УДК 004.457
DOI 10.21685/2587-7704-2020-5-1-2

Open Access RESEARCH ARTICLE

Применение средств контроля и предотвращения утечки информации

М. А. Лабазин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. Г. Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Произведен анализ средств контроля и предотвращения утечки информации, предназначенных для защиты локальных сетей организации. Составлен перечень основных требований и функциональных возможностей DLP-систем. Проведен обзор систем контроля и предотвращения утечки информации для защиты ПЭВМ, функционирующих под управлением ОС Linux.

Ключевые слова: средство контроля и предотвращения утечки информации, средство защиты информации, несанкционированный доступ, Linux, информационная система.

The use of data loss prevention systems

M. A. Labazin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. An analysis of data loss prevention (DLP) systems designed to secure local networks of the organization is performed. A list of basic requirements and functions for DLP-systems is given. A review of DLP-systems to protect computers operating under Linux OS is carried out.

Keywords: data loss prevention system, information protection facility, unauthorized access, Linux, information system.

В современном обществе информация является не только предметом профессиональных обменов, ресурсом принятия решений, но и все чаще выполняет функции объекта посягательств злоумышленников, средством конкурентной борьбы между организациями. В связи с установлением данных условий возрастает роль безопасного использования информации.

Для решения проблемы сохранения конфиденциальной информации разработчики систем защиты предлагают различные комплексы. На протяжении многих лет во многих организациях использовались классические средства защиты информации.

Средства защиты от несанкционированного доступа (СЗИ от НСД) – программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации. СЗИ от НСД имеют широкое распространение в государственных структурах, различных отраслях бизнеса и во многих частных компаниях. За время существования данных систем сложились определенные требования к этим системам и стандартный набор функций.

Основными функциями, которые реализуют системы защиты от несанкционируемого доступа, являются:

– полномочное (мандатное) и дискреционное распределение доступа;
– идентификация и аутентификация пользователей и устройств;
– регистрация запуска (завершения) программ;

– учет носителей информации;
– управление информационными потоками между устройствами.

Однако в настоящее время, исходя из анализа инцидентов информационной безопасности, все больше угроз конфиденциальной информации представляют пользователи, непосредственно работающие с ней. Работники организации в корыстных целях или по причине ошибки могут передавать, копировать и распространять обрабатываемую информацию.

Для решения данной проблемы на рынке средств защиты информации представлены системы контроля и предотвращения утечек информации (DLP – Data Loss Prevention). DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При анализе в этом потоке информации выявляется та информация, которая не должна передаваться за пределы защищаемой ИС.

DLP-системы производят анализ передаваемой информации по всем возможным каналам, обнаружение случаев несанкционированной передачи конфиденциальных данных, их блокирование и незамедлительное оповещение отдела информационной безопасности.

Одна из главных задач системы контроля и предотвращения утечек информации – отличать конфиденциальную информацию от неконфиденциальной. В большинстве случаев системы DLP работают совместно с ответственным специалистом, который не только обеспечивает корректную работу системы, вносит новые и удаляет неактуальные правила, но и проводит мониторинг текущих, заблокированных или подозрительных событий в информационной системе. В случае срабатывания заранее настроенного правила или политики, которыми определяется факт передачи защищаемой информации, система либо блокирует такую передачу, либо посылает тревожные уведомления сотруднику службы безопасности.

Требований к разработке и структуре данных систем нет, но, проанализировав множество систем контроля и предотвращения утечки информации, можно выделить основные функциональные возможности:

– использование известных видов протоколов для передачи данных;
– контроль действий сотрудников в процессе выполнения рабочих обязанностей;
– средства создания аналитической отчетности и наглядного представления информации и др.;
– перехват, запись и идентификация голосового трафика;
– контроль хранения информации на внешних носителях;
– предотвращение попыток пересылки конфиденциальных данных;
– мониторинг коммуникаций сотрудников;
– контроль связи коллектива с уволенными сотрудниками;
– консоль централизованного управления;
– клиентский модуль;
– база данных;
– выделенные серверы;
– модули анализа информации.

Перечень основных функциональных возможностей составлен с учетом результатов анализа существующих DLP-систем [1].

