И. С. Боридько, А. А. Забелиский, Ю. И. Коваленко

ПРИМЕНЕНИЕ DLP-СИСТЕМ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с Федеральным законом «О персональных данных», оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

При этом защита информации представляет собой принятие правовых, организационных и технических мер, которые направлены на выполнение следующих операций:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализация права на доступ к информации [1].

Обеспечение безопасности персональных данных достигается, в частности, определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных; применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных; применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации и другими мероприятиями [2].

Традиционные средства обеспечения информационной безопасности, такие как системы обнаружения атак, межсетевые экраны, антивирусы, выполняют функции защиты персональных данных от внешних угроз, но не обеспечивают защиту информационных ресурсов от утечки, искажения или уничтожения внутренним злоумышленником (инсайдером).

Поэтому задача защиты конфиденциальных данных становится одной из актуальных на сегодняшний день. Аналитики, изучающие инсайдерские угрозы, считают, что:

- внутренние угрозы безопасности по-прежнему беспокоят компании значительно больше внешних угроз. Наибольшие опасения вызывают угрозы утечки информации (73 %), а также халатность служащих (70 %);
- основной причиной актуальности внутренних проблем являются продолжающиеся утечки информации — только 5 % компаний заявили об отсутствии подобных инцидентов за год;
- распространение систем защиты от внутренних угроз за последний год выросло примерно на 30 %;
- в подавляющем большинстве случаев нарушители внутренней безопасности не несут практически никакой ответственности.

Организационные меры по защите персональных данных сформулированы в действующих нормативных правовых актах [1–3] и нормативных правовых документах [4–8].

По оценкам экспертов, утечки корпоративных данных, происходящие по злому умыслу или недосмотру персонала, выдвигаются на первое место в современных рейтингах угроз информационной безопасности. Помимо прямых многомиллионных потерь они наносят компаниям трудно оцениваемые в деньгах репутационные ущербы [9].

Сейчас у всех на слуху сайт WikiLeaks, который опубликовал еще недавно находившуюся под грифом строгой секретности информацию. Данный пример показал многим хозяйствующим субъектам, насколько серьезные последствия может иметь утечка информации. В результате подобных инцидентов лишаются работы руководители, и, как показывает практика, речь может идти даже о крупных дипломатических скандалах.

Решить проблему защиты от случайных и умышленных утечек конфиденциальной информации позволяют DLP-системы (Data Leak Prevention System), или системы предотвращения утечек.

DLP-система реализуется путем использования технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также за счет применения технических устройств (программных или программно-аппаратных) для предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При обнаружении в исходящем потоке конфиденциальной информации (персональных данных) срабатывает DLP-система и передача сообщения (пакета, потока, сессии) блокируется.

Каждый разработчик DLP-решения предлагает свою собственную архитектуру развертывания, но, в общем, принципиальные модули системы следующие:

- перехватчики/контроллеры на разные каналы передачи информации;
- агентские программы, устанавливаемые на оконечные устройства;
- центральный управляющий сервер.

Перехватчики анализируют потоки информации, которая может быть выведена из периметра компании, обнаруживают конфиденциальные данные, классифицируют информацию и передают для обработки возможного инцидента на управляющий сервер. Перехватчики могут быть как для копии исходящего трафика, так и для установки в разрыв трафика. В последнем случае потенциальная утечка может быть остановлена системой DLP.

На деле большинство DLP-решений работает в пассивном режиме, т. е. не блокирует утечки информации. Подобные DLP только анализируют копию сетевого трафика и сообщают об имевшей место утечке постфактум.

Второй особенностью существующих DLP-решений является имеющийся набор технологий анализа и обнаружения утечек конфиденциальных документов. Для анализа и обнаружения утечек данных в современных DLP применяются лишь один-два метода. Технологические ограничения сужают сферу применения таких DLP-решений, так как почти для каждой категории конфиденциальных данных требуется своя адаптированная технология анализа.

Контроллеры для обнаружения хранимых данных запускают процессы обнаружения в сетевых ресурсах конфиденциальной информации. Способы запуска обнаружения могут быть различными: от собственно сканирования сервера контроллера до запуска отдельных программных агентов на существующие серверы или рабочие станции.

Контроллеры для операций на рабочих станциях распределяют политики безопасности на оконечные устройства, анализируют результаты деятельности сотрудников с конфиденциальной информацией и передают данные возможного инцидента на управляющий сервер.

