Список літератури

1. *Сенюк И.А.* "Этот сложный жесткий диск".: - Науково-технічний журнал "Камуфляж", 2004 р. №5(19).
2. *Коженевский С.Р.* Безопасность хранения информации на жестких дисках.: - Зб. наук. праць НАН України, 2003 р. №4. – С. 67-84.
3. *Волощенко А.С., Остапенко Г.П.* Забезпечення збереженості даних в сучасних автоматизованих системах шляхом покращення фізичних властивостей накопичувачів інформації// Зб. наук. праць "Спеціальні телекомунікаційні системи та захист інформації".- № 1(10).– К.: ДССЗЗІ України.- 2005.– С.56-61.
4. *Шпак А.П., Куницкий Ю.А., Карбовский В.Л.* Кластерные и наноструктурные материалы. т.1.- К.: Академпериодика, 2001.- 588 с.

В статті розглядаються концептуальні підходи впровадження новітніх технологій до побудови комплексів технічного захисту інформації.
Ключові слова: новітні технології, захист інформації, електромагнітний екран.

В статье рассматриваются концептуальные подходы внедрения новейших технологий к построению комплексов технической защиты информации.
Ключевые слова: новейшие технологии, защита информации, электромагнитный экран.

The article discusses conceptual approaches to the introduction of new technologies to build complex technical information security.
Keywords: new technologies, information security, electromagnetic screen.

Надійшла 13.04.2010

УДК 004.621.3

Климентов В.В. (ООО «Парисет»),
Трощило А.С. (Институт радиоэлектроники АН Украины)

«ВИРТУАЛЬНЫЙ КЛЮЧ» КАК СРЕДСТВО ЗАЩИТЫ БАЗ ДАННЫХ

Введение

В современных условиях ссуществует необходимость быстрой и корректной обработки больших объемов информации автоматизированными системами (АС), что, в свою очередь, приводит к появлению проблемы чрезмерных сетевых нагрузок и защиты данных. Это обусловливается общими требованиями к организации, аппаратному и программному обеспечению, в частности, к системам управления базами данных (СУБД). При этом особую актуальность приобретает защищенность информации от негативных воздействий (хищения, видоизменения и т.д.) непосредственно в базах данных (БД) и СУБД. Поэтому проблема надежной защиты информации в автоматизированных системах обработки данных (АСОД) становится приоритетной.

Одним из вариантов решения данной проблемы может рассматриваться защита АСОД с помощью криптографических методов и средств. Анализ работ [1,2], посвященных оценке качества программных средств АСОД, позволяет применить практически весь набор характеристик и атрибутов стандарта ISO 9126 «Качество программных средств» для использования в составе требований к СУБД. По сути, они сводятся к возможности контроля изменений в состоянии базы данных и являются главным свойством всех мероприятий, направленных на соответствие требованиям.В исследованиях [3,4], посвященных анализу методов и средств защиты информации в АСОД, сделаны попытки измерить и описать качество защищенности информации обобщенно, трудоемкостью и временем, необходимыми для преодоления злоумышленниками системы защиты. При этом косвенным

показателем качества БД и СУБД может являться относительная доля вычислительных ресурсов, используемых непосредственно средствами защиты информации. [4] В работах [5,6] анализируются угрозы информационной безопасности БД и СУБД в [8,9], способы противодействия угрозам с использованием криптографических методов ЗИ.

Основная часть

Особенность ситуации состоит в том, что организации и компании сталкиваются с требованиями соблюдения законодательных норм по информационной безопасности (ИБ) и конфиденциальности данных, которые не определены и строго не нормированы. Большинство законодательных норм в области информационных технологий (ИТ) имеют расплывчатые формулировки. Поэтому специалисты по ЗИ вынуждены использовать дополнительные источники для интерпретации соответствующих руководств, например: Payment Card Industry's Data Security Standard (PCI DSS), ISO 17799 – Code of Practice for Information Security Management, Control Objectives for Information and related Technology (CobiT), IT Infrastructure Library (ITIL). Эти факты говорят о том, что в любых рекомендациях, связанных с проектированием, управлением и защитой БД, будут изложены только общие принципы или усредненные методики. Естественно, при таком разнообразии подходов к проблеме возникает вопрос о надежности системы ЗИ, особенно от пользователей, уполномоченных работать с данными по долгу службы. Традиционно защита осуществляется только на уровне клиент-серверного взаимодействия. Однако у серверного администратора и, возможно, у ряда сотрудников предприятия имеется прямой доступ к базе данных, которым может воспользоваться злоумышленник.

