Формализация модели мониторинга защищенности работы СУБД SQL

Воробьева Диана Евгеньевна

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

АННОТАЦИЯ

Введение: В 1976 году Харрисон, Руззо и Ульман доказали, что в самом общем случае вопрос определения безопасности компьютерной системы неразрешим. Иными словами, не существует алгоритма, позволяющего определить, будет ли компьютерная система безопасна или небезопасна в общем случае является вычислительно неразрешимой. Однако в частных случаях проблема безопасности решается, а именно, безопасными являются монотонные системы (не содержащие операции DROP и DELETE), системы, не содержащие операций CREATE, и моно-условные системы (запрос к которым содержит только одно условие). **Постановка задачи:** Для создания систем гарантированной защиты при работе с СУБД в АСУ проектирования кораблей требуется разработка таких методов ограничения функциональности автоматизированного рабочего места, которые исключили бы саму возможность хакерских действий со стороны внутренних нарушителей. **Методы:** методы синтеза программных систем защиты информации. **Результаты**: модель мониторинга защищенности работы базы данных. **Практическая значимость**: обеспечение безопасной работы СУБД SQL в условиях заранее неизвестных компьютерных атак. **Обсуждение**: новизна предложенной задачи состоит в том, что принцип мониторинга таких действий отличается от традиционно применяемых.

КЛЮЧЕВЫЕ СЛОВА: целостность баз данных; защита от атак внутреннего нарушителя; программная система; блокировка опасных действий.

Введение

Актуальность темы данной статьи обусловлена необходимостью защиты значимых объектов критической информационной инфраструктуры в условиях целенаправленных атак при отсутствии шаблонов безопасности для заранее неизвестных программно-технических воздействий на базы данных, используемые при проектировании кораблей.

Для оценки безопасности работы автоматизированного рабочего места с СУБД SQL может быть использована модель Take-Grant [1]. В качестве основных элементов модели используются граф доступа и правила его преобразования. В модели доминируют два правила: "давать" и "брать". Они играют в ней особую роль, переписывая правила, описывающие допустимые пути изменения графа. В общей сложности существует четыре правила преобразования: правило «брать», правило «давать», правило «создать» и правило «удалить». Используя эти правила, можно воспроизвести состояния, в которых будет находиться СУБД в зависимости от распределения и изменения прав доступа. Следовательно, можно проанализировать возможные угрозы для данной системы.

Степень разработанности темы

В настоящее время разработка систем мониторинга работы СУБД с точки зрения не системы разграничения доступа, а процессов происходящих в программно-аппаратной среде является достаточно малоисследованной задачей. Такие программы необходимы как для защиты серверов баз данных, так и для СУБД запускаемой на автоматизированных рабочих местах что накладывает определенные трудности на особенности их синтеза [2-5].

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

- Мониторинг компьютерных атак рассматривался в работах С.А.Петренко, К.Мак-Клар, Л.Стюарта, Джоэл Скембрей, Дж.Курца, И.Д.Медведовского, П.В.Семьянова, В.В. Платонова, но мониторинг компьютерных атак при взаимодействии с ГосСОПКа не описан в открытой литературе.
- Противодействие компьютерным атакам исследовано в работах С.А.Петренко, С.М.Климова, М.П.Сычева, А.В.Астахова, А.В.Лукацкого, А.Н.Лукашкина, но в них противодействие компьютерным атакам на СУБД описывается только с точки зрения криптографической защиты данных.
- Теория сетей Петри и моделирование систем подробно рассмотрена в работах Дж.Питерсона, но современных условиях требуется разработка моделей, адаптированных к определенным структурам и алгоритмам функционирования СУБД.

Мониторинг безопасности работы с базами данных

В формальную теорию защиты информации вводится понятие монитора безопасности. Концепция монитора безопасности обращений является достаточно естественной формализацией некого механизма, реализующего разграничение доступа в системе. Монитор безопасности обращений представляет собой фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах разграничения доступа [6-10]. Монитор безопасности обращений удовлетворяет следующим свойствам:

1. Ни один запрос на доступ субъекта к объекту не должен выполняться в обход монитора;

2. Работа монитора должна быть защищена от постороннего вмешательства;

3. Представление монитора должно быть достаточно простым для возможности верификации корректности его работы.

Несмотря на то, что концепция монитора безопасности обращений является абстракцией, перечисленные свойства справедливы и для программных или аппаратных модулей, реализующих функции монитора обращений в реальных системах.