Консоль централизованного управления является основным средством управления работой системы и может быть установлена на любом компьютере. С помощью данной консоли имеется возможность установки, контроля, а также настройки других компонентов системы.

Клиентский модуль устанавливается на каждый контролируемый компьютер в организации. С помощью него администратор безопасности осуществляет контроль за действиями сотрудников и обеспечивается применение политик безопасности. Такой агент должен быть защищен от вмешательства пользователя в свою работу и может вести как пассивное наблюдение за его действиями, так и активно препятствовать тем из них, которые пользователю запрещены политикой безопасности компании. Перечень контролируемых действий может ограничиваться входом/выходом пользователя из системы и подключением USB-устройств, а может включать перехват и блокировку сетевых протоколов, теневое копирование документов на любые внешние носители, печать документов на локальные и сетевые принтеры, передачу информации по Wi-Fi и Bluetooth и много другое. Некоторые системы контроля и предотвращения утечек информации способны записывать все нажатия на клавиатуре (keylogging) и сохранять копии экрана.

База данных необходима для хранения информации, начиная от правил контроля и подробной информации об инцидентах и заканчивая всеми документами, попавшими в поле зрения системы за

определенный период. В некоторых случаях система может хранить копию всего сетевого трафика, перехваченного в течение заданного периода времени.

Выделенные серверы могут потребоваться для таких модулей, как база данных, и иногда для модулей анализа информации. Эти модули, по сути, являются ядром системы контроля и предотвращения утечек информации.

Модули анализа информации предназначены для анализа текстов, извлеченных другими модулями из различных источников: сетевого трафика, документов на любых устройствах хранения информации. В некоторых системах предусмотрена возможность извлечения текста из изображений и распознавания перехваченных голосовых сообщений. Все анализируемые тексты сопоставляются с заранее заданными правилами и отмечаются соответствующим образом при обнаружении совпадения.

Главное отличие средств контроля и предотвращения утечек информации от классических СЗИ заключается в принципе работы данных систем. В классических СЗИ от НСД используется метод четкого разделения. К примеру, если запретить доступ к каталогу, то получить доступ к нему не получится уже никаким способом. DLP-системы же работают по принципу сбора и анализа статистики и вероятностей (процент встречаемых ключевых слов, процент соответствия шаблону документа и т.д.). В решения DLP-систем заложено принятие рисков некоторых утечек, что позволяет сделать вывод о глубоком исследовании и анализе файлов и информационных потоков средства контроля и предотвращения утечек информации.

Перед системами контроля и предотвращения утечек информации стоят немного отличные от систем СЗИ от НСД задачи, такие как:

– контроль информационных потоков и зашита от утечек данных;
– контроль лояльности персонала;
– ведение архива бизнес-коммуникации.

Для контроля информационных потоков системы контроля утечки информации отслеживают следующие каналы передачи данных [2]:

– электронная почта (SMTP, POP3, IMAP, MAPI, NNTP, S/MIME, контроль веб-почты);
– почтовые серверы (OSCAR (ICQ, QIP), MMP (любые клиенты, поддерживающие этот протокол, например Mail.Ru Агент), MSN (Windows Live Messenger), XMPP (Google Talk, Jabber), YMSG (любые клиенты, поддерживающие этот протокол, например Yahoo Messenger Protocol));
– социальные сети (ВКонтакте, Facebook);
– мессенджеры (Skype, Telegram, Viber);
– внешние устройства;
– принтеры;
– IP-телефония (контроль SIP, SDP, H.323, T.38, MGCP, SKINNY и др., включая видеотелефонию);
– пересылаемые файлы;
– кейлогер;
– сетевые диски;
– контроль приложений;
– снимки с рабочего стола;
– контроль рабочего времени.

На данный момент системы контроля и предотвращения утечек информации предоставляют возможность создания профиля каждого пользователя и постоянного контроля за действиями этих пользователей. На каждого пользователя создается личная карточка, которая содержит всю информацию о нем. В результате сотруднику службы безопасности обеспечивается возможность просмотра всех действий каждого сотрудника, анализ его работы и активности.