Изучив проблему утечки информации через лиц, имеющих официальный доступ к БД, специалисты Uncertainty of Data Breach Detection пришли к выводу, что факторы внутренних угроз преобладают над внешними. Так, руководители служб ЗИ, участвующих в опросах, причинами утечек информации назвали:

- халатность сотрудников - 75% опрошенных (следует учесть тот факт, что рассеянные или недисциплинированные сотрудники могут нанести ущерб, но действуют ненамеренно);
- действия специалистов "третьих" (аутсорсинговых) компаний, разделяющих доступ к конфиденциальной информации с заказчиком аутсорсинга - 42% опрошенных;
- злонамеренные действия сотрудников, использующих доступ к конфиденциальным данным в личных целях - 26% опрошенных.

Учитывая смещение акцентов в сторону внутренних угроз, необходимо рассмотреть цепь методологических предпосылок, приводящих к использованию криптографических методов ЗИ в АСОД.

1. Для надежной безопасности баз данных необходимо обеспечить:
- невозможность прочтения содержимого БД злоумышленником;
- защиту от несанкционированного изменения содержимого БД;
- защиту от несанкционированного доступа к данным;
- защиту на уровне сети;
- защиту на уровне рабочей станции;
- защиту на уровне сервера Клиент-сервер;
- защиту на уровне СУБД.

2. Вышеизложенные требования подразумевают применение:
- алгоритмов шифрации, обеспечивающих невозможность прочтения содержимого БД;
- алгоритмов определения целостности данных, обеспечивающих защиту от несанкционированного изменения информации в БД;
- алгоритмов распределения информации по различным базам;

• административных методов контроля, аудита и обеспечения защиты от несанкционированного доступа к данным.

3. Наиболее надежное и удобное решение обеспечения ЗИ - защита БД шифрованием. Применение этого решения обеспечивает:

• защиту от несанкционированного копирования содержимого БД (информация хранится в зашифрованном виде);

• реализацию алгоритмов шифрования и дешифрования полей БД Клиент-сервером;

• невозможность работы с содержимым БД без ключей шифрования в случае копирования.

К недостаткам данного решения можно отнести:

• снижение скорости работы системы из-за реализации функций шифрования и дешифрования;

• снижение скорости работы системы из-за реализации части операций над данными не на уровне СУБД, а на уровне Клиент-сервера.

Ввиду однозначного шифрования внешних ключей таблиц существует потенциальная угроза частичной расшифровки базы данных, что компенсируется внесением большого числа фиктивных записей. Качество защиты можно характеризовать величиной предотвращенного ущерба, возможного при проявлении дестабилизирующих факторов и реализации конкретных угроз безопасности, а также средним временем между возможными проявлениями угроз, преодолевающих защиту данных.

Целью данной публикации является ознакомление с новым подходом к созданию эффективной защиты АСОД на основе системы ЗИ с использованием «виртуального ключа», которая предполагает решение задачи защиты данных от злонамеренных действий пользователей, уполномоченных работать с ними по долгу службы.

По мнению авторов, наиболее рациональное решение достигается с помощью криптографических методов и средств [10,11] .

Для анализа возможных технических решений ЗИ в АСОД рассмотрим в качестве примера организацию БД, представленную на рис.1.

