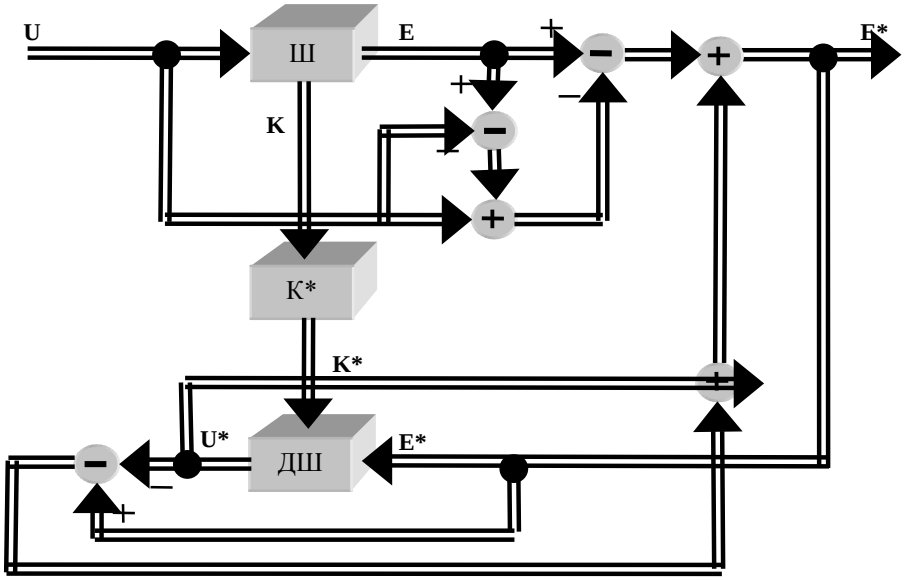

Рис. 1. Общая схема формирования информационных потоков в процессе шифрования при переходе от действительного к виртуальному информационному пространству

Предложенная стратегия открывает новую область исследований, позволяющую реализовывать дополнительные потенциальные возможности уже известных методов и способов защиты информации, а также получать принципиально новые решения, обеспечивающие выполнение условий теоретической недешифруемости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Галлагер Р.* Теория информации и надёжная связь. – М.: Советское радио, 1974. – 720с.

2. *Величкин А.И.* Передача аналоговых сообщений по цифровым каналам. – М.: Радио и связь, 1983. – 240 с.

3. Котенко В.В., Румянцев К.Е., Поликарпов С.В.. Новый подход к оценке эффективности способов шифрования с позиций теории информации // Вопросы защиты информации. 2004. №1. – С.16 − 22.

О.О. Варламов
Россия, г. Москва,
Московская академия рынка труда и информационных технологий

ПОЛЬЗОВАТЕЛЬСКАЯ ТЕХНИЧЕСКАЯ КОМПЬЮТЕРНАЯ УГРОЗА И СПОСОБЫ ЗАЩИТЫ ОТ НЕЕ НА ОСНОВЕ ОБРАБОТКИ ИЗБЫТОЧНЫХ И ЗАКРЫТЫХ ЗАПРОСОВ К БАЗАМ ДАННЫХ

Как известно, для обеспечения технической защиты информации разработана Модель технических компьютерных угроз на основе выделения девяти типов: семантических, алгоритмических, вирусных, разграничительных, сетевых, потоковых, аппаратных, форматных и пользовательских технических компьютерных угроз. В данной работе исследована пользовательская техническая компьютерная

угроза и предложены способы защиты от нее на основе обработки избыточных и закрытых запросов к базам данных.