Для контроля пользователей администраторам безопасности доступны возможности:

– снимки экрана;
– видео экрана;
– просмотр рабочего стола в режиме реального времени;
– запись звука через микрофон ноутбука или подключенную гарнитуру;
– контроль и журналирование использования приложений;
– учет рабочего времени пользователя;
– возможность блокировки копируемой на устройство информации;
– шифрование файлов на USB-устройствах;
– контроль печати;
– контроль буфера обмена.

Одним из компонентов, позволяющих в реальном времени контролировать пользователей, является модуль анализа рисков. Модуль анализа риска – это контрольно-аналитическая система, которая в режиме реального времени информирует специалистов отдела безопасности об уровне потенциального риска. Модуль анализирует деятельность каждого сотрудника и на основе статистики формирует список работников, представляющих повышенный риск. Все изменения отображаются графически в реальном времени. Вся необходимая информация и отчеты для исследования тенденций поведения пользователей генерируются автоматически. Модуль позволяет специалистам отдела безопасности устранять угрозы до возникновения серьезного инцидента, а не работать с его последствиями. Это приводит к существенной экономии ресурсов компании.

На основании проанализированных действий пользователей системы контроля и предотвращения утечек информации в своем функционале имеют компоненты для построения отчетов. Существует несколько типов отчетов:

– интерактивные отчеты. Позволяют анализировать бизнес-процессы компании и оперативно выявлять проблемные моменты. Отчеты по заданным критериям помогают оценить работу отдельных сотрудников и подразделений. Все отчеты интерактивны и дают возможность перейти к просмотру события, что ускоряет расследование инцидентов. В некоторых системах предусмотрена возможность расследования инцидентов и формирования дел, в которых подробно фиксируется ход расследования, выявления фигурантов дел, а после завершения расследования – получения автоматически составленного отчета для руководителя. Собранные данные могут использоваться в суде в качестве доказательной базы;

– граф-анализатор взаимосвязей персонала. В графе-анализаторе для каждого сотрудника система создает профайл, автоматически привязываемый к ActiveDirectory, и отображает его коммуникации с другими людьми. В этом профайле отображаются адреса электронной почты работника, имена в мессенджерах, аккаунты в социальных сетях и на других сайтах. Для выявления недоброжелателей вне компании система контроля и предотвращения утечки информации запоминает адреса внешних абонентов и также создает для них профайлы. Такой инструмент дополнительно позволяет выявить неформальных лидеров в коллективе, определить круг общения сотрудника, а также найти потенциальных инсайдеров в случаях, когда утечка конфиденциальной информации инициируется извне;

– отчеты, отображающие картину рабочего дня сотрудника. Система проводит анализ действий сотрудника за рабочий день, благодаря чему руководство может оценить, насколько активно сотрудник использует каналы коммуникации. Кроме того, некоторые системы предполагают возможность удаленного подключения к камере или рабочему столу, а также к микрофону, установленному на рабочем месте сотрудника.

Широкий набор функций комплексов контроля и предотвращения утечек информации позволяет осуществлять контроль за действиями сотрудников в режиме реального времени с сохранением результатов анализа в журналы регистрации событий и базы данных. Разработчики не прекращают внедрять новые программные модули для повышения уровня защиты от утечек информации. Так, например, некоторые системы имеют в своем арсенале модуль расследования инцидентов. При срабатывании правил безопасности система показывает сотруднику все необходимые данные для расследования (переданные файлы, взаимодействующие лица и т.д.) в форме, пригодной для приобщения к делу в ходе судебного разбирательства.

Бесспорно, DLP-системы имеют меньшее распространение, нежели классические СЗИ от НСД, но с течением времени становятся все более популярными. Акцент защиты информации с течением времени смещается в сторону контроля персонала, его действий и коммуникации. Анализ современных систем контроля и предотвращения утечки информации позволяет сделать вывод об эволюции механизмов защиты: системы осуществили переход от контроля каждого канала к контролю каждого пользователя. Большинство компаний, являющихся лидирующими разработчиками таких систем, не проводят обучение персонала по настройке и управлению DLP-системой. Обучение осуществляется в основном после приобретения продукта, непосредственно при его установке в организацию. Данный факт негативно сказывается на распространении систем контроля и предотвращения утечек информации, поскольку перед руководителями организаций остро встает вопрос о квалифицированном персонале.