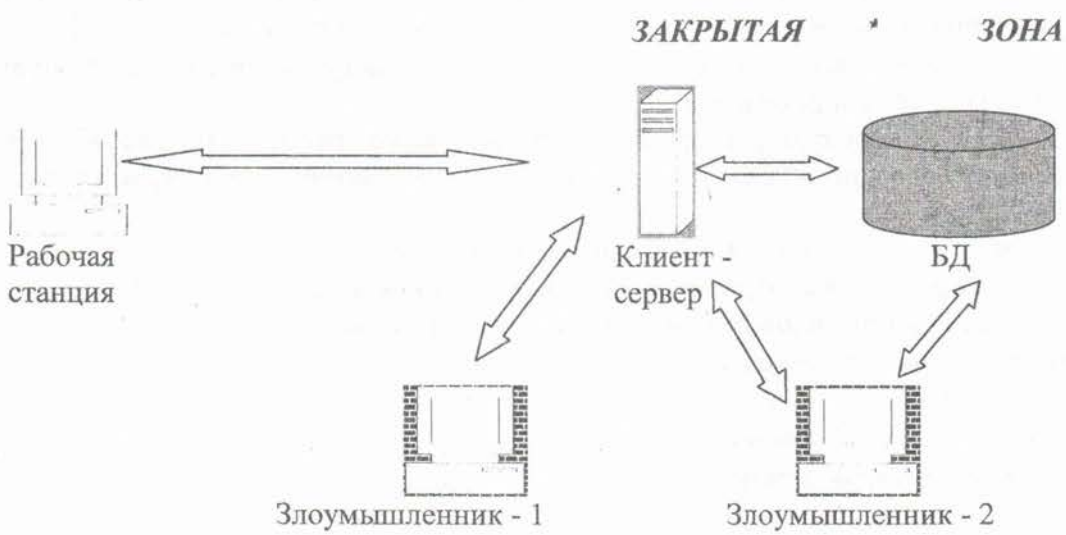

Рис. 1. Организация БД

Как видно из рисунка, сама информация - БД и система управления - СУБД находятся в зоне с ограниченным доступом («Закрытая зона»). «Злоумышленник - 1» (хакер или халатный сотрудник) имеет возможность атаки данных только со стороны «Рабочей

станции», причем халатный сотрудник сгенерирует незлонамеренную утечку, а хакер будет атаковать «Клиент-сервер», т.е. именно ту часть, которая традиционно достаточно хорошо защищена от внешних атак общеизвестными способами защиты. Из этого следует, что максимально возможный ущерб от злоумышленных действий «Злоумышленника – 1» составят:

- утечка или хищение какой-то части информации;
- вывод из строя Клиент-сервера, что приведет к работе БД в аварийном режиме.

«Злоумышленник - 2», имея доступ в «Закрытую зону», получает возможность:

- создать утечку;
- создать аварию;
- уничтожить, похитить, видоизменить информацию в БД;
- создать бреши в системе ЗИ, что позволит совершать злоумышленные действия в дальнейшем.

Вышеизложенное мотивирует следующие выводы:

1. Злоумышленные действия «Злоумышленника - 2» приведут к более тяжелым последствиям, чем аналогичные действия «Злоумышленника – 1»;

2. Наиболее рациональный способ противодействия «Злоумышленнику – 2» состоит в выводе его из «Закрытой зоны» в зону «Рабочей станции», что приведет к перераспределению тяжести угроз в сторону увеличения количества атакующих с внешней стороны. Основой такой защиты является регламент, аудит санкционирования доступа, а также контроль организации и эффективности ограничений доступа.

3. Способы противодействия не решают проблему инсайдера в полном объеме, т.к. к категории «Злоумышленник – 2» можно отнести пользователей с наиболее высоким уровнем доступа (владельцы, администраторы и т.д.).

4. Человеческий фактор - самое слабое звено в системе ЗИ, поэтому необходимо максимально автоматизировать систему защиты информации от внутренних атак на этапе проектирования АСОД.

Рассмотрим наиболее распространенные концепции ЗИ, используемые при проектировании информационных систем (ИС) для автоматизации защиты от внутренних атак.

Концепция сосредоточения всех полномочий доступа к данным в рамках одного программного модуля [11]. Суть ее заключается в построении универсального единственного канала (способа) доступа к системе с собственным форматом обмена, электронной цифровой подписью (ЭЦП) отправителя в каждом запросе на выполнение операции.

В программном модуле (ПМ) сосредоточены все полномочия доступа к БД, включая хранящийся в нем зашифрованный пароль суперпользователя, который создает доступ к закрытым таблицам и расшифровывается закрытым ключом- сертификатом владельца, загружаемым в оперативную память на этапе загрузки системы. ПМ является шлюзом в БД:

- ведет реестр сертификатов электронных подписей субъектов, осуществляющих доступ к БД с предустановленным сертификатом владельца;
- идентифицирует отправителей по их сертификатам и принимает решение о выполнении запроса;
- на этапе загрузки расставляются приоритеты и ограничения доступа согласно сертификатам пользователей БД по инструкциям владельца БД.