Объектами защиты от технических компьютерных угроз принято считать компьютерные системы (сети) и характеристики их пользователей и программно-аппаратных средств. Девять типов компьютерных угроз необходимо учитывать в первую очередь при обеспечении безопасности информации в ключевых системах информационных инфраструктур - ОБИ КСИИ, являющихся по существу гетерогенными территориально распределенными компьютерными сетями, аналогичными Интернет. Хотя, не все компьютерные сети имеют физическое подключение к Интернету, но практически все они используют однотиповые технические решения. Ранее было доказано, что под компьютерной разведкой (КпР) не достаточно понимать только получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования [1]. В настоящее время КпР – это добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [2]. Существует три типа источников информации для КпР:

1) данные, сведения и информация, обрабатываемые, в т.ч. передаваемые и хранимые, в компьютерных системах и сетях;

2) характеристики программных, аппаратных и программно-аппаратных комплексов;

3) характеристики пользователей компьютерных систем и сетей.

Различным видам КпР посвящено множество научно-исследовательских работ. Так как **пользовательская КпР** позволяет получать данные непосредственно о пользователях (людях и программах) компьютерных систем и сетей, то необходимо разработать методы защиты от нее. Напомним, что пользователями компьютерных сетей являются не только люди, но и отдельные программы или программно-аппаратные комплексы.

Пользовательская КпР – это добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (приманка).

Появление и развитие **пользовательской** угрозы информационной безопасности обусловлено повсеместным использованием компьютерных сетей, когда некоторая информация, самого верхнего уровня, о непосредственных пользователях-людях может добываться техническими средствами, что ранее было прерогативой исключительно "человеческих" агентурных методов. Например, путем системного анализа запросов человека в различные базы данных и к информационным ресурсам, участия его в телеконференциях, получения его адресно-именной информации и т.п. представляется возможным добывание информации о пользователях, их деятельности и интересах. Кроме того, путем обеспечения изучаемым пользователям доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (приманка), также возможно добывание техническими средствами информации об интересах пользователей, их организационной принадлежности, функциональным обязанностям и других сведений (пороках, запросах, проблемах личного характера, психологического портрета и т.п.), которые могут использоваться для агентурных и других целей.

Итак, рассмотрим более подробно обращение пользователей к различным информационным ресурсам и базам данных, которые для краткости будем обозна-

чать - БД. Суть пользовательской КпР заключается в анализе интересов пользователей по их запросам к БД. Следовательно, для защиты от пользовательской КпР необходимо:

1) либо замаскировать истинные потребности в ресурсах БД избыточными, ложными запросами,

2) либо скрывать авторов запросов к БД,

3)либо скрывать сами запросы.

Возможно, есть и другие типы способов, которые еще ждут своих первооткрывателей.

1. Наиболее простым и широко распространенным способом является маскирование истинных запросов путем генерации избыточных запросов, который будем называть "способ избыточных запросов". Суть данного способа заключается в том, чтобы создавать большой поток самых разнообразных запросов, в котором сложно будет выявить небольшое количество истинных запросов. Образно говоря, надо создать "шум" и скрыть истинные "сигналы". На данном этапе необходимо переходить к количественным оценкам создания подобного шумового фона, разработать методики определения типового разнообразия избыточных запросов.

Способ "избыточных запросов" в настоящее время активно применяется. Например, если какой-либо фармацевтической компании нужно получить у сторонних организаций опытные данные по некоторому конкретному "препарату", то осуществляется закупка всей базы данных для маскирования истинного узкого направления исследований фармацевтической компании. Это аналогично походу в книжный магазин и закупке там, вместо нескольких нужных книг, полного ассортимента имеющихся книг. Конечно же, это огромные затраты, но в некоторых случаях они себя оправдывают: ведь никто не узнает, какие именно книги вам были нужны, а, следовательно, не узнают и чем вы занимаетесь.

