УДК 004.056.5

д.т.н., проф. **Бойченко О.В.** (Тавр.НУ)
Тупота Е.С. (Тавр.НУ)

DLP-ТЕХНОЛОГИИ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В статье исследованы возможности использования систем типа Data Leak Prevention для выявления внешних вмешательств и утечки корпоративной информации. Определены отличительные признаки технологии исследования на основе DLP-систем для анализа защищенности распределенной информационной системы управления предприятием.

Установлено, что инновационные DLP-системы наиболее эффективно использовать для построения системы информационной безопасности в экономической сфере в части организации обнаружения фактов несанкционированной передачи конфиденциальных драанных неавторизованным пользователям.

Обоснована актуальность применения исследованной технологии для усовершенствования системы мер хранения клиентской базы экономического предприятия путем оперативного мониторинга каналов утечки.

Разработана методика рационализации выбора DLP-системы соответственно особенностям деятельности предприятия в условиях возможных угроз информационной безопасности и ключевых аспектов по оптимизации системы экономической безопасности.

Ключевые слова: информационная система, информационная безопасность, DLP системы, мониторинг утечек.

Постановка проблемы. Актуальность исследования обусловлена необходимостью разработки новых подходов в решении защиты коммерческих данных фирмы в условиях

широкого и повсеместного роста фактов несанкционированного доступа к ресурсам компании и утечек информации.

При ведении любой коммерческой деятельности на данном этапе развития современного общества важнейшим аспектом является информация. Потеря данных является критичной для фирмы, поскольку это может привести к потере клиентской базы предприятия.

Анализ экспертных исследований современной проблематики экономической безопасности предприятий в части утечек корпоративной информации, проведенный аналитическим центром «InfoWatch», показывает 1505 случаев потери важных данных коммерческой деятельности (рис. 1), что на 10% больше по сравнению с 2014 годом. При этом 32% обнаруженных проникновений относятся к внешним угрозам.

Рис. 1. Количество утечек коммерческой информации на предприятиях за 2007-2015 гг.

Анализ характера выявленных утечек показывает, что в большинстве случаев утечка организована с помощью атаки на массивы данных (клиентская база, база поставщиков, база посредников и т.д.). Кроме того, установлено, что 8% эпизодов, связанных с потерей данных, являются проникновениями с несанкционированным доступом к информации с последующим ее изменением и превышением прав доступа [1].

Приведенные результаты исследования определяют необходимость разработки новых способов и методов в системе защиты данных распределенной корпоративной информационной системы.

Постановка задачи. Цель исследования состоит в проведении анализа механизмов защиты коммерческих данных предприятия на основе DLP-систем, а также разработки новых методик их применения для оптимизации функционирования системы экономической безопасности.

Изложение основного материала. Информационная безопасность является ключевым аспектом в деятельности предприятия. Риски, связанные с утечкой данных, влияют на его привлекательность для инвесторов и клиентов.

Опыт показывает, что вероятность образования внутреннего канала утечки информации (пользовательский аспект) в компании выше, чем утечка данных по причине взлома (внешний аспект) [2]. Наиболее часто это связано с неправомерными или халатными действиями сотрудника предприятия по ошибочной отправке информации не зарегистрированному адресату. Потому для организации обнаружения несанкционированной передачи конфиденциальных данных неавторизованным пользователям на предприятиях необходимо внедрять инновационные технологии исследования, в частности на основе DLP-систем.

Рис. 2. Потенциально опасные каналы утечки информации

Главным достоинством DLP-технологий является то, что их внедрение в процессы автоматизации управления деятельностью предприятия обеспечивает создание условий для предотвращения утечек конфиденциальной информации и других коммерческих данных.

Кроме того, программный комплекс DLP позволяет вести учет состояния потенциально опасных каналов связи, по которым возможно могут проходить утечки корпоративной информации (рис. 2.)

