ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

С.Г. Красочкин, *руководитель группы разработки интеграций*
Компания Xpate
(Россия, г. Москва)

DOI:10.24412/2500-1000-2022-7-1-89-95

Аннотация. *Развитие информационных технологий несет в себе как положительные, так и отрицательные моменты. Регулирование информационной безопасности является одним из направлений государственной политики. Информационная безопасность баз данных зависит от 3 составляющих: конфиденциальность, доступность и целостность. Основные подходы защиты (ПЗ) баз данных: использование шифрования; применение брандмауэра (сетевого экрана операционной системы); реализация автоматического мониторинга БД.*

Ключевые слова: *информационная безопасность, шифрование, брандмауэр (сетевого мониторинг БД, AES и DES, планировщик Cron).*

В условиях развития современного мира информация выступает основополагающим источником оказания влияния на людей. Сам термин «информация» представляет собой один из главных элементов информационного общества, которое так активно формируется в России. Информация непосредственно влияет на большинство направлений деятельности российского государства, формируя тем самым пути его развития. Актуальность проблемы информационной безопасности постоянно растет, и поощряется поиск новых способов защиты информации. С другой стороны, стремительное развитие информационно-коммуникационных технологий предоставляет возможности для внедрения новых способов защиты этой информации, и, конечно же, очень сильным катализатором этого процесса является очень сильное развитие общедоступной компьютерной сети.

Средства массовой информации, информационные ресурсы сети «Интернет» позволяют без особого труда оставаться в курсе всех событий. Но независимо от времени не теряет своей актуальности вопрос достоверности и безопасности информации, которую предоставляют нашему вниманию. Развитие информационных технологий несет в себе как положительные, так и отрицательные моменты. С одной стороны – информация служит основным фактором развития экономики и улучшения государственных и общественных институтов. С другой стороны – информация влечет за собой новые формационные угрозы. Регулирование информационной безопасности является одним из направлений государственной политики. Информационная система базы данных представлена на рисунке 1.

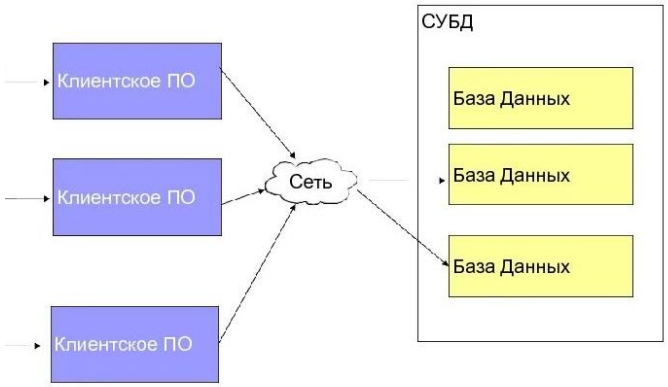

Рис. 1. Информационная система базы данных

Информационная безопасность (ИБ) баз данных зависит от 3 составляющих: конфиденциальность, доступность и целостность [5, 6]. В июне 2021 года партнеры Роскачества из потребительской организации Великобритании «Which?» провели тесты умного дома на кибербезопасность. За первую неделю тестирования эксперты увидели более 1 000 попыток взлома извне. Всего же за время исследования было зарегистрировано 12 807 инцидентов. В пересчете на часы – это одна кибератака каждые 4,5 минуты. Нарушитель может непрерывно следить за жертвой, управлять устройствами, а также украсть или удалить личные данные при взломе устройства.

Основные подходы защиты (ПЗ) баз данных на микрокомпьютере Raspberry Pi:

- использование шифрования;
- применение брандмауэра (сетевого экрана операционной системы);
- реализация автоматического мониторинга БД.

Данные могут быть зашифрованы как в самой базе данных, так и в тоннеле между БД и приложением, которое взаимодействует с ней. Это обеспечивает дополнительную защиту и сокрытие информации от нежелательных лиц. Часто используются симметричные алгоритмы блочного шифрования AES и DES [7]. Однако внедрение шифрования отрицательно сказывается на производительности БД, что необходимо учитывать при разработке решений. Система защиты баз данных ГИС «Интеграция» представлена на рисунке 2