В связи с тем что пароль суперпользователя неизвестен ни одному из пользователей, хранится независимо от базы данных и генерируется на этапе первичной настройки, администратор не имеет приоритета по сравнению с другими пользователями системы, т.к доступ к системе осуществляется только через программный модуль.

Инструкции программному модулю, генерируемые администратором, можно разбить на две категории:

1. безопасные – подпрограммы с проведенным аудитом, для вызова которых администратор запрашивает наименование инструкции и передает только параметры вызова, но не сам код;

2. независимые – это код на языке управления БД в чистом виде, который ПМ пропускает через себя после уведомления владельца о необходимости выполнить независимую инструкцию (или требование его разрешения, то есть подписи), электронной подписи администратора под каждой такой инструкцией и записи в журнале выполненных инструкций, ведущемся на отдельном сервере. «Тогда в случае утечки можно будет найти виновника. Конечно, важно, чтобы страх злоумышленника от осознания этой неизбежности превалировал над утешением для владельца от его поимки после раскрытия информации» [11].

Концепция деления записей на части ориентирована на ЗИ содержания баз данных. Ее суть заключается в логическом делении записей на части таким образом, чтобы каждая из частей содержала только ту информацию, на основании которой было бы невозможно провести соответствие между частями записи, т.е. обеспечивается независимость с точки зрения идентификации. Разделенные части записей хранятся в разных таблицах или базах данных, разнесенных логически, физически или географически. Восстановление производится при помощи секретного реестра сопоставления, хранящего идентификаторы объединения частей записей, монопольный доступ к которому обеспечивает ПМ.

Концепция «шифрования на лету» в большей степени ориентирована на защиту хранилища данных. Суть ее заключается в санкционированном шифровании/ дешифровании всех данных, перед записью/чтением. При хищении хранилище или сервер не будут представлять интереса для злоумышленника, т.к. шифрование/дешифрование выполняется не средствами центрального процессора, а дополнительным криптоустройством. Считывание секретного ключа из оперативной памяти устройства должно быть настолько же трудоемкой задачей, насколько ценна информация в базе данных.

Концепция ограничения потока данных ориентирована на противодействие злоумышленным действиям рядового пользователя. Суть ее состоит в ограничении потока данных, передаваемых пользователю, по количественным или качественно-количественным критериям: ограничение по времени (запросы после окончания рабочего дня), количество информации в единицу времени, ограничение запросов по группам пользователей (группы адресов, от одного отдела, района, города) и т.п.

Система защиты информации (СЗИ) АСОД с «виртуальным ключом», разработанная авторами данной статьи, позволяет объединить достоинства всех четырех концепций. Она дает возможность, доработав уже существующую ИС, автоматизировать ЗИ и повысить надежность защиты любой АСОД при невысоких затратах.

Понятие «виртуальный ключ» базируется на Ноу-хау авторской позиции, в которой классическое понятие «ключ» наполняется новым содержанием: фактически функция ключа подменяется функциями алгоритма и синхронизации, уникальными для каждого сообщения, и позволяет зашифрованному сообщению попадать в канал с «ключом», приблизительно равным длине передаваемого файла[10]. Ключ, по сути, является виртуальным. Таким образом, появляется возможность создавать совершенно стойкие шифры, в соответствии с формулировкой Шеннона [4].

Краткое описание криптосистемы приведено ниже.

Назначение:

обмен конфиденциальной информацией (аудио, видео, текст) по открытым каналам проводной и беспроводной связи (телефонная связь, Интернет и т.п.) и ее хранение на электронных носителях.

Криптоалгоритм:

получение зашифрованного сообщения: шифрование со сжатием – преобразование – вложение в аудиоинформацию (например, в музыку) - кодирование и сжатие аудиоинформации.

Получение расшифрованного сообщения: декодирование с декомпрессией – идентификация аудиоинформации (распознавание) – преобразование – декомпрессия – преобразование – декодирование (дешифрование).

Состав:

система состоит из абонентских устройств, центра синхронизации передаваемых сообщений, канала аудиоданных и устройства активации.