Существуют операторы SQL предоставления и отмены привилегий. В стандарте SQL определены два оператора GRANT и REVOKE для предоставления и отмены привилегий соответственно [2].

Оператор предоставления привилегий имеет следующий формат:

GRANT {<список действий>|ALL PRIVILEGES} ON <имя объекта>

TO {<список пользователей>|PUBLIC} [WITH GRANT OPTION]

где <список действий> определяет набор действий из доступного списка действий над объектом данного типа (параметр ALL PRIVILEGES указывает, что разрешены все действия, допустимые для объектов данного типа), <имя объекта> определяет имя объекта защиты: таблицы, представления, хранимой процедуры или триггера, <список пользователей> определяет список идентификаторов пользователей, кому предоставляются данные привилегии. Вместо списка идентификаторов можно воспользоваться параметром PUBLIC. Параметр WITH GRANT OPTION является необязательным и определяет режим, при котором передаются не только права на указанные действия, но и право передавать эти права другим пользователям. Передавать права в этом случае пользователь может только в рамках разрешенных ему действий. В общем случае набор привилегий зависит от реализации СУБД (определяется производителем).

К достоинствам дискреционного разграничения доступа относятся относительно простая реализация (проверка прав доступа субъекта к объекту производится в момент открытия этого объекта в процессе субъекта), хорошая изученность, универсальность, наглядность и гибкость. Однако дискреционная защита является довольно слабой, так как привилегии существуют отдельно от данных и доступ ограничивается только к именованным объектам, а не собственно к хранящимся данным. В случае реляционной БД объектом будет, например, именованное отношение (таблица) [11-12]. В этом случае нельзя в полном объеме ограничить доступ только к части информации, хранящейся в таблице. Это связано с тем, что даже если ввести отдельный атрибут, который будет хранить информацию о метке конфиденциальности документа, то средствами SQL можно будет получить выборку данных без учета атрибута данной метки. Фактически это означает, что либо сам сервер баз данных должен предоставить более высокий уровень защиты информации, либо придется реализовать данный уровень защиты информации с помощью жесткого ограничения операций, которые пользователь может выполнить посредством SQL. На некотором уровне такое разграничение можно реализовать с помощью хранимых процедур, но не полностью - в том смысле, что само ядро СУБД позволяет разорвать связь «защищаемый объект - метка конфиденциальности». Дискреционное разграничение доступа имеет ряд и других недостатков. Перечислим все недостатки дискреционной модели в виде списка:

1. Хранение привилегий доступа отдельно от данных;

2. Ограничение доступа производится на уровне именованных объектов, а не самих хранящихся данных;

3. Уязвимость по отношению к вредоносным программам вида Троянских коней. Дискреционная модель позволяет пользователям без ограничений передавать свои права другим пользователям (что и используется Троянскими конями). Нет различия между пользователем и субъектом, т.е. между человеком, кому, в конечном счете, были назначены определенные права доступа к объектам и процессам, порожденным данным пользователем. Это также позволяет Троянским коням, запущенным от имени авторизованных пользователей, получать свободный доступ к данным.

4. Статичность разграничения доступа — права доступа к уже открытому объекту в дальнейшем не изменяются независимо от изменения состояния компьютерной системы;

5. Отсутствие средств защиты от утечки конфиденциальной информации. Иначе говоря, дискреционное разграничение доступа не обеспечивает возможность проверки, не приведет ли разрешение доступа к объекту для некоторого субъекта к нарушению безопасности информации в компьютерной системе;

6. Средства защиты не позволяют отследить передачу секретных материалов;

7. Возможность множественного назначения и отзыва привилегий доступа к одному и тому же объекту может привести к неконтролируемому доступу к данным. Предположим, субъект s1 предоставил определенные права доступа к объекту o1 субъекту s2. Затем субъект s3 предоставил те же привилегии к o1 все тому же субъекту s2, будучи не поставленным в известность, что это уже было сделано субъектом s1. Позднее субъект s3 изменил свое мнение и отозвал предоставленные им привилегии. Но его действие не вызвало желаемый эффект, поскольку отозванные им привилегии по-прежнему остаются в матрице доступа, поскольку они были ранее назначены субъектом s1;

8. При большом количестве пользователей трудно отследить все пути доступа [13].

Дискреционная модель является очень популярной у разработчиков СУБД. Она реализована в практически всех SQL-совместимых СУБД. Операторы SQL GRANT, REVOKE, DENY, реализующие дискреционную модель разграничения доступа, определены в стандарте языка SQL.