В отличие от СЗИ от НСД, сертификат Федеральной службы по техническому и экспертному контролю (ФСТЭК) имеет малое количество систем DLP. К данным системам применяют требования руководящего документа «Решение председателя Гостехкомиссии России от 25 июля 1997 г.» [3]. Из большого количества DLP-систем сертификат ФСТЭК имеют лишь две системы:

– Zecurion DLP enterprise RV. Сертификат № 3399/1 сроком действия до 30.04.2021 [4];

– DeviceLock 8 DLP Suite. Сертификат № 3465 сроком действия до 05.11.2023 [5].

Отсутствие сертификата ФСТЭК негативно сказывается на распространении систем, поскольку ставится под вопрос использование систем в государственных и муниципальных учреждениях.

Все большее количество компаний и государственных структур переходит на отечественное программное обеспечение в рамках импортозамещения. При этом в организациях возникает необходимость защиты данных от утечек на Linux-машинах. Для разработчиков это отличная возможность усовершенствовать DLP, предложив новую версию продукта под востребованные операционные системы. На данный момент лишь компания Zecurion предлагает продукт, работающий совместно с системой Linux. Система Zecurion DLP Linux предназначена для работы на российских дистрибутивах: «Альт Линукс», «Гослинукс», Astra Linux и «РЕД ОС». В системе предусмотрен контроль использования съемных устройств, печати на принтерах, передачи данных по сети и электронной почте с рабочих станций. Также Zecurion DLP Linux Agent делает снимки экрана и перехватывает ввод текста на клавиатуре. Весь перехваченный сетевой трафик отправляется на DLP Processor – серверный модуль контентного анализа. Для обнаружения конфиденциальной информации используются более десяти различных технологий детектирования, которые доступны и в Windows-версии.

Предусмотрена возможность создания гибких политик безопасности для съемных носителей. При этом можно не только запретить или разрешить использование USB-накопителей, но и установить ограничение, например разрешить только просмотр данных. При записи на устройства, печати документов и передаче данных по сети DLP-система сохраняет файлы и всю сопутствующую информацию в архив. Управление политиками Linux-агентов происходит через единую консоль управления Zecurion, при этом политики также универсальны для Windows и Linux-агентов. Это существенно упрощает работу сотрудника безопасности и сокращает время на настройку системы и обработку данных по инцидентам. На данный момент система представлена в бета-версии и дорабатывается для поступления в продажу [5].

Возможно, другие компании в скором времени представят заказчикам версии своих систем контроля и предотвращения утечки информации, однако разработка осложняется тем, что в отечественных дистрибутивах защищенных операционных систем на базе Linux есть встроенные механизмы защиты, которые зачастую рассматриваются администраторами как механизмы, достаточные для обеспечения безопасности ПЭВМ.

Библиографический список

1. Сравнительный анализ DLP-систем. Часть 1 // anti-malware.ru : информ.-справочный портал. – URL : https://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1 (свободный).
2. Сравнительный анализ DLP-систем. Часть 2 // anti-malware.ru : информ.-справочный портал. – URL : https://www.anti-malware.ru/comparisons/data_leak_protection_2014_part2 (свободный).
3. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 // ФСТЭК России : официальный сайт. – URL : https://fstec.ru/tekhnicheskaya- zaschita-informatsii/dokumenty-po-sertifickatsii/153-sistema–sertifikatsii/591(свободный).
4. Система Zecurion // Zecurion : официальный сайт разработчиков. – URL : https://www.zecurion.ru/solution/dlp/data-loss-prevention/ (свободный).
5. Система DeviceLock 8 DLP Suite // DeviceLock DLP : официальный сайт разработчиков. – URL : https://www.devicelock.com/ru/products/ (свободный).

Образец цитирования:

Лабазин, М. А. Применение средств контроля и предотвращения утечки информации / М. А. Лабазин, А. Г. Фатеев // Инжиниринг и технологии. – 2020. – Vol. 5(1). – С. 1–5. – DOI 10.21685/2587-7704-2020-5-1-2.