Результаты экспертных заключений указывают на необходимость для каждого предприятия, в соответствии с принятым регламентом (политикой безопасности), организовывать систему контроля над потенциально опасными каналами связи. Особого внимания требует необходимость обеспечения своевременного контроля бизнес-процессов в части обработки и использования конфиденциальной информации в комплексном сочетании кадровой политики по подбору лиц, ответственных за своевременный контроль сетевой активности рабочих мест [3].

Отдельной проблемой, наряду с внедрением программного комплекса, является необходимость эффективного функционирования аппаратного комплекса консоли централизованного управления DLP системой. Исследования определяют, что в настоящее время наиболее надежными комплексами являются системы таких мировых брэндов, как Hewlett-Packard, IBM, EMC, Dell и т.д.

Следует также отметить, что такие системы строятся на анализе потока данных

(«алгоритме обнаружения»), функционирующего внутри информационной системы (ИС).

Использование такого алгоритма при обнаружении потока утечки данных в системе приводит к немедленному срабатыванию активной компоненты DLP, и передача потока блокируется. При этом DLP-система проводит обязательный анализ данных, входящих в защищаемую систему, а выявление степени конфиденциальности информации и дальнейшее ее блокирование происходит благодаря проведению аналитических операций по выявлению содержания пакетов. Однако следует отметить, что не все DLP-системы эффективно определяют содержание передаваемого пакета данных вследствие того, что отдельным программным продуктам свойственно нахождение специальных маркеров, характерных для конфиденциальной информации (гриф документа, мета-код, значение хэш-функций и т.д.).

Характеризуя отличительные признаки анализируемой технологии, особо следует выделить задачу анализа потока данных, являющейся ключевой для DLP-системы в целом. Наряду с этим, современный этап развития информационно коммуникационных технологий позволяет интегрировать в DLP-систему большое количество инновационных нетривиальных методов анализа, позволяющих повысить эффективность технологий исследования в целом [4].

При этом современные технологии в области исследования условно можно разделить на две группы (рис. 3).

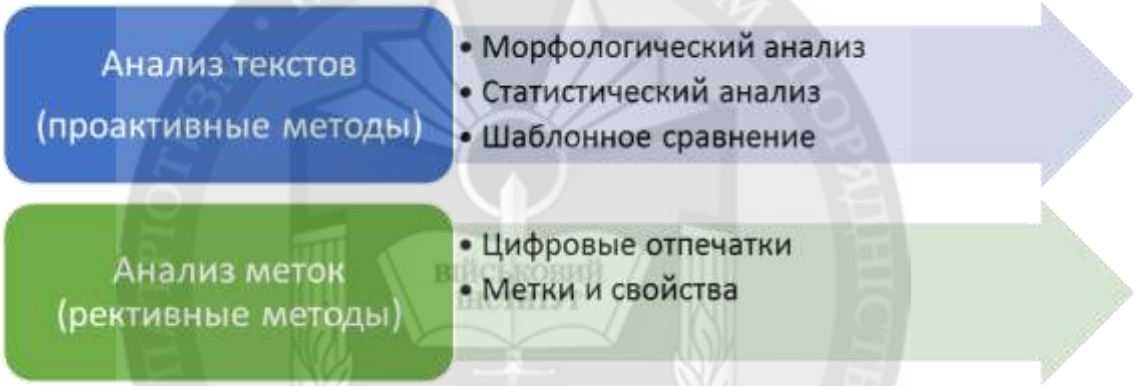

Рис. 3. Методы анализа потоков данных в DLP-системах

Детальное изучение указанных методов позволяет заключить, что морфологический анализ, входящий в группу проактивных методов, является самым популярным способом нахождения утечек конфиденциальной информации. Его суть состоит в нахождении ключевых слов в передаваемых текстах.

В аналогичную группу входит статистический анализ данных. Суть данного метода заключается в расчете вероятностей утечки определенной информации с предприятия. Однако данный метод отличается большей сложностью в реализации, так как требует необходимости разработки дерева решений для последующего проведения анализа.