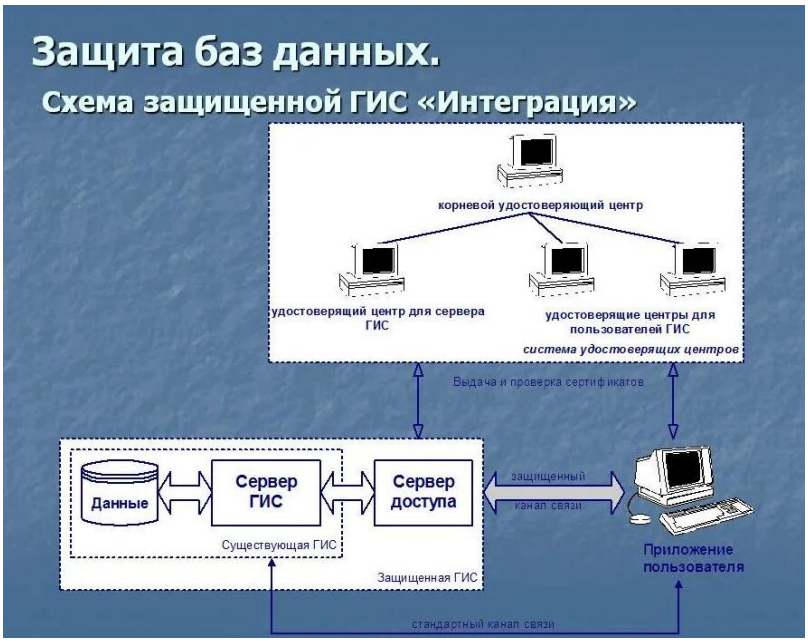

Рис. 2. Система защиты базы данных

Автоматический мониторинг баз данных может быть представлен различными программами, которые выдают каждодневный отчет о состоянии базы данных и выполняют ее резервное копирование, запускают различные команды [8], а также проверяют текущий статус базы данных и ее работоспособность. Например, для этой задачи может использоваться планировщик Cron – утилита, выполняющая скрипты на сервере по расписанию с заранее определенной периодичностью. Брандмауэр служит для контроля трафика сети, с его помощью можно задавать правила фильтрации. Он позволяет ограничить доступ к базе данных с недоверенных узлов, а также сократить возможность реализации DDoS атаки на устройства умного дома. Категории безопасности сервера баз данных представлены на рисунке 3.

Рис. 3. Категории безопасности сервера баз данных

Помимо удобства и комфорта, установленная система умного дома позволяет существенно снизить затраты на энергоносители, повысить безопасность проживания, а также производить контроль над приборами с помощью одного устройства. Однако разработчики зачастую не сообщают какие механизмы безопасности используются в своих решениях, а также недостаточно уделяют внимания ИБ. Не стоит забывать о безопасности личных данных на любых устройствах, которые окружают нас повсеместно. Рекомендуется устанавливать шифрование конфиденциальной информации, устанавливать специальные программы для мониторинга систем и контролировать трафик в сети, ограничивая нежелательный.

Информация нуждается в надежной защите. Большой процент утечек информации происходит по вине внутренних нарушителей, будь то халатное отношение к работе, злой умысел нарушителя или желание самоутвердиться. Внешние нарушители, как правило, более квалифицированы и действуют целенаправленно. Для решения таких проблем существуют методы, которые включат в себя организационные и технические методы защиты информации.

Для защиты от утечки информации рассмотрим совокупность этих двух методов. В ходе исследования были выделены основные принципы защиты корпоративной сети, такие как разграничение прав доступа, логирование действий на оборудовании, резервное копирование, своевременное обновление программного обеспечения, информирование и обучение пользователей, и использование специализированного программного обеспечения такого как, антивирусы, системы обнаружения вторжения, фаерволлы и другие. Доступ к оборудованию должен быть ограничен минимальным кругом лиц. Ограничение

распространяется как на физический, так и на удаленный доступ к оборудованию.

Логирование позволяет отслеживать практически все действия на оборудовании. Логи мощнейший инструмент для поиска неисправностей, а также для расследования инцидентов. К сожалению, у сетевого оборудования ограничено место для логов, что сказывается на временном промежутке хранения, то есть более старые логи удаляются, освобождая место для новых логов. Для решения данной проблемы рекомендовано использовать Лог-серверы. Резервное копирование одно из важнейших средств в арсенале системного администратора. Резервное копирование нужно делать при любых крупных изменениях конфигураций сетевого оборудования. В случае неудачной настройки будет возможность вернуть старые конфигурации оборудования. Старые версии прошивок сетевого оборудования несут множество уязвимостей. Для исключения использования этих уязвимостей злоумышленником, прошивку оборудования нужно обновлять по мере выхода новых версий. Также своевременно нужно обновлять всё программное обеспечение сети.

Информирование и обучение персонала одна из важнейших превентивных защитных мер. Персонал должен быть проинформирован о новых актуальных угрозах безопасности информации, о правилах безопасной эксплуатации информационной системы, о требованиях по защите информации (нормативные и внутренние документы организации) Специализированное программное обеспечение выбирается исходя из класса защищенности информационной системы. Организация защиты корпоративной сети трудоемкая задача со своими нюансами. При организации защиты сети нужно учитывать факторы нарастания внутренних и внешних угроз информационной безопасности, связанных с ростом сектора киберпреступности. Одним из серьезных препятствий обеспечения высокого уровня информационной безопасности является дороговизна готовых решений.

