УДК 658.5, 004.9

Ю. В. Трифонова – студентка кафедры комплексной защиты информации
Р. Ф. Жаринов – аспирант кафедры технологий защиты информации

ПРАВОВЫЕ АСПЕКТЫ ПЕРЛЮСТРАЦИИ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПЕРЛЮСТРАЦИИ ПРИ ИСПОЛЬЗОВАНИИ DLP СИСТЕМ

Современному предприятию в работе сложно избежать наличия конфиденциальной информации. Это может быть ноу-хау, технологии, базы данных поставщиков, клиентов, сотрудников (т.е. коммерческая тайна, банковская тайна, налоговая тайна и персональные данные). Разглашение такой информации может принести огромный ущерб предприятию, поэтому конфиденциальная информация находится под постоянными внешними и внутренними угрозами. Однако, как известно, чаще всего разглашение конфиденциальной информации происходит по вине собственных сотрудников предприятия. Такое разглашение может быть как намеренным, так и случайным.

Если предприятие серьезно озабочено информационной безопасностью, то вынести физически конфиденциальную информацию за пределы предприятия практически невозможно, но остается вероятность разглашения во время ведения деловой или личной переписки с рабочего места через сети общего доступа. Именно поэтому системы, позволяющие производить перлюстрацию электронной переписки, могут быть весьма полезны на предприятии. Под перлюстрацией понимается просмотр личной пересылаемой корреспонденции, совершаемый втайне от отправителя и получателя.

Одним из способов защиты конфиденциальной информации от утечки на предприятии может стать Data Leak Prevention (DLP) система (системы предотвращения утечки информации). DLP система анализирует поток данных исходя из политик безопасности, при нахождении конфиденциальной информации в потоке данных система, исходя из заданных параметров, может блокировать сообщение или же просто сохранять соответствующее сообщение. Администратор системы может просматривать сохраненные сообщения и реагировать на инциденты.

Для осуществления наблюдения за электронной корреспонденцией достаточно установить на одном из узлов компонент DLP-системы, регистрирующий весь проходящий трафик. Такая система поможет разобраться в структуре и содержании сетевого трафика, оценить эффективность принимаемых мер информационной безопасности. Если же злоумышленнику удастся обойти систему защиты, то при использовании DLP-системы вероятность его нахождения возрастает, а перехваченная сессия может использоваться в качестве доказательства в суде, но только в том случае, если перлюстрация корреспонденции происходила на законном основании.

Что же говорит законодательство об использовании систем перлюстрации электронной корреспонденции? Согласно п. 2 ст. 23 Конституции Российской Федерации «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Подобное положение присутствовало и в предыдущих конституциях (ст. 56 Конституции СССР 1977 года; ст. 128 Конституции СССР 1936 года), и в конституциях большинства зарубежных стран. Оно же утверждается во «Всеобщей декларации прав человека» 1948 года.

Ограничить право на тайну переписки согласно ст. 13 Уголовно-процессуального кодекса Российской Федерации возможно только на основании судебного решения. Однако, согласно п. 1 ст. 63 Гражданского процессуального кодекса Российской Федерации «…Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами».

Такими законами являются:

- Федеральный конституционный закон «О военном положении»;
- Федеральный закон «Об оперативно-розыскной деятельности»;
- Федеральный закон «О Федеральной службе безопасности»;
- Федеральный закон «О противодействии терроризму».

Каждый из законов предусматривает обязательное подтверждение правомерности ограничения на тайну переписки судебным решением, за исключением закона «О военном положении». Таким образом, если отправитель и получатель не дали своего согласия на проведение мониторинга своей корреспонденции и отсутствует судебное решения, то перлюстрация является уголовно наказуемым деянием и влечет за собой ответственность в соответствии со ст. 138 Уголовного кодекса Российской Федерации:

«1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.

2. То же деяние, совершенное лицом с использованием своего служебного положения, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо принудительными работами на срок до четырех лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до четырех лет».

Подводя итог всему вышесказанному можно заключить, что служба информационной безопасности не имеет права проводить перлюстрации своих сотрудников. А в соответствии со ст. 138 Уголовного кодекса Российской Федерации такое деяние будет классифицироваться по п. 2, так как производятся с использованием служебного положения.

Однако использование DLP-системы на предприятии не может стать основанием для возбуждения уголовного или административного дела, поскольку субъектом разбирательства может стать только человек.

Трудовой кодекс Российской федерации дает работодателям возможность применения систем перлюстрации электронной корреспонденции своих работников в процессе исполнения ими их служебных обязанностей. Мониторинг корреспонденции сотрудников направлен на обеспечение исполнения работниками их служебных обязанностей и сохранение конфиденциальных данных предприятия, а согласно ст. 22 работодатель имеет право требовать от работников исполнения ими трудовых обязанностей, бережного отношения к имуществу работодателя и других работников, соблюдение правил внутреннего трудового распорядка организации. Под правилами внутреннего трудового распорядка, согласно ст. 189 понимается локальный нормативный акт, регламентирующий порядок приема и увольнения работников, основные права, обязанности и ответственность сторон трудового договора, режим работы, время отдыха, применяемые к работникам меры поощрения и взыскания, а также иные вопросы регулирования трудовых отношений у данного работодателя.