Агентские программы на оконечных рабочих местах замечают конфиденциальные данные в обработке и следят за соблюдением таких правил, как сохранение на сменный носитель информации, отправки, распечатывания, копирования через буфер обмена.

Управляющий сервер сопоставляет поступающие от перехватчиков и контроллеров сведения и предоставляет интерфейс проработки инцидентов и построения отчетности.

Таким образом, решения DLP нацелены на централизованный контроль за всеми инцидентами нарушения политик безопасности по отношению к конфиденциальной информации.

Для защиты информации от инсайдеров российская компания SecurIT предлагает средства класса DLP, которые эффективно предотвращают утечки конфиденциальной информации через подключаемые устройства и сетевые каналы (система Zlock и система Zgate).

Система Zlock реализует контроль доступа к внешним и внутренним устройствам компьютеров в масштабах корпоративной сети.

Основное назначение DLP-системы Zlock компании SecurIT — предотвращение утечек конфиденциальной информации через периферийные устройства. Zlock разграничивает доступ к накопителям и принтерам, анализирует содержимое файлов, распечатываемых и записываемых на устройства, и блокирует действия пользователей в случае выявления нарушений политик безопасности.

Zlock дает возможность гибко настраивать права доступа пользователей и групп пользователей к любым устройствам. Это обеспечивает существенное снижение риска утечек как через устройства, подключаемые к внешним портам (USB, LPT, COM, IrDA, PCMCIA, IEEE 1394 и т. д.), так и через внутренние устройства (сетевые карты, модемы, Bluetooth, Wi-Fi, CD/DVD-дисководы и т. д.). Кроме этого, Zlock может контролировать доступ к локальным и сетевым принтерам.

Разграничение доступа к устройствам в Zlock осуществляется на основе политик доступа. В политике могут использоваться различные параметры устройств, к которым она будет применяться: серийный номер, класс и идентификатор устройства, данные о производителе и другие параметры, которые позволяют максимально точно идентифицировать конкретное устройство или группу устройств. В системе Zlock есть возможность хранения описаний устройств в едином каталоге и создания политик на их основе, это существенно повышает гибкость системы и оперативность реагирования на требования бизнес-пользователей.

Документы, передаваемые на USB-устройства и принтеры, подвергаются контентному анализу. При обнаружении конфиденциальной информации в передаваемых файлах система может мгновенно блокировать действия пользователя (чтение, запись, печать) и сообщить администратору безопасности. Для анализа содержимого применяется гибридный анализ — комплекс технологий детектирования данных разного типа.

Централизованная установка и управление Zlock могут осуществляться через единую консоль управления продуктами SecurIT либо через групповые политики домена. При этом в Zlock также реализована расширенная интеграция с Active Directory, что дополнительно позволяет использовать доменные списки компьютеров и пользователей для создания и распространения политик безопасности.

В Zlock впервые для DLP-систем подобного класса была реализована система мониторинга клиентских модулей, которая позволяет администратору безопасности в режиме реального времени получать информацию о событиях Zlock. Это дает возможность максимально оперативно реагировать на любые несанкционированные и подозрительные действия со стороны пользователей.

Архивирование (теневое копирование) и сбор событий Zlock позволяет контролировать всю информацию, которая записывается на разрешенные устройства. Это помогает в создании ретроспективной картины использования устройств и последующем анализе возможных инцидентов. При этом теневое копирование работает по превентивному принципу — данные сохраняются в теневой копии до записи на внешний носитель. Такая реализация гарантирует высокую надежность работы и невозможность записи данных на внешний носитель в обход теневого копирования. Также Zlock может фиксировать в хранилище теневых копий документы, которые пользователь распечатывал на локальных или сетевых принтерах.

Использование DLP-системы Zlock позволяет свести к минимуму риск утечки конфиденциальной информации, значительно затруднить деятельность инсайдеров и предоставить руководству предприятия полную информацию для расследования инцидентов.

Система Zgate реализует защиту от утечек через электронную почту, веб-сайты, интернет-мессенджеры и FTP-серверы и является надежным средством для реализации корпоративной политики безопасности.

В современных условиях руководители организации понимают, что потеря или кража конфиденциальных данных ведет не только к прямым финансовым убыткам, но и к снижению доверия со стороны клиентов, партнеров и инвесторов. Любая утечка данных, даже отправка письма с конфиденциальными документами по ошибочному адресу, приводит к повышенному интересу со стороны регулирующих органов и СМИ.

