novosadtatty@gmail.com; *к.ф.-м.н., доцент,* ***Осипов М.Н.****, osipov@samsu.ru - кафедра безопасности информационных систем Самарского государственного университета*

**УДК 519.25; 004.8**

# ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ ПАТЕНТНОЙ ИНФОРМАЦИИ

А.Ю. Исхаков, В.И. Карнышев, Е.Ю. Костюченко, Р.В. Мещеряков, А.О.Шумская

В работе проводится описание методов защиты программного обеспечения, реализующего поиск, накопление информации из общедоступных патентных и справочно-информационных баз данных. Предлагается разграничение прав доступа как к данным, так и к выполняемым операциям. Особенность системы – рост уровня конфиденциальности при накоплении и сопоставлении информации.

**Ключевые слова:** защита информации; информационная безопасность, патентная информация

**Актуальность**

Научно-техническое прогнозирование является одной из актуальных задач в современном мире. При наличии значительного объема данных и грамотной аналитической работе появляется возможность проводить оценку перспективности работ и технологий.[1]

Вместе с тем, как правило, разнородные данные имеют более низкий уровень конфиденциальности, нежели данные с упорядоченной структурой без избыточной информации.

В ТУСУРе ведется работа по созданию технологии интеллектуального анализа и прогноза патентной и реферативной информации зарубежных электронных ресурсов на основе формируемых баз данных[2].Данная технология легла в основу разрабатываемого специализированного программного обеспечения.

**Конфиденциальность информации**

В рассматриваемом программном обеспечении циркулирует информация, которая в том числе относится к персональным данным. Согласно Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных», принятому ГД ФС РФ 08.07.2006, под персональными данными понимается «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

Перед выполнением классификации информационной системы необходимо определить категорию обрабатываемых данных.

Разработанное программное обеспечение позволяет обрабатывать информацию о патентах, информационных ресурсах, статьях, рефератах, книгах, персональные данные, позволяющие идентифицировать автора работы, таким образом включает как общедоступные сведения, так и конфиденциальную информацию [3].

При составлении частной модели угроз можно воспользоваться базовой моделью угроз согласно нормативно-методическим рекомендациям ФСТЭК России и ФСБ России. По результатам категорирования данных и составления модели угроз для системы, она может быть отнесена к одному из четырех классов.

Необходимо рассмотреть разработанное программное обеспечение на предмет отсутствия недекларированных возможностей в соответствие с руководящим документом Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (далее по тексту – НДВ)» №114 от 04.06.1999 г. Данный РД НДВ устанавливает четыре уровня контроля программного обеспечения, которые отличаются глубиной, объемом и условиями проведения испытаний. Наличие нескольких уровней контроля при проведении испытаний на отсутствие НДВ, с одной стороны, регламентирует степень конфиденциальности информации, защита которой осуществляется с помощью программного обеспечения, проверенного по тому или иному уровню. С другой стороны, разные условия контроля позволяют дифференцировать степень вероятности отсутствия в исследуемом программном обеспечении недекларированных возможностей.

Самый низкий уровень контроля, установленный в рассматриваемом РД, четвертый. Данный уровень предусматривает про-

верку программного обеспечения, используемого при защите, обработке, хранении, передаче конфиденциальной информации. Именно этот уровень является актуальным при рассмотрении разработанного программного обеспечения с точки зрения отсутствия НДВ. Для проверки программного обеспечения на отсутствие недекларированных возможностей, необходимо разработать следующий пакет документов:

- спецификация программного обеспечения по ГОСТ 19.202-78;

- описание программного обеспечения по ГОСТ 19.402 – 78;

- описание применения по ГОСТ 19.502-78;

- тексты программ, входящих в состав программного обеспечения по ГОСТ 19.401-78;

- руководство пользователя.

**Организационное обеспечение информационной безопасности**

Организационный элемент системы защиты информации должен включать в себя меры управленческого, ограничительного и технологического характера, которые определяют содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации научного учреждения. [3]

Применение разработанного программного продукта предполагает обязательное наличие нескольких из следующих факторов организационного обеспечения информационной безопасности:

- организация пропускного режима в здание (-я) и помещения, где находится система. Предполагает наличие у сотрудников пропусков, идентифицирующих владельца. Пропуска должны проверяться охранником или администратором, обеспечивающим доступ в помещения учреждения, и/или с помощью автоматизированной системы;

- обязательное разграничение доступа персонала и клиентов непосредственно в помещения, в которых хранится защищаемая информация. Сотрудник, имеющий право доступа к данной информации, должен иметь при себе ключ от данного помещения;

- наличие систем безопасности на территории объекта, в здании; охрана оборудования и персонала учреждения;

- наличие подразделения организации, регламентирующего организационные вопросы защиты компьютеров, информационных систем, локальных сетей.