К основным характеристикам мандатного (обязательного) подхода разграничения доступа относятся следующие положения [14]:

- все субъекты и объекты должны быть однозначно идентифицированы;
- имеется линейно упорядоченный набор меток конфиденциальности (секретности) и соответствующих им уровней (степеней) допуска (нулевая метка или степень соответствуют общедоступному объекту и степени допуска к работе только с общедоступными объектами), например: U - Unclassified, SU – Sensitive but unclassified, S – Secret, TS – Top secret;
- каждому объекту присвоена метка конфиденциальности;
- каждому субъекту присваивается степень допуска;
- право на чтение информации из объекта получает только тот субъект, чья степень допуска не меньше метки конфиденциальности данного объекта;
- право на запись информации в объект получает только тот субъект, чей уровень конфиденциальности не больше метки конфиденциальности данного объекта. Это означает также, что всякая информация, записанная некоторым субъектом, автоматически получает уровень классификации, равный уровню допуска этого субъекта;

- в процессе своего существования каждый субъект имеет свой уровень конфиденциальности, равный максимуму из меток конфиденциальности объектов, к которым данный субъект получил доступ.

Мандатный подход используется специальными системами, предназначенными для государственных, военных и других организаций с жёсткой структурой. Основной целью мандатного разграничения доступа к объектам является предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности (противодействие созданию каналов передачи информации «сверху вниз»).

Для мандатного разграничения доступа к объектам компьютерной системы формально доказано следующее важное утверждение (принципиально отличающее MAC от DAC): если начальное состояние компьютерной системы безопасно и все переходы из одного состояния системы в другое не нарушают правил разграничения доступа, то любое последующее состояние компьютерной системы также безопасно. К другим достоинствам мандатного разграничения доступа относятся:

- более высокая надежность работы системы, так как при разграничении доступа к объектам контролируется и состояние самой системы, а не только соблюдение установленных правил;
- большая простота определения правил разграничения доступа по сравнению с дискреционным разграничением.

Главное отличие MAC от DAC состоит в том, что в MAC метки конфиденциальности неизменны на всем протяжении существования объекта защиты (они создаются и уничтожаются только вместе с ним) и располагаются вместе с защищаемыми данными, а не в системном каталоге, как это происходит в DAC [15-16]. Другим важным отличием является то, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение). Мандатный принцип построения системы разграничения доступа в СУБД реализует многоуровневую модель безопасности данных, называемую еще моделью Белл – ЛаПадула.

В данной модели устанавливаются и поддерживаются два основных ограничения политики безопасности:

1. Простое правило безопасности (Simple Security), реализующее запрет чтения вверх (No Read Up — NRU);
2. *-свойство (star-property), реализующее запрет записи вниз (No Write Down - NWD).

Ограничение NRU является логическим следствием мандатного принципа разграничения доступа, запрещая субъектам читать данные из объектов более высокой степени секретности, чем позволяет их допуск.

Ограничение NWD предотвращает перенос (утечку) конфиденциальной информации путем ее копирования из объектов с высоким уровнем конфиденциальности в неконфиденциальные объекты или в объекты с меньшим уровнем конфиденциальности.

Ограничения NRU и NWD приводят к тому, что по разным типам доступа (чтение, запись, создание, удаление) в модели Белл - ЛаПадула устанавливается разный порядок доступа конкретного субъекта к объектам. В частности, по типу доступа

«создание» субъект с низшим уровнем допуска имеет возможность создавать объекты (записи) в объектах более высокого уровня конфиденциальности. Такой подход, тем не менее, отражает реальные ситуации, когда служащий отдела кадров может порождать первичные документы личных дел новых сотрудников, но при этом не имеет собственно самого доступа к этим документам по другим типам операций (чтение, удаление, изменение).

Ключевым понятием в модели Белла и ЛаПадулла является понятие решетки безопасности (security lattice). Математически, решеткой безопасности называется алгебраическая система, состоящая из оператора, определяющего отношение порядка (dominance) для уровней секретности и операторов наименьшей верхней и наибольшей нижней границ.

Отношение порядка обладает свойствами рефлективности (разрешены потоки информации между субъектами и объектами одного уровня секретности) и транзитивности (если информация может передаваться от субъектов и объектов уровня A к субъектам и объектам уровня B и от субъектов и объектов уровня B к субъектам и объектам уровня C, то она может передаваться от субъектов и объектов уровня A к субъектам и объектам уровня C). Операторы наименьшей и наибольшей границ определяются таким образом, чтобы для каждой пары уровней секретности существовал единственный элемент наименьшей верхней границы и единственный элемент наибольшей нижней границы [17-18].

