизаций значительно превышает возможности человеческой деятельности в части осуществления практической обработки и извлечении необходимых данных. В ходе установления особой важности и практической применимости современных технологий ведется активная работа по созданию центров обработки данных и различных баз данных, по запросам из которых должностное лицо в минимальные сроки может произвести выборку данных об интересующем подконтрольном объекте. Вследствие этого в настоящее время одним из приоритетных направлений деятельности таможенных органов является обеспечение безопасности баз данных, так как при атаках на хранилища обработки данных может произойти утечка конфиденциальной информации, а также значительный рост временных издержек из-за физической невозможности должностного лица вручную обрабатывать большие потоки информации. Данные факторы негативно скажутся как на материальном состоянии участников внешнеэкономической деятельности, так и на государственных органах. Ссылаясь на статистические данные компании Infowatch, можно сделать вывод о том, что количественная численность утечек стратегически важных для государства данных беспрерывно растет. Стоит отметить, что на 2019 год более 44,4 % утечек было произведено в результате присутствия внешних нарушителей, а свыше 55,6 % осуществлялось в ходе неумышленного участия сотрудников [1]. Исходя из вышесказанного, можно отметить

особую необходимость в рассмотрении часто встречающихся проблемных аспектов в сфере защиты баз данных и выявлении наиболее целесообразных предложений возможных перспектив совершенствования.

Вследствие того, что основная ориентация Федеральной таможенной службы России на современном этапе представляет собой внедрение перспективных информационных технологий для повышения уровня эффективности функционирования и качества, предоставляемых участникам ВЭД, таможенных услуг, необходимо также обеспечить и должный уровень защиты передаваемых в информационной среде сведений.

Атаки на хранилища информационных ресурсов баз данных выступают в качестве одних из самых значимых и опасных для государственных контролирующих органов, так как санкционируют утечку конфиденциальных данных. В результате данных атак целесообразно рассмотреть основные слабые места анализируемых систем и выявить наиболее часто встречающиеся проблемные аспекты в области обеспечения защиты баз данных.

На современном этапе список основных слабых мест системы управления базой данных не претерпевал значительных модификаций по отношению к предыдущим годам [2, С. 28]. Путем проведения анализа существующих в настоящее время средств обеспечения безопасности СУБД, их архитектуру, а также ранее обнародованные уязвимости и практическую деятельность по обеспечению безопасности, можно установить ряд следующих оснований для возникновения проблемных ситуаций в области защиты баз данных. К данным аспектам относится:

а) программисты баз данных и их администраторы зачастую не предоставляют должный уровень внимания вопросам безопасности, так как их деятельность сконцентрирована больше на конечном итоге, чем на целях его достижения;

б) разность совокупности масштабов и разновидностей хранимых информационных ресурсов нуждаются в установлении различных подходов к безопасности в зависимости от уровня их использования, например ФТС, РТУ, таможни либо таможенные посты;

в) различные СУБД используют разные языковые конструкции для доступа к данным, которые организованы на базе одной модели;

г) со стремительным ростом научно-технического процесса образуются новые виды и модели хранения данных, а при учете того факта, что деятельность преступных группировок также не стоит на месте довольно важно своевременно вносит модернизации в обеспечение безопасности хранимой информации [3, С. 38].

Использование разнообразных механизмов для защиты баз данных также выступает в качестве компромисса в финансовой сфере, так как зачастую внедрение в систему новейших методов защиты информации путем приобретения защищенных продуктов и отбор более квалифицированных специалистов данной отрасли несет и соответствующие крупные материальные издержки для государственных органов. Именно поэтому данные компоненты могут часто оказывать влияние и быть одной из причин уязвимости баз данных.