На практике хорошо зарекомендовал себя способ создания разнообразного трафика путем выделения многим сотрудникам одного "пользовательского имени", когда внешним наблюдателям неизвестно кто и какую информацию запрашивает внутри организации. В качестве аналога, возможно, следует использовать методы защиты акустических сигналов. Это пока лишь направление для серьезной математической работы и обоснования методик защиты. Многие организации пытаются бороться с "лишним" трафиком, запрещают сотрудникам использование сети в личных и неслужебных целях, однако, с точки зрения защиты от пользовательской КпР - это именно один наиболее доступных способов защиты от нее. Ведь понятно, что когда истинный трафик составляет 5-10 % от общего трафика, то внешним наблюдателям, в том числе и злоумышленникам, будет достаточно сложно получить информацию путем пользовательской КпР.

2. Вторым способом является скрытие авторства информационных запросов к БД. Это можно осуществить, например, подобно тому, как в библиотеке можно либо просить разных людей взять необходимые вам материалы, либо самому записаться в различные библиотеки и в каждой брать малую долю необходимых материалов, либо записаться в библиотеку под разными фамилиями (реальность этого - отдельный разговор) и опять же под каждой фамилией брать малую долю необходимых материалов. Получаем следующие варианты защиты: получать требуемые материалы через различных пользователей малыми долями; обращаться к различным источникам информации за малыми долями; зарегистрироваться разными пользователями - "масками" и получать те же самые малые доли требуемой информации. При этом, важно обеспечить маскирование и избыточные для вас запросы и от истинных пользователей, и от ваших "масок". Методика регистрации разных "масок" требует, возможно, "входа в сеть" действительно с физически раз-

личных мест подключения к сети. Впрочем, при достаточных усилиях, все эти методы могут быть реализованы уже в настоящее время. Побочным эффектом первого и второго направления является избыточный трафик, подобный "спаму", но это еще необходимо исследовать.

3. Скрытие самих запросов. В этом направлении защиты возможны два основных варианта: 1) скрытие самого факта запроса и 2) при известном "легальном" запросе скрытие содержания запроса. Для скрытия самого запроса необходимо использовать "вирусоподобные" и/или "разграничительные" (несанкционированный доступ - НСД) методики, которые в данной работе не рассматриваются.

Наибольший интерес в определенных "легальных" применениях представляет проблема при известном запросе скрытия именно и только содержания запроса. В данном направлении выделим, прежде всего, такую область, которую принято называть: **обработка закрытых запросов (ОЗЗ)**. В работах Дмитрия Валерьевича Асонова [3-9] предложен оригинальный подход к решению проблемы "обработки закрытых запросов". Кратко опишем предлагаемые решения, а желающим более подробно разобраться в данном методе рекомендуем обратиться к указанной выше литературе. Итак, в докладе Асонова Д.В. [3] рассматриваются две нестандартные проблемы обработки запросов к базам данных (БД).

Первая проблема ОЗЗ заключается в обработке запроса к БД так, что:

– сервер (и владелец) базы данных не может получить никакой информации о содержании и результате запроса пользователя и

– пользователь не получает никакой информации о БД, за исключением ответа на свой запрос.

Подчеркнем, что доступ к БД нам разрешен, но никто, кроме нас, не должен в принципе знать ни о нашем вопросе, ни о полученном ответе. Администратор БД видит только факт самого запроса и размер полученных по этому запросу данных. Это позволяет владельцу БД выставить соответствующий счет на оплату услуг.