Поэтому использование электронных средств коммуникации для личных целей противоречит существу трудовых правоотношений и ставит под угрозу сохранность конфиденциальной информации предприятия, которая составляет коммерческую тайну. Подпункты 1 – 3 ст. 183 Уголовного кодекса Российской Федерации определяют ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Таким образом, для законной перлюстрации корреспонденции работников необходимо внести соответствующие пункты в трудовой договор или в правила внутреннего трудового распорядка. Еще одним способом является отчуждение прав работников от всей своей корреспонденции, отправленной ими с рабочих компьютеров, в пользу работодателя. Этот факт также должен быть отражен в трудовом договоре. При этом получатели корреспонденции от сотрудников предприятия должны быть уведомлены, о том, что на предприятии происходит мониторинг корреспонденции, так как для законности перлюстрации дать свое согласие должны как отправитель, так и получатель.

В таком случае сложно избежать ситуаций, когда мониторинг корреспонденции будет производиться незаконно. Например, когда сетью предприятия воспользуются посторонние люди или получатели сообщений не были предупреждены. Кроме того администратор DLP-системы ограничен только договоренностями и личными этическими нормами, так как у него есть возможность просмотра вообще

всего трафика. Однако необходимо реализовать DLP-систему в рамках закона, контролируя при этом исходящую информацию и ограничивая права администраторов.

Для этого предполагается расширить DLP-систему таким образом, чтобы сообщения от пользователя шли в зашифрованном виде, а DLP-система осуществляла бы поиск ключевых слов в зашифрованном сообщении. Производить операции над открытым текстом, при работе с зашифрованным, позволяет гомоморфное шифрование.

Под гомоморфным шифрованием понимается криптосистема, где функция шифрования удовлетворяет требованию гомоморфности относительно заданного набора операций над открытым текстом [1].

Пусть $E(m_i) = c_i$ – функция шифрования, $D(c_i) = m_i$ - функция дешифрования, '$*$' – некая математическая операция. Тогда функция E гомоморфна относительно операции $*$, если существует алгоритм M, который получив на вход пару шифрограмм $c_1 = E(m_1)$ и $c_2 = E(m_2)$, выдает результат $c' = M(c_1,\ c_2)$, при дешифровании которого получится результат операции $*$ над исходными открытыми текстами $D(c') = m_1 * m_2$. Гомоморфизм позволяет выполнять операции над данными на стороне сервера, не выполняя дешифрования (Рис. 1).

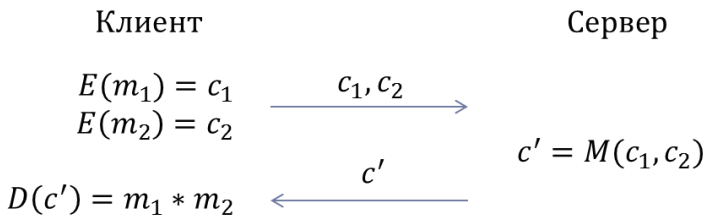

Рис. 1. Схема выполнения операции, относительно которой гомоморфна функция шифрования, на стороне сервера

Понятие полного гомоморфизма подразумевает наличие двух математических операций, относительно которых функция шифрования отвечает требованию гомоморфности, и для которых выполнима любая функция, содержащая любые комбинации из этих операций. Примеров полного гомоморфизма на сегодняшний день не существует, но есть ряд ограниченных решений:

- для одной математической операции;
- для двух операций, но с ограничением их количества внутри выполнимой функции;
- периодический обмен данными между сервером и клиентом.

Для того чтобы DLP-система могла производить проверку наличия конфиденциальной информации в зашифрованном сообщении без его расшифровки, необходимо разработать метод поиска слова в зашифрованном сообщении. Для этого рассматриваются существующие подходы с точки зрения представленной задачи, определяется функция сравнения, и минимизируются объемы данных, обрабатываемых на сервере и передаваемых по каналу DLP-системе.

В работающей системе данные от сотрудника будут уходить в зашифрованном виде, DLP-система, проверив сообщение по зашифрованным политикам безопасности, сохранит обезличенный ответ. Под обезличенным ответом подразумевается ответ вида «да/нет» на вопрос содержания в сообщении конфиденциальной информации и само зашифрованное сообщение, если в нем присутствуют конфиденциальные данные.

Система должна предусматривать общий ключ, который будет разделен, например, между членами совета директоров. Этот ключ позволит расшифровать сохраненный трафик, когда будет идти разбирательство по факту разглашения конфиденциальной информации и будет получено судебное решения на перлюстрацию корреспонденции на данном предприятии.

Библиографический список

1. *Варновский Н.*П., Шокуров А.В. Гомоморфное шифрование// Труды Института Системного Программирования, Методы синтеза и анализа алгоритмов, Том 12, Москва 2006г, С.27-37.
2. Конституция Российской Федерации

3. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ
4. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 N 174-ФЗ
5. «Гражданский процессуальный кодекс Российской Федерации» от 14.11.2002 N 138-ФЗ
6. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ
7. Федеральный конституционный закон от 30.01.2002 № 1-ФКЗ «О военном положении»
8. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»
9. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»
10. Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности»
11. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму»
12. Федотов *Н.Н.,* Тайна связи против технических средств защиты информации в Интернете, http://forensics.ru/zi-ts.html. Дата обращения: 13.04.2012г.
13. *Лукацкий А.,* Легитимна ли перлюстрация электронной почты на предприятии, Bankir.Ru, http://bankir.ru/tehnologii/s/legitimna-li-perlustraciya-elektronnoi-pochti-na-predpriyatii-1367747/. Дата обращения: 13.04.2012г.