Математическая формализация модели позволяет сформулировать основные положения безопасности системы и по возможности строго доказать их. Состояние системы называется безопасным по чтению (или simple-безопасным), если для каждого субъекта, осуществляющего в этом состоянии доступ по чтению к объекту, уровень доступа субъекта доминирует над уровнем секретности объекта. Состояние системы называется безопасным по записи (или *-безопасным), если для каждого субъекта, осуществляющего в этом состоянии доступ по записи к объекту, уровень секретности объекта доминирует над уровнем доступа субъекта. Состояние системы называется безопасным, если оно безопасно по чтению и по записи и наконец, система называется безопасной, если начальное и все последующие состояния безопасны. Как уже упоминалось, в рамках данной модели доказано важное утверждение, если начальное состояние системы безопасно и все переходы из одного состояния системы в другое не нарушают правил разграничения доступа, то любое последующее состояние системы также безопасно, что позволяет применять мандатную модель в системах с высоким уровнем секретности.

Отметим и недостатки мандатного разграничения доступа:

- невозможность автоматизации назначения уровней секретности и определения границ защищаемых данных, что в больших системах может приводить к практически бесконечному ручному процессу конфигурации системы;
- снижение эффективности работы компьютерной системы, так как проверка прав доступа субъекта к объекту выполняется не только при открытии объекта в процессе субъекта, но и перед выполнением любой операции чтения из объекта или записи в объект;
- создание дополнительных неудобств в работе пользователей компьютерной системы, связанных с невозможностью изменения информации в неконфиденциальном объекте, если тот же самый процесс использует информацию из конфиденциального

объекта (его уровень конфиденциальности больше нуля). Это зачастую решается путем разрешения пользователю выступать от имени субъекта с меньшим уровнем доступа, что в свою очередь приводит к деградации системы защиты;

- пользователь нижнего уровня имеет право записи в объекты всех уровней, таким образом этот пользователь может переписать существующий объект, что равносильно его удалению. Для устранения этого недостатка второе правило изменяется так, что пользователь имеет доступ на запись только на своем уровне.

Из-за отмеченных недостатков мандатного разграничения доступа в реальных СУБД множество объектов, к которым применяется мандатное разграничение, является подмножеством множества объектов, доступ к которым осуществляется на основе дискреционного разграничения. В целях уменьшения негативных последствий ограничения NWD в систему вводят привилегированного пользователя, имеющего специальные полномочия на удаление любого объекта системы и понижения метки конфиденциальности. Имеются также расширения мандатной модели, adapted mandatory access model и др., некоторым образом снимающие недостатки MAC [19].

Примером реализации мандатного подхода разграничения доступа можно считать компонент Oracle Label Security (OLS), реализованный в СУБД Oracle, начиная с 9i версии. Примером Российской СУБД, реализующей стандарт SQL-92 является СУБД ЛИНТЕР.

Обеспечение целостности данных

Под целостностью данных понимают соответствие информационной модели предметной области, т.е. данных, хранимых в базе данных, объектам реального мира и их взаимосвязям в каждый момент времени. Любое изменение в предметной области, значимое для построенной модели, должно отражаться в базе данных, и при этом должна сохраняться однозначная интерпретация информационной модели в терминах предметной области. Целостность БД не гарантирует достоверности содержащейся в ней информации, но обеспечивает по крайней мере правдоподобность этой информации, отвергая заведомо невероятные, невозможные значения. Таким образом, не следует путать целостность БД с достоверностью данных. Достоверность (или истинность) есть соответствие фактов, хранящихся в БД, реальному миру. Контроль целостности данных это способность СУБД или КС в целом обеспечить неизменность данных (данные, хранящиеся в системе, не отличаются в семантическом отношении от данных в исходных документах) в условиях случайного и (или) преднамеренного искажения (разрушения) или, иначе, под целостностью данных подразумевает отсутствие ненадлежащих изменений.

Понятие «ненадлежащее изменение» введено Д. Кларком и Д. Вильсоном: ни одному пользователю КС, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю. В работах Кларка и Вильсона определены девять абстрактных теоретических принципов, выполнение которых позволит обеспечить целостность данных:

- корректность транзакций;
- авторизация пользователей;
- минимизация привилегий;
- разграничение функциональных обязанностей;
- аудит произошедших событий;

- объективный контроль;
- управление передачей привилегий;
- эффективное применение механизмов защиты;
- простота использования защитных механизмов.