Наиболее широко используемой областью информационной безопасности сегодня являются криптографические методы. Однако на этом пути остается много нерешенных проблем, таких как влияние информационного оружия, такого как компьютерные вирусы и логические бомбы. Рассмотрим основные методы защиты при передачи секретной информации. Существует несколько методов скрытия данных в аудиосигнале: кодирование наименьших значащих бит, метод фазового кодирования. Стеганография – это метод сокрытия данных в изображениях, аудио и видео файлах. Сокрытие информации таким образом служит лучшим способом защиты данных, передаваемых от отправителя к получателю. При добавлении в исходное сообщение секретных данных с помощью различных методов стеганографии, каждый из которых имеет свои преимущества и недостатки. Абсолютной невидимости скрываемого сообщения достичь нельзя [3]. Стеганография в изображении также получила широкое распространение. Основная часть методов компьютерной стеганографии базируются на том, что файлы могут быть изменены без потери своей функциональности, а органы зрения человека не могут надежно различать модификацию изображения без помощи специальных инструментов. Существуют следующие методы скрытия данных в изображениях: скрытие данных в пространственной области, скрытие данных в частотной области изображения, методы расширения спектра. Для демонстрации надежности использования стеганографии рассмотрим скрытие данных в неподвижных изображениях с помощью метода замены наименее значащего бита и метода Куттера Джордана-Боссена. Оба метода будут реализованы с помощью программы MATLAB [4]. Тенденции развития науки и образования Метод замены наименее значащих бит является наиболее популярным в пространственной области. В младших значащих битах содержится меньше всего информации, а человек в большинстве случаев не замечает изменений в этом бите. Поэтому такие биты можно использовать для сокрытия информации путем их замены на биты скрываемого сообщения. Метод замены наименее значащих бит

позволяет скрывать в небольших файлах достаточно большой объем информации. Заметим, что невооруженным глазом увидеть какие-либо изменения в файле нельзя. Разница заметна лишь в пиксельном представлении изображений. Метод Куттера-Джордана-Боссена использует одно из свойств зрительной системы человека.

Глаз человека менее восприимчив к модификации яркости синего цвета по сравнению с зеленым и красным, поэтому для встраивания информации идет работа с синим цветом изображения. Суть метода заключается в изменении яркости синего цвета в пикселях изображения. Встраивание информации данным методом не изменяет размер файла и тем самым усложняет обнаружение факта скрытия данных [4]. С другой стороны, проблема распределения ключей при использовании криптографических методов также остается нерешенной и по сей день. Комбинация компьютерной стенографии и криптографии была бы хорошим способом избавиться от ситуации, поскольку это устранило бы слабые стороны методов информационной безопасности. Таким образом, компьютерная стенография в настоящее время является одной из ключевых технологий информационной безопасности.

Основными особенностями современной компьютерной стенографии являются [5]:

1. Методы скрытия должны обеспечивать аутентификацию и целостность файлов;

2. Предполагается, что методы стенографии, применяемые к злоумышленникам, хорошо известны;

3. Методы защиты информации основаны на сохранении основных свойств открытого файла с сокращенными изменениями и некоторой информацией – ключом, который неизвестен другим. Если время отправки сообщения известно злоумышленникам, сам процесс извлечения секретного сообщения следует рассматривать как вопрос сложного расчета. Например, наименее значимые маленькие фрагменты звука заменяются скрытым сообщением. Это изменение незаметно для большинства людей, когда они слышат голосовое сообщение. Стенографические методы, направленные на мониторинг деятельности систем промышленного шпионажа и управление сетевыми ресурсами, позволяют противодействовать попыткам контролировать поток информации с серверов локальных и глобальных компьютерных сетей. Еще одна область компьютерной стенографии, которая используется в настоящее время, – это программная маскировка.

Программы, запущенные в операционной среде Windows в дополнение к аутентификации информации могут быть решены следующие проблемы:

1) аутентификация пользователя, т.е. идентификация пользователя, который хочет получить доступ к ресурсам компьютерной системы;

2) взаимная аутентификация сетевых абонентов во время общения. Одной из областей, которые сегодня нуждаются в защите, являются электронные платежные системы и электронная торговля через Интернет.

Криптография – это набор методов модификации данных, которые решают две ключевые проблемы защиты данных: конфиденциальность и целостность. В то время как конфиденциальность понимается как сокрытие информации от злоумышленников, целостность означает, что информация не может быть изменена злоумышленниками. Здесь ключ отправляется по некоторому защищенному каналу (обозначенному пунктирными линиями на чертеже) [1].