Хранилище данных представляет собой ряд компонентов, куда относятся совокупность информационных ресурсов – база данных и программы, которые осуществляют управление – СУБД. Исходя из приведенной иерархии, стоит отметить, что все уязвимости в области защиты данных подразделяются на категории, зависящие и не зависящие от данных. Уязвимости, которые не зависят от данных, выступают в качестве свойственных для всех видов ПО. Основной причиной наличия в системе таких уязвимостей может послужить несвоевременное обновление ПО, наличие неиспользуемых функций или недостаточность квалификации администратора ПО. Тем не менее, большее количество уязвимостей баз данных являются зависимыми от данных. В качестве примера можно привести тот факт, что СУБД поддерживают запросы к данным только при использовании определенного языка запросов, который содержит в себе наборы доступных пользователю функций, выступающих в качестве операторов языка. В результате этого в зависимости от используемого синтаксиса языка могут быть обнаружены те или иные уязвимости [4, С. 318].

Также в качестве распространенных проблем защиты баз данных можно выделить и отсутствие интегрированного контроля всех баз данных. Данная проблема является довольно серьезной, так как ведение отдельных аналитических выкладок по каждой базе данных не может гарантиро-

вать раскрытие полноты действий пользователей. На современном этапе злоумышленники могут замаскировать нарушения под совершенно допустимые действия пользователей БД [5, С. 57].

Также специалисты в сфере ИТ технологий при текучести кадров зачастую несвоевременно удаляют не используемые учетные записи лица, который больше не является должностным лицом, что в свою очередь предоставляет большой потенциал для злоумышленников. При помощи различных неправомерных технологий подбора злоумышленники могут получить доступ к данной учетной записи, и не только взломать ее, а также поднять права доступа в системе. Так как существующие стандартные системы мониторинга активности пользователей не реагируют на данные происшествия, так как с точки зрения системы они выступают в качестве легитимных.

В результате вышесказанного, так как осуществление мероприятий, связанных с обеспечением информационной безопасности, а также установление комплексной защиты информации выступает в качестве основного вида деятельности таможенных органов, то данные положения закреплены и в Стратегии развития таможенных органов на период до 2030 года [6]. Для решения вышеприведенных проблемных аспектов в сфере обеспечения информационной безопасности баз данных, можно предложить ряд следующих методов противодействия угрозам:

1. Разработать комплексную методику обеспечения безопасности хранилища данных в структуре государственных органов. В результате формирования данной схемы в отношении должностных лиц произойдет снижение уровня вероятности совершить ошибки при управлении СУБД и защитить базу данных от наиболее часто встречающихся слабых мест системы.

2. Произвести оценку и классификацию всех вероятных угроз и слабых мест базы данных. При осуществлении данного мероприятия произойдет упорядочение данных аспектов, что послужит существенным преимуществом для обеспечения защиты и проведения последующего анализа целесообразности применения тех или иных мер по минимизации по отношению к классифицируемым угрозам. В результате внедрения данного механизма администраторы будут наделены возможностью установления и прогнозирования ряда классифицируемых угроз, и заблаговременно обеспечить защиту наиболее слабым местам базы данных.

3. Осуществить разработку стандартизированных механизмов по защите данных и обеспечению информационной безопасности в целом. Данная стандартизация позволит сформировать единые средства защиты, которые будут наделены возможностью применения к различным базам данных. В соответствии с тематикой исследуемой работы, в первую очередь, предлагается стандартизировать подходы к работе с БД в государственных контролирующих органах, так как информация данных структур оценивается на уровне государственной безопасности.

4. Обеспечить функционирование баз данных исключительно в доверенной среде. В качестве доверенной можно выделить среду, которая объединяет всю совокупность механизмов, обеспечивающих защиту баз данных, и хранимой в ней информации. Также в данной системе должны быть соответствующие защищенные методы и каналы обмена данными.

5. Осуществление актуальной настройки СУБД и организацией ее безопасности. К данному аспекту можно отнести ряд общих требований и рекомендаций, таких как: своевременность установки обновлений, исключение из базы неиспользуемых модулей, а также формирование результативной политики паролей.

6. Формирование теоретических баз, в которых установлен порядок информационной защиты баз данных [7, С. 126]. Вследствие того, что информационная сфера постоянно модернизируется, появляются новые протоколы безопасности, программные продукты, а вместе тем и совершенствуются методы преступных деяний, связанных с компрометацией данных, целесообразно своевременно модернизировать теоретические базы в контексте формализации модели данных, а также разработке подходов обеспечения целостности информации для новых хранилищ [8, С. 28].