По первому принципу данные могут изменяться только посредством «корректных» транзакций. Прямое (произвольным образом) изменение данных не допускается. В свою очередь корректность транзакций должна быть некоторым способом доказана. Второй принцип гласит, что изменение данных может осуществляться только авторизованными пользователями, имеющими определенные привилегии. Минимальность привилегий подразумевает, что пользователи (в конечном счете, субъекты) должны быть наделены теми и только теми привилегиями, которые минимально необходимы для выполнения тех или иных действий. Аудит произошедших событий (включая возможность восстановления полной картины происшедшего) является превентивной мерой в отношении потенциальных нарушителей и позволяет восстановить данные в случае их повреждения.

Разграничение функциональных обязанностей подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный с точки зрения целостности процесс, необходимо участие различных пользователей. Этим гарантируется, что один пользователь не может выполнить весь процесс целиком (или даже две его стадии) с тем, чтобы нарушить целостность данных. Принцип объективного контроля также является одним из краеугольных камней политики контроля целостности. Суть данного принципа заключается в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей. В связи с этим Кларк и Вильсон указывают на необходимость регулярных проверок, целью которых является выявление возможных несоответствий между защищаемыми данными и объективной реальностью, которую они отражают.

Управление передачей привилегий необходимо для эффективной работы всей политики безопасности. Если схема назначения привилегий неадекватно отражает организационную структуру предприятия или не позволяет администраторам безопасности гибко манипулировать ею для обеспечения эффективности производственной деятельности, защита становится тяжким бременем и провоцирует попытки обойти ее там, где она мешает «нормальной» работе. В основу восьмого принципа контроля целостности заложен ряд идей, призванных обеспечить эффективное применение имеющихся механизмов обеспечения безопасности. На практике зачастую оказывается, что предусмотренные в системе механизмы безопасности или некорректно используются, или полностью игнорируются системными администраторами. Простота использования защитных механизмов подразумевает, что самый безопасный путь эксплуатации системы будет также наиболее простым, и наоборот, самый простой - наиболее защищенным.

На практике наиболее часто употребляются две модели обеспечения целостности данных, модель целостности Кларка-Вильсона и модель Биба [20]. Поскольку в АСУ проектирования кораблей используется мандатная модель, будем рассматривать в дальнейшем только модель Биба.

Модель Биба была разработана в 1977 году как модификация модели Белла-ЛаПадулы, ориентированная на обеспечение целостности данных. Аналогично модели

Белла-ЛаПадулы, модель Биба использует решётку классов безопасности, трактуемых в ней как решетку классов целостности.

Базовые правила модели Биба формулируются следующим образом:

1. Простое правило целостности (Simple Integrity, SI). Субъект с уровнем целостности XS может читать информацию из объекта с уровнем целостности XO тогда и только тогда, когда XO преобладает над XS.

2. * - свойство (star-integrity). Субъект с уровнем целостности XS может писать информацию в объект с уровнем целостности XO тогда и только тогда, когда XS преобладает над XO.

Для первого правила существует мнемоническое обозначение No Read Down (NRD) - доступ на чтение дается, если уровень целостности (безопасности) объекта не ниже (а также включает в себя) уровень целостности (безопасности) субъекта, а для второго No Write Up (NWU) - доступ на запись дается, если уровень целостности (безопасности) субъекта не выше (а также включает в себя) уровня целостности (безопасности) объекта. Следовательно, состояние системы будет целостным тогда и только тогда, когда оно безопасно по чтению и записи.

Отдельного комментария заслуживает вопрос, что именно понимается в модели Биба под уровнями целостности. Действительно, в большинстве приложений целостность данных рассматривается как некое свойство, которое либо сохраняется, либо не сохраняется – и введение иерархических уровней целостности может представляться излишним. В действительности уровни целостности в модели Биба стоит рассматривать как уровни достоверности, а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот. То есть, модель Биба основывается на следующих допущениях: чем выше уровень безопасности объекта, тем выше его достоверность и чем выше уровень безопасности субъекта, тем более достоверную информацию он может вносить в систему.

Формальное описание модели Биба полностью аналогично описанию модели Белла-ЛаПадулы. К достоинствам модели Биба следует отнести её простоту, а также использование хорошо изученного математического аппарата. В то же время модель сохраняет все недостатки, присущие модели Белла-ЛаПадулы.