**Вопросы программного обеспечения информационной безопасности**

Разграничение доступа к данным

Для реализации возможности разграничение прав администраторов и пользователей БД в MySQLAdministrator существует интерфейс для создания пользователей БД и наделения их необходимыми правами. Данный интерфейс представлен на рисунке 1

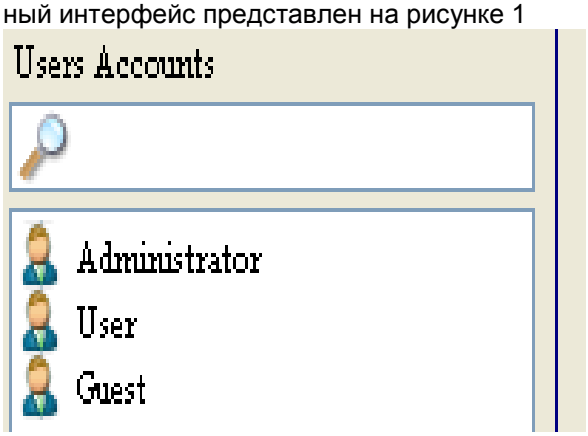


Рисунок 1 – Окно отображения созданных пользователей БД

При создании пользователей, каждому из них необходимо присвоить уникальный идентификатор и пароль.

Чтобы выдать права пользователям, необходимо определить перечень разрешенных действий. Для этих целей будет использоваться разграничительная политика управления доступом. Основной идеей такого подхода является определение типа доступа каждого субъекта к каждому объекту путём недвусмысленного перечисления для каждой пары субъект – объект типов доступа. На рисунке 2 представлен общий принцип работы системы при использовании дискреционной политики безопасности.

Представим в таблице 1 матрицу доступа пользователей к разработанной базе данных.

Таблица 1 – Матрица доступа пользователей к БД

| | Administrator | User | Guest |
|---|---|---|---|
| TLA | r w d m | r w m | r |

В таблице 1 использованы следующие сокращения:

- r (read) – право на чтение данных;
- w (write)- право на запись информации;
- d (delete) – право на удаление;
- m (modify) – право на модификацию данных.

Использование разграничительной политики безопасности не является достаточным условием обеспечения сохранности данных, но является неотъемлемым элементом программного обеспечения информационной безопасности.

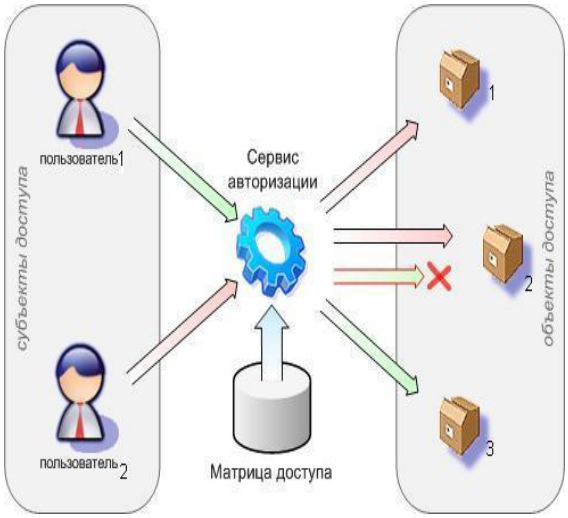


Рисунок 2 – Принцип работы дискреционного управления доступом

**Защита от повторного запуска копии программы**

Следующим элементом обеспечения информационной безопасности с помощью программных средств является ограничение числа запускаемых копий программы на локальной машине до одной. Такая мера позволит противодействовать возникновению следующих ситуаций:

- отказ в обслуживании;
- случайные ошибки при работе пользователей.

Отказ в обслуживании может быть вызван действиями злоумышленника, получившего удаленный доступ к управлению системой. Также, данная ситуация может быть вызвана вирусом, который злоумышленник может передать пользователям на съемном носителе или же внедрить его в систему каким-либо другим способом.

Сам по себе запуск нескольких копий программы не влечёт за собой негативных последствий. Однако, при каждом запуске, происходит выделение операционной системой ресурсов для данного экземпляра приложения, что особенно критично при условии низких производственных характеристик компьютеров. Ресурсы могут довольно быстро быть исчерпаны, что приведет критическим ошибкам системы.