- Количество абонентских устройств от 2 до n.
- А - абонентское устройство, состоящее из: компьютера; ШДУ - шифрующего/дешифрующего устройства, реализующего криптоалгоритм и обеспечивающего внутреннюю синхронизацию, которое можно условно назвать «физическим ключом» абонентского устройства, и устройства сопряжения с сетью (например, модем и т.п.); ШДУ - конструктивно выполнено в виде «флешки» и подключается к USB;
- ЦСС - центр внешней синхронизации сообщений (не работает с реальными данными, а работает либо с образами данных, передаваемых абонентам, либо со служебными сигналами), реализует алгоритм синхронизации обмена между абонентскими устройствами; производит учет абонентов, состоявшихся и несостоявшихся соединений, проверку правильности работы сигналов синхронизации и обнаружения несанкционированного использования устройства (работа под контролем); осуществляет арбитраж и отключение абонентов, ведет реестр аутентификации абонентов (аналогия сертификатов ЭЦП) и санкционирует дешифрацию информации;

- состоит из компьютера, мультиплексора и устройства сопряжения сетью;

- КАД - виртуальный канал аудиоданных, предназначен для постоянной передачи аудиоинформации пользователям системы;

- реализуется пользователем;

- Устройство активации ШДУ – предназначено для активации ШДУ в момент первого запуска.

Описание и структурная схема представлена в [12].

Защищенная АСОД является закономерным результатом использования свойств многокомпонентности алгоритма и некоторого видоизменения функций ЦСС. При этом:

- одна из его частей обеспечивает начальное шифрование и сжатие данных для хранения и «поиска без распаковки», в зашифрованном и сжатом виде реализуя функции «шифрования на лету»;
- другая часть осуществляет окончательное преобразование и шифрование сообщения перед передачей в канал связи.

Наблюдатель [13], алгоритмы, сигналы синхронизации, устройства и их взаимодействие представляют собой единую целостную макросистему ЗИ АСОД, которую можно представить множеством целостных микросистем защиты АСОД «абонентское устройство – данные». В случае возникновения угрозы безопасности произойдет нарушение целостности микросистемы, в которой она возникла, ее автоматическое отключение и уведомление наблюдателя о причинах возникновения угрозы для проведения расследования. Отключение

микросистемы не влияет на работоспособность макросистемы ЗИ АСОД. Структурная схема защищенной АСОД представлена на рис.2.

Состав:

система состоит из W-количества рабочих станций (А - абонентских устройств), центра синхронизации передаваемых сообщений (ЦСС), канала аудиоданных (КАД), Клиент-сервера (КС), N-количества баз данных, устройства активации (УА) шифрующих/дешифрующих устройств и наблюдателя (Н). Функции рабочих станций (А - абонентских устройств), КАД, УА не видоизменены и были приведены выше.

• Клиент-сервер - устойство(а), обеспеивающее(ие) работу технологии Client-server, оснащенное(ые) многоканальным ШДУ и поддерживающее(ие) бизнес-правила (процедуры управления и т.д., которые указывают, как клиент получает доступ к данным на сервере).