Это увеличивает риски финансовой ответственности за нарушение отраслевых стандартов и законодательства, регулирующих защиту персональных данных и другой конфиденциальной информации.

Система Zgate компании SecurIT разрабатывалась с учетом преимуществ и недостатков существующих DLP-решений. В отличие от них, Zgate позволяет блокировать утечки конфиденциальных данных по сетевым каналам. Для обнаружения и блокировки утечек в Zgate используется гибридный анализ, включающий в себя множество современных технологий детектирования конфиденциальных данных. Применение гибридного анализа позволило повысить эффективность детектирования со среднестатистических 60–70 % для существующих DLP до 95 % у Zgate.

Zgate анализирует все данные, передаваемые сотрудниками за пределы локальной сети организации, и позволяет предотвращать утечки конфиденциальной информации по сетевым каналам — через электронную почту, социальные сети, интернет-мессенджеры и т. д. В Zgate используются современные технологии, которые безошибочно определяют уровень конфиденциальности передаваемой информации и категорию документов с учетом особенностей бизнеса, требований отраслевых стандартов и законодательства России, СНГ, Европы и США.

Zgate позволяет контролировать и архивировать:

- переписку в корпоративной электронной почте;
- письма и вложения, отсылаемые через сервисы веб-почты;
- общение в социальных сетях, на форумах и в блогах;
- сообщения интернет-пейджеров;
- файлы, передаваемые по FTP,

а также проводить анализ всех контролируемых каналов утечки.

Для проведения внутренних расследований и профилактики утечек Zgate записывает подробную информацию обо всех происходящих инцидентах: передаваемые данные, сведения об отправителе, получателе, канале передачи и т. д. Встроенная система отчетности предоставляет полный набор инструментов для наглядного анализа сохраненных данных и улучшает эффективность процесса принятия решений по происходящим инцидентам. В дополнение к нескольким десяткам готовых отчетов в Zgate встроен специальный конструктор, дающий возможность создавать, сохранять и публиковать неограниченное количество индивидуальных отчетов.

Достоинства Zgate:

- Zgate контролирует весь сетевой трафик. В отличие от существующих DLP-систем, кроме исходящего трафика Zgate может анализировать входящий и внутренний трафик, что расширяет возможности для внутреннего контроля.

- Для обнаружения и своевременной блокировки утечек информации в Zgate применяется гибридный анализ, использующий более 10 специализированных технологий.
- Zgate контролирует сообщения и файлы, отправляемые через более чем 15 видов интернет-пейджеров и более чем 250 различных веб-сервисов — от почты Mail.ru до видеохостинга YouTube.
- Zgate может интегрироваться с Microsoft Forefront TMG (Microsoft ISA Server) и любым прокси-сервером, поддерживающим протокол ICAP (Internet Content Adaptation Protocol) — Blue Coat, Cisco ACNS, Squid и т. д.
- Система Zgate совместима с любой почтовой системой (MTA) и контролирует письма и вложения, отправляемые через Microsoft Exchange Server, IBM Lotus Domino, CommuniGate Pro и т. д.
- Zgate поддерживает анализ более 500 форматов файлов, в том числе Microsoft Office, OpenOffice.org, изображения, а также обработку архивов заданного уровня вложенности.
- Все пересылаемые письма, сообщения и файлы помещаются в специальный архив, не имеющий ограничений по объему и сроку хранения данных.
- В установку Zgate включено более 50 шаблонов, с помощью которых можно определять конфиденциальные данные. Это существенно сокращает трудозатраты при внедрении.
- Для настройки защиты информации в Zgate используются специальные политики безопасности, имеющие до 30 различных параметров.
- Управление Zgate осуществляется через единую систему управления DLP-решениями Zconsole, которая также поддерживает управление Zlock и Zserver Suite.

Таким образом, используя DLP-системы, можно обеспечить программную защиту персональных данных от злонамеренных действий внутреннего нарушителя.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 27 июля 2010 г., 6 апреля, 21 июля 2011 г.).
2. Федеральный закон от 27 июля 2006 г. 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г., 28 июня, 27 июля, 29 ноября, 23 декабря 2010 г., 4 июня, 25 июля 2011 г.).
3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
4. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г.).
6. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ России 21 февраля 2008 г. № 149/54-144).
7. Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».
8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 14 февраля 2008 г.).
9. *Синельников А.* Защита от утечки информации. URL: http://fingazeta.ru (дата обращения 10.09.2012).