Для совершенствования ряда вопросов, касающихся отсутствия интегрированного контроля всех баз данных, предлагается объединить статистику пользования всеми базами данных и обеспечить их полную визуализацию, что значительно повысит шансы оперативного выявления несанкционированного доступа. Данная технология и подход к обеспечению защиты базы

данных особенно является актуальным для государственных органов, которые используют облачные базы данных. Для таможенных органов Российской Федерации в качестве такой базы может быть рассмотрен личный кабинет [9, С. 4].

В настоящее время для фильтрации неиспользуемых учетных записей необходимо создать систему защиты, которая в автоматическом режиме будет выявлять все сеансы работы пользователей. О тех сеансах, которые идут вразрез с политикой безопасности, система должна своевременно в режиме онлайн уведомлять централизованное управление путем направления оповещений, а также выявлять основные способы обхода системы безопасности [5, С. 23].

В ходе осуществления данного исследования можно выделить текущий подход к обеспечению информационной безопасности баз данных. Таким образом, для обеспечения безопасности баз данных необходимо внедрить, как систематизацию и развитие уже существующих технологий, так и стандартизацию механизмов по защите данных и разработку комплексной методике обеспечения безопасности хранилища данных в структуре государственных органов. В результате комплексного внедрения перспективных механизмов совершенствования в систему обеспечения безопасности баз данных значительно сократятся, в первую очередь временные издержки, а также будет обеспечен должный уровень безопасности путем выработке прогнозирования ряда классифицируемых угроз, путем которого будет осуществляться защита баз данных на ранних этапах до совершения атак на них.

Список литературы

1. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года // INFOWATCH.RU – Официальный сайт аналитического центра InfoWatch. URL: infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 (дата обращения: 28.04.2020).
2. Барбышева Г.И., Мирзаев Ш.Ф. Обеспечение информационной безопасности таможенных органов РФ // Инновационная экономика: материалы II Международной научной конференции Казань: Бук, 2015. С. 22-24.
3. Полтавцева М.А., Хабаров А.В. Безопасность баз данных // Программные продукты и системы. 2016. № 3. С. 36-41.
4. Власова О.А., Васильева А.С. Защита и безопасность базы данных // Решетневские чтения. 2017. № 4. С. 317-318.
5. Жуков Ю.В. Основы веб-хакинга. Нападение и защита. М.: Питер, 2018. 208 с.
6. Стратегия развития таможенных органов на период до 2030 года // ALTA.RU – Официальный сайт Альта софт. URL:alta.ru/expert_opinion/70803/ (дата обращения: 28.04.2020)
7. Цидилина И.А. Проблемы правового регулирования информационной безопасности таможенного администрирования в Российской Федерации // Информационная безопасность регионов. 2014. № 2 (11). С. 124-128.
8. Самогин А.С. Перспективы развития защиты информации от нелегального копирования. Теоретический аспект проблемы // Дневник науки. 2019. № 5 (29). 109 с.
9. Погодина И.В. Обеспечение информационной безопасности таможенных органов РФ // Таможенное дело. 2017. № 2. 6 с.
10. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года // INFOWATCH.RU – Официальный сайт аналитического центра InfoWatch. URL:infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 (дата обращения: 28.04.2020).

Поступила в редакцию 28.05.2020

Сведения об авторах:

Павлова Яна Валерьевна – доцент кафедры информатики и информационных таможенных технологий Санкт-Петербургского филиала Российской таможенной академии, кандидат технических наук, e-mail: kotf.nspu@mail.ru

Самойленко Ольга Руслановна – студент Санкт-Петербургского филиала Российской таможенной академии, e-mail: samolga1997@mail.ru

Электронный научно-практический журнал "**Бюллетень инновационных технологий**" (**ISSN 2520-2839**) является сетевым средством массовой информации
регистрационный номер **Эл № ФС77-73203**
по вопросам публикации в Журнале обращайтесь по адресу bitjournal@yandex.ru