Выводы

При создании перспективных систем защиты среды работы СУБД на автоматизированных рабочих местах и серверах базы данных должны быть сняты ограничения существующих методов защиты [3]. Перечислим данные ограничения:

1. не рассматриваются вопросы сопряжения с ГосСОПКа;

2. не проработаны вопросы анализа СОВ запросов к базам данных, не разработаны шаблоны;

3. нет теории и нормативно-методического аппарата анализа защищенности БД от целенаправленных воздействий;

4. существует только общая теория для информационных систем в целом;

5. нет модели защищенной обработки транзакций в БД;

6. существующие модели и механизмы управления безопасностью нацелены только на защиту данных;

7. существующие критерии эффективности не учитывают целенаправленных воздействий;

8. мониторинг компьютерных атак при взаимодействии с ГосСОПКа не описан в открытой литературе;

9. противодействие компьютерным атакам на СУБД описывается только с точки зрения криптографической защиты данных;

10. требуется разработка моделей адаптированных к определенным структурам и алгоритмам функционирования СУБД.

Таким образом, выявлено 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.

Для создания эффективной системы мониторинга требуется модернизация модели Биба путем введения правила «Без мандата нет изменения правил (грамматик) исполнения со всех уровней для внешнего поступления кода».

Это означает необходимость блокирования как системных так и прикладных процессов которые не могут быть проконтролированы из запускаемой СУБД. А поскольку даже в защищенной отечественной СУБД «Линтер-ВС» такой механизм не реализован, для универсализации применения стоит ввести данный механизм защиты среды выполнения прикладных процессов ввести в операционную систему.

Заключение

Таким образом, мониторинг защищенности работы СУБД SQL в АСУ проектирования корабля с одной стороны должен обеспечиваться за счет системы разграничения доступа с точки зрения отслеживания доступа оператора к объектам защиты, а с другой стороны, должна быть реализована система блокирования опасной функциональности работающая на модифицированной в сторону ужесточения правил модели Биба.

Система мониторинга должна также фиксировать попытки запуска параллельно с работой СУБД неавторизованных процессов для передачи на дальнейший анализ в испытательные лаборатории ФСТЭК на выявление не декларируемых возможностей в выявленных исполнимых файлах.

Разработанная автором статьи программная модель системы защиты была предложена к реализации в виде программного комплекса, который должен также обеспечивать защиту работы СУБД в случае наличия закладок в операционной системе или хакерских действий по сети с удаленного компьютера по отношению к рабочему месту в интересах проекта Сейфнет НТИ РФ и апробирована на площадке киберполигона ИТЦ «Ингрия» (Санкт-Петербург) в 2022 году. Применение предложенной технологии защиты позволяет сделать следующий шаг к требуемым системам безопасности значимых объектов критической информационной инфраструктуры.

Литература

1. *Скакун В.В.* Защита информации в базах данных и экспертных системах. Минск: БГУ, 2018. 140 с.

2. *Воробьев Е.Г., Воробьева Д.Е.* Безопасное функционирование инфраструктуры телерадиовещания в аспекте влияния на цифровую экономику//«Защита информации. Инсайд». 2023. №1. С.2-6.

3. *Воробьев Е.Г., Воробьева Д.Е.* Модели оценки киберустойчивости транзакций в СУБД // «Защита информации. Инсайд». 2022. №6. С.67-70.

4. *Ефремов Н. А. Мужжавлева Т. В.* Процессы информатизации экономики и информационная безопасность // Экономика и предпринимательство. 2023. № 3. С. 287-294.

5. *Иванов А.А.* Ключевые понятия системного подхода к адаптивному мониторингу информационной безопасности киберфизических систем // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) Екатеринбург, 2022. С. 17-20.

6. *Иванов М. Ю., Сыготина М. В., Вахрушева М. Ю., Надршин В. В.* Информационная безопасность современного предприятия: парольная защита // Защита информации. Инсайд. 2022. № 6. С. 62-66.

7. *Смирнов С.И., Киселев А.Н., Азерский В.Д.* Комплексная методика проведения расследования инцидента информационной безопасности // Защита информации. Инсайд. 2023. № 2. С. 14-26.

8. *Коноплева Л. А*. Гуманитарные аспекты информационной безопасности. М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2022. 162 с.

9. *Красинский В.В., Машко В. В.* Кибертерроризм: криминологическая характеристика и квалификация. Государство и право. 2023. № 1. С. 79-91.