Известны три категории решения данной проблемы: 1) теоретические, 2) криптографические и 3) ОЗЗ на защищенном вычислительном устройстве (ЗВУ). Теоретические методы в разных вариациях рассматривают копирование всей БД. Криптографические решения существуют на основе доработок нестандартными методами, но для них обязателен доступ в реальном времени и перебор всей базы данных. Например, владелец БД пересылает заказчику всю БД в зашифрованном виде, что исключает возможность воровства информации. Заказчик через каталог или аннотации выбирает из БД требуемую ему одну запись и также шифрует ее "поверх" шифра владельца. Используемые шифры должны быть гомоморфными (или коммуникативными), что позволяет осуществлять замену шифров. Заказчик не может прочесть запись, так как она зашифрована владельцем. Заказчик отправляет зашифрованную запись владельцу БД, который также не может прочесть эту запись, ведь ему не известен шифр заказчика. Далее, владелец "снимает" свой шифр, выставляет счет на оплату и после получения денег пересылает запись заказчику. Заказчик после оплаты и получения записи расшифровывает ее и использует для своих целей. Получаем, что заказчик получает только одну запись, но ее содержание не известно никому, ведь она зашифрована самим заказчиком. Владелец БД отдает заказчику только одну запись, ведь все остальные записи зашифрованы именно владельцем. По каналам связи передается только зашифрованная информация, что исключает доступ к ней посторонних лиц. У этого класса криптографических решений существует огромный недостаток, обусловленный необходимостью перебора всей БД, что значительно увеличивает время между заказом и получением требуемой записи. Учитывая огромные размеры современных БД, этот недостаток делает невозможным реальное использование криптогра-

фических методов для решения проблемы обработки закрытых запросов к большим и/или часто обновляемым БД.

Обработка закрытых запросов на защищенном вычислительном устройстве. Защищенные вычислительные устройства - ЗВУ, представляют собой специальный класс устройств для хранения защищенных данных и исключения доступа к ним людей, даже системных администраторов и владельцев. При попытке проникновения в ЗВУ все данные на нем немедленно физически уничтожаются и проводится оповещение соответствующих служб. Это устройство выполняет функции "третьего доверенного лица", которому доверяют и владелец, и заказчик. Если любого человека хотя бы теоретически можно подкупить, то ЗВУ подкупить невозможно. Отметим, что ЗВУ используются для решения различных задач и достаточно большим количеством способов. В данной работе целесообразно для примера проанализировать только несколько способов. В целом ЗВУ представляют собой "черный ящик", который встраивается в оборудование владельца информационного ресурса. Возможно, что такое "встраивание" является рискованным и психологически сложным для владельца.

Рассмотрим запрос заказчика на получение конкретной записи от владельца БД. Заказчик посылает свой зашифрованный запрос к ЗВУ, которое его расшифровывает. Далее ЗВУ получает поочередно все записи из БД, но "откладывает", запоминает у себя внутри только одну - нужную заказчику. После выполнения финансовых действий, владелец разрешает ЗВУ отослать зашифрованную этим ЗВУ запись заказчику. Этот шифр знают только ЗВУ и заказчик, который после получения самостоятельно расшифровывает требуемую ему запись и использует ее. Таким образом, никто, кроме ЗВУ, не знает, какую запись получил заказчик, а заказчик не видит остальных записей БД владельца.

Разработаны различные модификации применения ЗВУ для сокращения времени обработки запросов и обеспечения их защищенности. Применяют различные виды препроцессинга и другие виды обработки БД. Например, можно хранить в ЗВУ специальным образом "перемешанный" каталог реальной БД, на основе которого значительно ускоряется время обработки запросов заказчика, ведь уже нет необходимости при каждом запросе перебирать всю БД, а заказчик заказывает и получает требуемую запись по преобразованному в ЗВУ номеру. Для повышения защищенности такой каталог в ЗВУ регулярно обновляют и осуществляют "пермутацию", т.е. случайное перемешивание.

Вторая проблема ОЗЗ заключается в обработке запроса на пересечение двух баз данных таким образом, что:

– владельцы баз данных не могут получить никакой информации о БД партнера, а также о результате запроса на пересечение;

– пользователь не может получить никакой информации из баз данных, за исключением результата запроса на пересечение.