Метод шаблонного сравнения также представляет достаточно высокую продуктивность за счет простой интеграции в программную среду информационной системы на основе шаблонов, свойственных конфиденциальной информации данного предприятия.

Характеризуя анализ цифровых отпечатков и цифровых меток (вторая основная группа методов), следует отметить, что он представляет собой совокупность конкретных характеристик документа, по которым его впоследствии можно будет распознать. Суть метода заключается в присвоении меток информации, доступность которых характерна только для клиентских модулей DLP-системы.

Особо следует выделить основную задачу DLP-систем, связанную с мониторингом, идентификацией и защитой конфиденциальной информации предприятия.

Для решения указанной задачи DLP-система, прежде всего, нацелена на обеспечение защиты в каналах утечек, связанных с:

- внешними устройствами;
- информацией, находящейся в сетевом доступе;
- средствами сетевой печати;
- Веб-ресурсами;
- передачей файлов по каналам HTTP, HTTTPS, FTP;
- электронной почтой;
- программами взаимодействия с клиентами.

Как указывалось, ранее, внутри информационной системы каждому потоку данных присваиваются метки и тэги. Использование такого подхода в дальнейшем обеспечивает более точный анализ контента, что, в свою очередь, создает условия для администратора по заданию определенных правил для отбора потоков. Кроме того, в режиме реального времени обеспечивается анализ всех событий передачи данных внутри системы, а также осуществляется блокировка нежелательных потоков.

Анализируя основные приложения для обеспечения функционирования рассматриваемой системы, прежде всего, следует выделить программный продукт Websense Data Security Suite, который обеспечивает высокий уровень мониторинга по каналам передачи электронной почты, а также сообщений MS Exchange, HTTP, FTP, HTTPS.

Кроме того, система может отправлять уведомления администратору о факте передачи конфиденциальной информации и полностью блокировать нежелательные потоки. Вместе с этим, в комплекте с системой представлен ряд готовых стандартных шаблонов и надстроек, что позволяет создавать условия для эффективного разграничения доступа к информации, а также ее удалению и изменению.

Опыт показывает, что для расширения функционала данной DLP-системы необходимо использовать специализированные программы, такие как Data Endpoint, Data Monitor, Data Protect, Data Discover. При этом, простота внедрения системы обусловлена наличием специального мастера. Однако недостатком данной системы является отсутствие русификатора, что может затруднить внедрение технологии в российских кампаниях.

Falcongaze SecureTower является отечественной разработкой, основанной на поиске конфиденциальной информации за счет ключевых слов, тег, подписей и т.д. Такой подход обеспечивает отслеживание трафика по всем контролируемым каналам связи.

Особенностью данного продукта является полная интеграция в среду Skype, что создает дополнительные условия защиты информации за счет осуществления перехвата голосовых сообщений. Кроме того, система обеспечивает отслеживание работы сотрудников предприятия использованием функции периодического производства скриншотов экрана сотрудников. Дополнительно система так же осуществляет контроль на уровне IP-адресов, создавая определенные карты посещения.

Функционально структура Falcongaze SecureTower состоит из сервера перехвата трафика, сервера контроля рабочих станций и сервера обработки информации. Еще одним явным преимуществом данной системы является ее легкая масштабируемость, что является весьма актуальным для развивающихся компаний [5].

Проведенные исследования указывают, что большинство известных DLP-систем имеют одинаковый функционал, однако могут иметь конкретные преимущества для бизнеса (таблица 1).

При этом каждому предприятию среднего бизнеса для решения вопросов обеспечения конфиденциальности информации на основе внедрения DLP-систем, необходимо исходить из номинальной стоимости комплекса в целом и максимального количества контролируемых каналов. Кроме того, предприятию необходимо обеспечить ответственного администратора системы и ответственного за безопасность системы в целом. В целом каждый выбранный комплекс может обеспечивать полную гарантию сохранности корпоративной информации на

предприятии. Анализ данных таблицы позволяет заключить, что на предприятии среднего масштаба (примерно 250 рабочих мест) стоимость комплекса DLP обойдется приблизительно в 1 000 000-2 500 000 руб.