10. *Полтавцева М.А., Ворошин Е. А.* Комплексное организационное обеспечение управления информационной безопасностью субъекта КИИ // Защита информации. Инсайд. 2023. № 2. С. 7-13.

11. Information security is information risk management / Bob Blakley, Ellen McDermott, Dan Geer // Proceedings of the 2001 workshop on New security paradigms. N. Y. : ACM, 2018. Pp. 97-104. ISBN 1-58113-457-6.

12. *Anderson, J. M.* Why we need a new definition of information security // Computers & Security. 2019. Vol. 22, No. 4. Pp. 308–313. doi:10.1016/S0167-4048(03)00407-3.

13. *Venter, H. S.* A taxonomy for information security technologies / H. S. Venter, J. H. P. Eloff // Computers & Security. 2019. Vol. 22, No. 4. Pp. 299–307. doi:10.1016/S0167-4048(03)00406-1.

14. Chapter 24 : A History of Internet Security / De Nardis, L. // The History of Information Security : A Comprehensive Handbook / edited by de Leeuw, K. M. M. and Bergstra, J.. Elsevier, 2021. ISBN 9780080550589.

15. *Cherdantseva, Y.* Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals // Organizational, Legal, and Technological Dimensions of Information System Administrator / Y. Cherdantseva, J. Hilton. IGI Global Publishing, 2020.

16. *Saltzer, H. Saltzer*. The Protection of Information in Computer Systems : [англ.] / H. Saltzer Saltzer, Michael D. Schroeder // Proceedings of the IEEE. USA : IEEE, 2020. Vol. 63, No. 09 (September). Pp. 1278—1308. ISSN 1558-2256.

17. *Hughes, J.* Quantitative Metrics and Risk Assessment : The Three Tenets Model of Cybersecurity : [англ.] / *J. Hughes, G. Cybenko* // Technology Innovation Management Review. Ottawa, Canada : Talent First Network (Carleton University), 2022. August. Pp. 15-24. ISSN 1927-0321.

18. *McCullagh, Adrian*. Non-Repudiation in the Digital Environment : [англ.] / Adrian McCullagh, William Caelli // Technology Innovation Management Review. Chicago, USA : First Monday, 2020. Vol. 8, No. 8 (August). ISSN 1396-0466.

19. NIST Interagency or Internal Report 7298 : Glossary of Key Information Security Terms : [англ.] / Richard L. Kissel, editor, Computer Security Division, Information Technology

Laboratory. Revision 2. Gaithersburg, MD, USA : National Institute of Standards and Technology, 2018. 222 p.

20. NIST Special Publication 800-14 : Generally Accepted Principles and Practices for Securing Information Technology Systems : [англ.]. Gaithersburg, MD, USA : National Institute of Standards and Technology, 2018. 61 p.

FORMALIZATION OF THE SQL DBMS SECURITY MONITORING MODEL

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

ABSTRACT

Introduction:: Introduction: In 1976, Harrison, Ruzzo, and Ullman proved that in the most general case, the question of determining the security of a computer system is unsolvable. In other words, there is no algorithm to determine whether a computer system will be secure or insecure in the general case computationally unsolvable. However, in special cases, the security problem is solved, namely, monotonic systems (which do not contain DROP and DELETE operations), systems that do not contain CREATE operations, and mono-conditional systems (the request to which contains only one condition) are secure. **Problem Statement:** In order to create systems of guaranteed protection when working with DBMS in the ship design ICS, it is necessary to develop such methods for limiting the functionality of the automated workstation that would exclude the very possibility of hacker actions on the part of internal intruders. **Methods:** methods of synthesis of information security software systems**. Results**: a model for monitoring the security of the database. **Practical significance**: ensuring the safe operation of the SQL DBMS in the face of previously unknown computer attacks. **Discussion:** The novelty of the proposed task lies in the fact that the principle of monitoring such actions differs from the traditionally applied ones.

Keywords: database integrity; protection against attacks by an internal intruder; software system; blocking dangerous actions.