В этом случае заказчик не узнает ничего лишнего о БД, кроме прямого ответа на свой запрос. ОЗЗ позволяет получать заказчикам такие ответы и не показывает никому содержание самих БД. Например, две компании могут проводить статистические исследования пересечений своих пользователей, но исходные данные о своих клиентах эти компании друг другу не показывают (только обобщенные статистические результаты и зависимости). Другой пример, когда транспортные компании перевозят пассажиров и собирают все данные на них, а внешние службы безопасности имеют списки "злоумышленников" ("стоп-списки"). Задача состоит в том, что бы при решении совместных задач по обеспечению безопасности пассажиров никто из злоумышленников, включенных в "стоп-списки", не мог попасть на транспорт и при этом, чтобы транспортные компании не знали самих "стоп-

списков", а службы безопасности не знали о перемещениях лиц, не входящих в "стоп-списки". Таким образом, формально решается задача получения взаимного доступа только к пересечениям двух баз данных, но владельцы этих БД не знают ничего другого о чужих БД. Решение этой проблемы также возможно криптографическими способами, аналогичными выше указанным способам. К недостаткам этих способов можно отнести то, что они способны выявлять только полное равенство (совпадение) признаков записей из разных баз данных. Более перспективным является применение защищенных вычислительных устройств. Такие ЗВУ внутри себя получают доступ ко всем базам данных и могут не только выявлять полное равенство (совпадение) записей из разных БД, но и определять степень их близости (находить близкие записи или подобные).

Потенциальные приложения этих двух проблем ОЗЗ очень разнообразны и включают, помимо технической защиты от пользовательской КпР, такие области, как коммерческая безопасность, антитеррористические меры, экономика (банковское дело, трейдинг, маркетинг, реклама, электронные магазины, и т.д.), биомедицина, патентное дело, и т.д. В настоящее время проводятся исследования по следующим основным направлениям в области обработки закрытых запросов: комбинирование криптографических методов и защищенных вычислительных устройств; закрытые запросы к сверхбольшим базам данных в режиме времени, близком к реальному; закрытые запросы к нескольким базам данных, а также по другим направлениям. Таким образом, в актуальной области пользовательской компьютерной разведки появляются новые угрозы и своевременно разрабатываются методы защиты от них. Извечная борьба средств нападения и защиты продолжается на новом (компьютерном) уровне развития технического прогресса.

Выводы. Для обеспечения технической защиты информации предложен и обоснован новый актуальный подход к исследованию пользовательской технической компьютерной угрозы или, другими словами: пользовательской компьютерной разведки. Предложены три вида способов защиты от нее на основе маскирования запросов, обработки избыточных и закрытых запросов к базам данных. Особый интерес представляет, предложенный Д.В. Ассоновым метод защиты от пользовательской технической компьютерной угрозы путем обработки закрытых запросов на основе защищенных вычислительных устройств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Меньшаков Ю.К.* Защита объектов и информации от технических средств разведки. - М.: Российский гос. гуманитарный ун-т, 2002. – 399с.

2. *Варламов О.О.* О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ТРТУ, Тематический выпуск "Информационная безопасность", – Таганрог: Изд-во ТРТУ, 2006, № 7 (62). – С. 216-223.

3. *Асонов Д.В.* Обработка закрытых запросов. Доклад на семинаре Московской секции ACM SIGMOD, ВМК МГУ. 26.04.2007

4. *Rakesh Agrawal, Dmitri Asonov, Murat Kantarcioglu, Yaping Li*: Sovereign Joins. ICDE 2006: 26

5. *Dmitri Asonov:* Querying Databases Privately: A New Approach to Private Information Retrieval Springer 2004

6. *Dmitri Asonov, Ramakrishnan Srikant*: Enabling Sovereign Information Sharing Using Web Services. SIGMOD Conference 2004: 873-877

7. *Dmitri Asonov, Johann Christoph Freytag*: Almost Optimal Private Information Retrieval. Privacy Enhancing Technologies 2002: 209-223

8. *Dmitri Asonov, Johann Christoph Freytag*: Repudiative information retrieval. WPES 2002: 32-40

9. *Dmitri Asonov*: Private Information Retrieval. GI Jahrestagung (2) 2001: 889-894