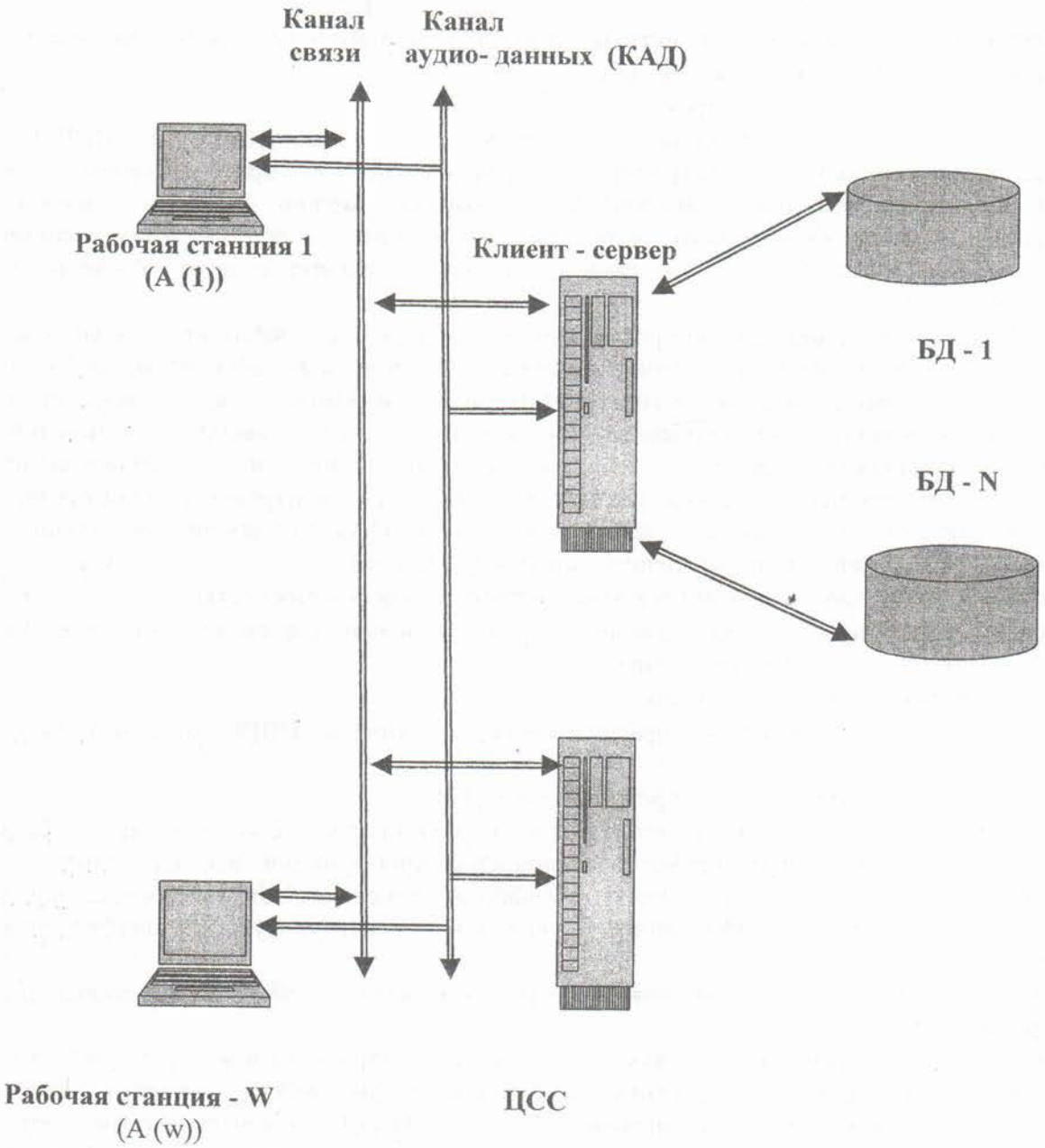

Рис. 2. Структурная схема защищенной АСОД

Таким образом, ШДУ КС может рассматриваться как виртуальная группа абонентских устройств с более высоким, относительно А, приоритетом обслуживания доступа к серверу. Эти правила реализуются клиентом А, сервером КС и центром синхронизации сообщений ЦСС.

• ЦСС - центр внешней синхронизации сообщений, кроме функций: синхронизаций, тестирования, учета абонентов, учета состоявшихся и несостоявшихся транзакций, арбитража и обеспечения аутентификации (аналогия функций ЭЦП),

- расставляет приоритеты;
- ограничивает доступ к представлению результатов и данным;
- поддерживает и контролирует соблюдение регламента, проверку функциональной пригодности информации БД при санкционированном ее видоизменении;
- регистрирует факт, время и причину возникновения угроз безопасности.

ЦСС обладает функциями «бизнес-логики», необходимыми для построения СУБД, что позволяет интегрировать ЗИ на основе «виртуального ключа» в уже существующие архитектуры АСОД и проектировать новые системы с учетом этих особенностей.

• Наблюдатель – сотрудник по безопасности информации (не обязательно IT специалист, малоквалифицированный пользователь), в обязанности которого входят: оперативный контроль над соблюдением регламента доступа к КС и БД, оперативное реагирование на нарушения целостности системы ЗИ, расследование причин возникновения угроз безопасности, контроль подключения абонентов. Фактически наблюдатель обладает функциями администрирования доступа к КС, но не имеет функций непосредственного доступа к БД.