REFERENCES

1. Skakun V.V. Information protection in databases and expert systems: a manual for students of the faculty. Radiophysics and Comp. Technologies / V. In. Horse. Minsk: BGU, 2018. 140 p. (in Russian).
2. Vorobiev E.G., Vorobieva D.E. Safe Functioning of TV and Radio Broadcasting Infrastructure in the Aspect of Influence on the Digital Economy. Information security. Inside. 2023. №1. Pp.2-6.
3. Vorobiev E.G., Vorobieva D.E. Models for assessing cyber stability of transactions in DBMS. Information security. Inside. 2022. №6. Pp.67-70.
4. Efremov N. A., Muzhavleva T. V. Processes of Informatization of Economics and Information Security. 2023. № 3. Pp. 287-294.
5. Ivanov A.A. Klyuchnye ponyatiya sistemnogo podkhoda k adaptivnomu monitoringu informatsionnoy bezopasnosti cyberfizicheskikh sistem [Key concepts of system approach to adaptive monitoring of information security of cyberphysical systems] / A. A. Ivanov // Digital transformation of society and information security: materials of Vseross. Sci.-Prakt. Conf. (Yekaterinburg, May 18, 2022) - Yekaterinburg, 2022. Pp. 17-20.
6. Ivanov Yu., Sygotina M. V., Vakhrusheva M. Yu., Nadrshin V. V. Information Security of a Modern Enterprise = Information Security of Advanced Company: Password Protection: Password Protection. Inside. 2022. № 6. Pp. 62-66.
7. Smirnov S.I., Kiselev A.N., Azerskiy V.D. Information Protection. Inside. 2023. № 2. Pp. 14-26.
8. Konopleva L. A. Gumanitarnye aspekty informatsionnoy bezopasnosti [Humanitarian aspects of information security]. Textbook / L. A. Konopleva; M-vo nauki i vysshe. Education Ros. Federation, Urals. State Econ. Un-t. - Ekaterinburg: Ural Publishing House. State Econ. University, 2022. 162 p.
9. Krasinskiy V.V., Mashko V.V. Cyberterrorism: criminological characteristics and qualification = Cyberterrorism: criminological characteristics and qualification. Gosudarstvo i pravo. 2023. № 1. Pp. 79-91.
10. Poltavtseva M.A., Voroshin E.A. Kompleksnoe organizatsionnoe obespechenie upravleniya informatsionnogo bezopasnosti sub'ekta CII = Comprehensive Organizational Support for Information Security Management of the CII Subject [Comprehensive Organizational Support for Information Security Management of the CII Subject]. Inside. 2023. № 2. Pp. 7-13.
11. Information security is information risk management / Bob Blakley, Ellen McDermott, Dan Geer . Proceedings of the 2001 workshop on New security paradigms. N. Y. : ACM, 2018. P. 97-104. ISBN 1-58113-457-6.
12. Anderson, J. M. Why we need a new definition of information security. Computers & Security. 2019. Vol. 22, No. 4. Pp. 308-313. doi:10.1016/S0167-4048(03)00407-3.
13. Venter, H. S. A taxonomy for information security technologies. Computers & Security. 2019. Vol. 22, No. 4. Pp. 299-307. doi:10.1016/S0167-4048(03)00406-1.
14. Chapter 24 : A History of Internet Security / De Nardis, L. // The History of Information Security : A Comprehensive Handbook / edited by de Leeuw, K. M. M. and Bergstra, J.. Elsevier, 2021. ISBN 9780080550589.
15. Cherdantseva, Y. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals // Organizational, Legal, and Technological Dimensions of Information System Administrator / Y. Cherdantseva, J. Hilton. IGI Global Publishing, 2020.
16. Saltzer, H. Saltzer. The Protection of Information in Computer Systems / H. Saltzer Saltzer, Michael D. Schroeder // Proceedings of the IEEE. USA : IEEE, 2020. Vol. 63, no. 09 (September). P. 1278-1308. ISSN 1558-2256.
17. Hughes, J. Quantitative Metrics and Risk Assessment : The Three Tenets Model of Cybersecurity : / J. Hughes, G. Cybenko // Technology Innovation Management Review. Ottawa, Canada : Talent First Network (Carleton University), 2022. August. Pp. 15-24. ISSN 1927-0321.
18. McCullagh, Adrian. Non-Repudiation in the Digital Environment : / Adrian McCullagh, William Caelli // Technology Innovation Management Review. Chicago, USA : First Monday, 2020. Vol. 8, No. 8 (August). ISSN 1396-0466.

19. NIST Interagency or Internal Report 7298 : Glossary of Key Information Security Terms : / Richard L. Kissel, editor, Computer Security Division, Information Technology Laboratory. Revision 2. Gaithersburg, MD, USA : National Institute of Standards and Technology, 2018. 222 p.
20. NIST Special Publication 800-14 : Generally Accepted Principles and Practices for Securing Information Technology Systems : Gaithersburg, MD, USA : National Institute of Standards and Technology, 2018. 61 p.