В общем, этот механизм применим к симметричной ключевой системе. В этом случае открытый ключ отправляется по защищенному каналу, а секретный ключ не отправляется. Если злоумышленникам не удается достичь своих целей, и криптоаналитики не могут повторно использовать зашифрованную информацию, не зная ключа, то криптосистема называется криптографической системой. Надежность криптосистемы определяется ее ключом, и это одно из основных правил криптоанализа [2]. Основная предпосылка этого определения заключается в том, что криптосистема – это хорошо известная система,

для изменения которой требуется много времени и денег, поэтому необходимо защитить информацию только путем изменения ключа. Эти инструменты можно классифицировать следующим образом [4]:

1. Система идентификации и аутентификации пользователя. Система определяет, следует ли пользователю пройти верификацию, верификацию, а затем разрешить работать с системой. В этом случае возникает проблема с отбором информации у пользователя, которая может быть следующих типов:

2. Конфиденциальная информация, известная пользователю, такая как пароли, секретные ключи и т.д.;

3. Физиологические параметры человека, такие как отпечатки пальцев, изображение глаз и т.д.

4. Система шифрования дисковых данных. Основной целью этой системы является защита данных на диске. В этом случае логический и физический этапы разделены. На логической стадии файл является основным объектом, и защищены только некоторые файлы. Примером этого является программное обеспечение для архивирования. Физически диск полностью защищен. Примером этого является программа шифрования Diskreet в Norton Utilities. Система шифрования сетевых данных. Есть два способа сделать это [5]: шифрование всех данных, передаваемых по каналу, то есть каналам связи; шифрование только содержимого данных, отправляемых абонентами, то есть каналами связи, и оставить остальную служебную информацию открытой.

Таким образом, чтобы защитить секретные данные при передаче, имеется несколько способов ее сокрытия: стенографическая система защиты, криптографическая, а также система шифрования дисковых данных и тому подобные.

Библиографический список

1. Пантелеев, А.В. Системный анализ в телекоммуникационных системах / А.В. Пантелеев, С.Д. Шибайкин // Наука и бизнес: пути развития. – 2019. – № 11 (101). – С. 102-104.

2. Каляев А.И. Об одном методе мультиагентной организации облачных вычислений на базе сети компьютеров частных пользователей // Научно-исследовательский институт многопроцессорных вычислительных систем Южного федерального университета: 2012, дата обращения 10 марта 2014. – [Электронный ресурс]. – Режим доступа: http://paco2012.ipu.ru/procdngs/C207.pdf.

3. Прохоров А.В., Пахнина Е.М. Мультиагентные технологии управления ресурсами в распределенных вычислительных средах // Национальный аэрокосмический университет им. Н.Е. Жуковского: 2013, дата обращения 20 марта 2014. – [Электронный ресурс]. – Режим доступа: http://hpc-ua.org/cc-13/files/proceedings/41.pdf.

4. Кузнецов К.О. Облачная мультиагентная платформа на основе JADE и Google App Engine: магистрская диссертация. Санкт-Петербургский Государственный Университет, Санкт-Петербург: 2013, дата обращения 20 марта 2014.

5. Чемеркин Ю.С. Безопасность публичных сред облачных вычислений в условиях функциональной неопределенности // T-Comm – Телекоммуникации и транспорт. – 2014. – №6. – С. 56-60.

6. Долбилов А.В., Литягин П.Е. Технология облачных вычислений // Мир телекома. – 2013. – №6. – С. 3-14.

7. NIST SP 500-292. NIST Cloud Computing Standards Roadmap 2010, National Institute of Standards and Technology, дата обращения 20 марта 2014. – [Электронный ресурс]. – Режим доступа: http://www.nist.gov.

8. OpenFOAM. – [Электронный ресурс]. – Режим доступа: http://openfoam.org.

9. Wilcox D.C. Turbulence Modeling for CFD. – California: DCW Industries, Inc, 1993. – 460 p.

10. Kulikovsky A.G. Mathematical problems of the numerical solution of hyperbolic systems of equations / A.G. Kulikovsky, N.V. Pogorelov, A.Yu. Semenov. – M.: Fizmatlit, 2001. – 656 p.

INFORMATION SECURITY OF DATABASES

S.G. Krasochkin, *Head of the Integration Development Group*
Xpath Company
(Russia, Moscow)

Abstract. *The development of information technology carries both positive and negative aspects. Regulation of information security is one of the directions of state policy. The information security of databases depends on 3 components: confidentiality, availability and integrity. The main approaches to protecting databases: the use of encryption; the use of a firewall (operating system firewall); the implementation of automatic database monitoring.*

Keywords: *information security, encryption, firewall (network database monitoring, AES and DES, Cron scheduler).*