Особенности функционирования:

Порядок функционирования системы ЗИ на основе «виртуального ключа» зависит от архитектуры конкретной АСОД и требований заказчика. При установке СЗИ в ЦСС прописываются условия доступа к серверу (регламент, полномочия, условия аутентификации и т.д.). Специфика заключается в алгоритме и структуре запроса «клиент-сервер» и ответа «сервер-клиент». Запрос состоит из запрашиваемой информации и сигналов управления, несущих в себе признаки аутентификации оператора, записи (видоизменение, уничтожение), чтения и разрешения выполнения. Ответ, по аналогии с запросом, также состоит из информационной и управляющей частей.

Алгоритм запроса имеет вид: формирование запроса абонентом (клиентом) → шифрование запроса → передача серверу → обработка и выделение сигналов управления (СУ) → шифрование СУ → передача СУ в ЦСС, обработка и шифрование СУ → передача СУ абоненту → дешифрование → выполнение СУ абонентом.

Алгоритм ответа следующий: формирование ответа сервером → шифрование запроса → передача абоненту (клиенту) → обработка и выделение сигналов управления(СУ) → шифрование СУ → передача СУ в ЦСС, обработка и шифрование СУ → передача СУ серверу → дешифрование → выполнение СУ сервером.

Как видно из алгоритмов, генератором интереса к данным всегда выступает клиент. Одновременно он формирует сигналы управления, которые после их выделения шифруются и передаются в ЦСС, где они обрабатываются. После обработки (аутентификация, проверка полномочий и т.д.) и шифрации клиенту передается сигнал разрешения чтения ответа. В случае нарушения условий доступа (регламент, аутентификация, ограничения доступа и т.д.) производится запись в журнале контроля угроз, сигнал разрешения чтения не передается и ответ не может быть прочитан. Клиент предупреждается, проводится контрольный сеанс ЦСС – клиент, после чего абонент либо отключается, либо продолжает работу. При отключении уведомляется Наблюдатель, который проводит служебное расследование и изымает ШДУ. В случае невозможности физического изъятия, Наблюдатель уничтожает

сигналы синхронизации, что приводит к невозможности использования ШДУ без повторной активации.

Таким образом, не имея доступа к информации и не принимая непосредственного участия в ее обработке, ЦСС СЗИ с «виртуальным ключом» выполняет функции СУБД при построении на ее основе защищенной АСОД или интеграции СЗИ в существующую ИС.

Выводы

Криптографические методы и средства играют важную роль при решении проблемы защиты ИС от внутренних угроз безопасности данных.

Система защиты информации с использованием «виртуального ключа» повышает эффективность ЗИ по сравнению с другими решениями и позволяет:

- защитить хранилища и каналы передачи данных;
- интегрировать СЗИ с минимальными затратами в уже функционирующую АСОД;
- использовать СЗИ с базами данных разнообразной классификации;
- в значительной степени автоматизировать процесс противодействия внутренним атакам со стороны лиц, имеющих доступ к информационной системе по долгу службы;
- обеспечить оперативный контроль и реагирование на возникающие угрозы со стороны внутренних злоумышленников;
- использовать в качестве администраторов сотрудников безопасности без специальной подготовки (малоквалифицированный пользователь);
- проводить аудит действий администраторов («контроль за контролером»);
- уменьшить количество обслуживающего персонала.