Таблица 1

Сравнительная таблица наиболее известных DLP-систем

Название Критерий оценки системы	Falcongaze SecureTower	Websense Data Security Suite	InfoWatch Security Monitor
Общие характеристики			
Модульность	Нет	Да	Нет
Место установки	Оператор, сервер	Оператор, сервер	Оператор, сервер
История попыток взлома	Да	Да	Да
Анализ контекста утечек	Нет	Да	Нет
Количество «ответственных» мест	2	Любое количество	Ограниченное количество
История осуществлённых взломов	Да	Да	Да
Рабочая Лицензия	Каждое рабочее место	-	Контролируемые каналы
Контролируемые каналы			
IM	Да	Да	Да
HTTP/HTTPS; FTP	Да	Да	Да
Skype	Видео, звук, текст	Нет	Текст
Почта	Да, корпоративная и личная	Да, корпоративная и личная	Да, корпоративная и личная
Социальные сети	Да	Да	Да
Внешние подключаемые устройства	Отсутствует	Полный контроль	Дополнительная надстройка
Сетевая печать (с возможностью оптического распознавания текста OCR)	Да	Да	Информация отсутствует
Аналитические характеристики			
Определение и анализ не правильного шифрования	Да	Да	Да
Анализ подозрительного трафика	Да	Да	Да
Анализ мультимедийных вложений	Нет	Да	Да
Остановка передачи несанкционированных сообщений	Нет, происходит информирование контролера системы	Происходит обучение системы оператором	Да, система определяет автоматически
Хранение отчетности	Да	Да	Да
Стоимостные показатели			
Цена рабочего места	6000 руб.	8000-10000 руб.	Информация отсутствует

Полученные научные результаты. Таким образом, в результате проведенного исследования установлено, что эффективная деятельность современных предприятий не возможна без использования инновационных технологий защиты конфиденциальной информации, что обусловлено высоким уровнем утечек информации, прежде всего по внешним каналам (33% за 2015 год).

По результатам исследования разработана таблица, использование которой обеспечивает рационализацию выбора конкретной DLP-системы для предприятия путем ориентировки на выделение ключевых аспектов, отличающих программные комплексы различных фирм.

Выводы. В системе информационной безопасности фирмы DLP-системы являются эффективным инструментом, который позволяет создавать условия для решения проблем защиты конфиденциальной информации. Это обеспечивает значительное снижения риска потери критических данных, высокий уровень мониторинга каналов утечки, возможность контроля периметра корпоративной ИС наряду с доступностью стоимости в установке на действующих системах управления.

Дополнительный эффект внедрения систем достигается комплексным использованием с другими мерами контроля несанкционированного влияния на информационные ресурсы предприятия.

ЛИТЕРАТУРА:

1. Бойченко О.В.Технологии data leak prevention в системе защиты коммерческих данных / О.В. Бойченко, Е.С. Тупота // Региональная информатика. Юбилейная XV Санкт-Петербургская междунар. конфер., 25-28 окт. 2016 г., сборник тезисов. - С-ПБ, 2016. – С.146-147.

2. Бойченко О.В. Пользователь в системе информационной безопасности АСУ / О.В. Бойченко // Теория и практика экономики и предпринимательства: XII Междунар. науч.-технич. конф., 23-25 апреля 2015 г.: тезисы докладов. – Симферополь, 2015. – С. 12-15.

3. Жабин С.Ф. Исследование систем обнаружения вторжений операционного уровня информационных систем / С.Ф. Жабин, А.Е. Захаров // Тезисы научно-технического семинара «Координационный совет по информатизации Владимирской области», 2008. – С. 34-37.

4. Фенюк М.В. Аналіз недоліків систем автоматизованого захисту інформації та методів біометричної автентифікації, які в них використовуються / М.В. Фенюк // ММС, 2012. – №3. – С.116-123.