Второй случай характерен для случайного запуска пользователем нескольких копий программы..

Возможность контроля количества экземпляров приложения реализуется с помощью встроенных в операционную систему Windows механизмов разграничения доступа приложений к ресурсам. В частности, использован механизм мьютексов.

Мьютексы – это объекты ядра операционной системы, которые гарантируют потокам взаимоисключающий доступ к единственному ресурсу. Отсюда вытекает название этих объектов: mutex (mutualexclusion). В общем виде работу мьютексов можно представить следующим образом: при запуске приложения происходит создание мьютекса для конкретного экземпляра приложения. Далее, по дескриптору мьютекса проверяется, свободен ли поток с таким же идентификатором или нет. Если да, то происходит установка значения мьютекса в отличное от нуля значение, если нет, то пользователь получает соответствующее уведомление.

Реализованная возможность позволит оповестить пользователя об ошибочных действиях. Если это действие выполняет сторонняя программа или злоумышленник, уведомление послужит сигналом для легального пользователя о вероятных посторонних воздействиях на программное обеспечение.

**Проверка целостности файла дампирования базы данных**

В разработанном программном обеспечении присутствует возможность опционального создания резервной копии базы данных. Резервная копия создается с помощью специальной программы, входящей в состав СУБД MySQL. Поскольку файлы СУБД могут периодически обновляться (например, когда происходит переход на более новую версию СУБД), в разработанной программе предусмотрена возможность смены целевой директории СУБД.

Эта возможность является, с одной стороны, удобным средством создания дампа БД, с другой стороны, уязвимостью программного обеспечения. Злоумышленнику, в случае необходимости, не составит труда подменить файл дампирования СУБД своей программой, виру-

сом или же модифицированным файлом дампирования, который может автоматически пересылать копию БД злоумышленнику.

Для предотвращения такой подмены перед выполнением дампирования осуществляется контроль целостности файла путём взятия контрольной суммы и проверки с эталонным (исходным) значением.

В целях обеспечения необходимого уровня защищенности системы обработки данных патентной информации необходимо использовать подсистему авторизации [5,6].

**Выводы**

Несмотря на то, что способы и технологии защиты программного обеспечения имеют большую историю, существует необходимость развития систем узкого назначения, в которых конфиденциальность информации может изменяться в связи с различными алгоритмами обработки.

Работа поддержана грантом РФФИ 14-07-00449 «Создание технологии интеллектуального анализа и прогноза на основе формируемых специализированных баз данных патентной и реферативной информации зарубежных электронных ресурсов»

**СПИСОК ЛИТЕРАТУРЫ**

1. Доклад по результатам НИР в рамках комплекса работ по долгосрочному прогнозу важнейших направлений научно-технологического развития на период до 2030 года[Электронный ресурс] / Учреждение Российской академии наук Институт Народнохозяйственного прогнозирования Российской академии наук. – Электрон.дан. – М., [2011]. – Режим доступа: http://www.hse.ru/data/2012/02/02/1262749006/Доклад_ИНП%20РАН.pdf
2. Авдзейко, В.И.Анализ результатов конкурсов на выполнение НИОКТР [Текст] / В.И. Авдзейко [и др.] // Научное обозрение. – 2013. – № 2. – С. 310-323.
3. Мещеряков, Р.В. Методика оценки рисков при внедрении ERP-систем на предприятиях [Текст] / Р.В. Мещеряков, М.В. Савчук// Качество. Инновации. Образование. – 2012.– № 8 (87). – С. 61-64.
4. Сабанов, А.Г. Требования к системам аутентификации по уровням строгости [Текст] / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2-1. – С. 61-67.
5. Ходашинский, И.А. Технология усиленной аутентификации пользователей информационных процессов [Текст] / И.А. Ходашинский и др.] // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2011. – № 2-3. – С. 236-248.

*аспирант **Исхаков А.Ю.**, email: iay@security.tomsk.ru - каф. КИБЭВС ТУСУР; заведующий патентно-информационным отделом **Карнышев В.И.**, email: pio@main.tusur.ru – ТУСУР; доцент **Костюченко Е.Ю.**, email: key@keva.tusur.ru; профессор **Мещеряков Р.В.**, email: mrv@security.tomsk.ru; аспирант **Шумская А.О.**, email: shumskaya.ao@gmail.com - каф. КИБЭВС ТУСУР Томский государственный университет систем управления и радиоэлектроники*