Список литературы

1. *Липаев В.В.* Выбор и оценивание характеристик качества программных средств. - М.: «Синтег», 2001. - 224 с.
2. *Липаев В.В.* Методы обеспечения качества крупномасштабных программных средств/РАН. Институт системного программирования. - М.: «Синтег», 2003. - 511 с.
3. *Липаев В.В.* Экономика производства сложных программных продуктов/РАН. Институт системного программирования. - М.: «Синтег», 2008. - 490 с.
4. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. Кн. 1 и 2. - М.: «Энергоатомиздат», 1994.
5. *Палагин А.В., Алишов Н.И., Марченко В.А., Широков В.А.* Технология защиты больших баз данных от несанкционированного копирования// Комп'ютерні засоби, мережі та системи. – 2006.-№ 5.-С. 73 – 79.
6. *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети анализ технологий и синтез решений. - М.: ДМК Пресс, 2004. - 616 с.
7. *Коннолли Т., Бегг К.* Базы данных. Проектирование, реализация и сопровождение. Теория и практика: 3-е изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2003. -1440 с.
8. ISO/IEC 17799 – Практические правила обеспечения безопасности информации (кодекс лучшей практики).
9. ISO/IEC 15408 – Общие критерии оценки защищенности систем информационных технологий.
10. *Климентов В.В., Трощило А.С., Дыс Л.И., Бурлаков В.М.* Проблемы и перспективы применения криптографических систем // Інформаційна безпека. Матеріали науково-практичної конференції. Україна, Київ, 26-27 березня 2009 року. -С. 270 - 274.
11. *Алябушкин И.Б., Бабушкин В.В.* Методики защиты баз данных от внутренних злоумышленников // Защита информации INSIDE.-2006.- №6.- С. 58 - 63.
12. *Климентов В.В., Трощило А.С.* Криптосистема с «виртуальным ключом» // Захист інформації.- 2010.- №1(46). Україна, Київ, ДУІКТ. - С. 89 - 94.
13. *Шабанов-Кушнаренко Ю.П.* Применение метода нуль-органа в психофизике // Проблемы бионики.- 1978. - №21. Харьков: «Вища школа».- С. 3 -10
14. *Шабанов-Кушнаренко Ю.П.* Применение метода нуль-органа в лингвистике // Проблемы бионики.- 1978.- №21.- Харьков: «Вища школа». - С. 109 -112.

У статті розглядається вирішення проблеми захисту інформації від внутрішніх загроз (розкрадання, видозміни і т.д.) з боку користувачів, уповноважених за службовими обов'язками працювати з базами даних і системами управління базами даних. Засобом вирішення проблеми є система захисту інформації з «віртуальним ключем».
Ключові слова: автоматизована система обробки даних, система управління базами даних, Клієнт-сервер, «шифрування на льоту», аутентифікація, шифрування, дешифровка, инсайдер, система захисту інформації, «віртуальний ключ».

В статье рассматривается решение проблемы защиты информации от внутренних угроз (хищения, видоизменения и т.д.) со стороны пользователей, уполномоченных работать по долгу службы с базами данных и системами управления базами данных. Средством решения проблемы является система защиты информации с «виртуальным ключом».
Ключевые слова: автоматизированная система обработки данных, система управления базами данных, Клиент-сервер, «шифрование на лету», аутентификация, шифрование, дешифрование, инсайдер, система защиты информации, «виртуальный ключ».

In the article the decision of problem of defence of information is examined against internal threats (thefts, modifications and etc) from the side of users, who are obligated to work with the databases and control databases systems in the course on duty inside a company. The tool of decision of problem is the system of defence of information with the «virtual key».
Keywords:Automated data handling system, control databases system, Client-server, «coding on the fly», authentification, coding, decoding, insider, system of defence of information, «virtual key».

Поступила 16.06.2010

UDK 004.621.3

Kovtun V., Kuznetsov A.,
(Telecomunication and Information Security Research Lab,
Kharkiv Air Force Unsversity)
Evseev S.
(Kharkiv National University of Economics)

SOFTWARE IMPLEMENTATION OF GENUS-2 HYPERELLIPTIC CURVE CRYPTOSYSTEMS OVER PRIME FIELDS

Introduction

With the recent boost of information technology in modern society, the problem of information security becomes of special urgency. The most difficult task is to provide a secure handling and storage of critical and confidential data for government and private companies, banks and other systems. A solution to this problem is to implement systems which provide information confidentiality, integrity, authenticity and accessibility by means of cryptographic software and cryptographic hardware.

At the same time cryptanalytical methods, multiplied by the progress in capabilities of modern computers, puts high requirements on the security parameters of modern cryptosystems. Moreover, the increased data amount processed in modern information systems requires a high performance of modern cryptosystems. Hence the timing requirements to cryptographical applications have increased dramatically. I.e., prospective cryptoalgorithms must provide efficient processing of bulk data and, at the same time, a high level of security. Under this circumstances, the most urgent direction is the development of public key cryptosystems which are efficient in software and hardware and allow for setting up a PKI.

In recent decades, elliptic curve cryptosystems (ECC) have been widely exploited which can be seen by recent standardization efforts [1, 2]. However, this is not the last frontier of the research