5. Шимон Н.С. Способы и средства защиты от сетевых атак в Единой информационно-телекоммуникационной системе органов внутренних дел // Вестник ВИ МВД России, 2009. – №1. – С.164-167.

REFERENCES:

1. Bojchenko O.V., Tupota E.S. (2016) Tehnologii data leak prevention v sisteme zashhity kommercheskih dannyh [Data Leak Prevention Technologies in systems of economics security enterprise] Regional’naja informatika. Jubilejnaja XV Sankt-Peterburgskaja mezhdunar. konfer., 25-28 okt. 2016 g., sbornik tezisov, S-PB, 2016. – pp.146-147 (In Russian).

2. Bojchenko O.V. Polzovatel v sisteme informacionnoj bezopasnosti ASU [Users in security systems like ASC] / O.V. Bojchenko // Teorija i practica economici i predprinimatelstva. – Simferopol, 2015. – pp. 12-15. (In Russian).

3. Zhabin S.F., Zaharov A.E. (2008) Issledovanie sistem obnaruzhenija vtorzhenij operacionnogo urovnja informacionnyh sistem [Research of systems which detect on operational-level information systems] Tezisy nauchno-tehnicheskogo seminara «Koordinacionnyj sovet po informatizacii Vladimirskoj oblasti», 2008. – pp. 34-37. (In Russian).

4. Fenjuk M. V. Analiz nedolikiv sistem avtomatizovanogo zahistu informacii ta metodiv biometrichnoї avtentifikacii, jaki v nih vikoristovujut’sja [Analysis of the shortcomings of automated information security and biometric authentication techniques used in them] MMS, 2012. - №3. - pp.116-123 (In Ukraanian)

5. Shimon Nikolaj Stepanovich Sposoby i sredstva zashhity ot setevyh atak v Edinoj informacionno-telekommunikacionnoj sisteme organov vnutrennih del [Ways and means of protection against network

attacks in a Single information-telecommunication system of Internal Affairs] // Vestnik VI MVD Rossii, 2009. - №1. - pp.164-167. (In Russian)

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

д.т.н., проф. Бойченко О.В., Тупота О.С.

DLP-ТЕХНОЛОГІЇ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті досліджено можливості використання систем типу Data Leak Prevention для встановлення зовнішніх втручань й витоку корпоративної інформації. Визначені відмітні ознаки технології дослідження на основі DLP-систем для аналізу захищеності розподіленої інформаційної системи управління підприємством.

Встановлено, що інноваційні DLP-системи найбільш ефективно застосовувати для розбудови системи інформаційної безпеки в економічній галузі в частині організації виявлення фактів несанкціонованої передачі конфіденційних даних неавторизованим користувачам.

Обґрунтована актуальність застосування досліджуваної технології для удосконалення системи заходів зберігання клієнтської бази економічного підприємства шляхом оперативного моніторингу каналів витоку.

Розроблено методику раціоналізації вибору DLP-системи відповідно особливостям діяльності підприємства в умовах можливих загроз інформаційної безпеки та ключових аспектів з оптимізації системи економічної безпеки.

Ключові слова: інформаційна система, інформаційна безпека, системи DLP, моніторинг витоків.

prof. Boychenko O.V., Tupota E.S.

DLP TECHNOLOGY IN THE SYSTEM OF ECONOMIC SECURITY OF ENTERPRISE

This Article reveals the possibility of using systems such as Data Leak Prevention for identifying external interference and leakage of corporate information. The distinctive features of technology study on the basis of DLP-systems for security analysis of distributed information system of enterprise management were identified.

Innovative DLP system is most effective to use to build information security system in the economic sphere on the detection of unauthorized transmission of confidential data to unauthorized users.

Actuality of application of the studied technologies to improve the system of measures of a client base of economic enterprise by online monitoring of leakage channels were also established.

Method of rationalizing the choice of a DLP system according to characteristics of enterprise activity in terms of possible information security threats and key aspects for the optimization of the system of economic security were developed.

Key words: information system, information security, DLP systems monitor leaks.