где $E_z$ — вес, приписываемый оценке z-го эксперта; FV — функциональная возможность (основная или дополнительная); $\varphi$ *(VF)* — ранг функциональной возможности; k — оценка функциональной возможности; $\psi$ *(G)*— ранг группы функциональных возможностей.

Разработанная методика комплексной оценки функциональных возможностей АПМДЗ обеспечивает оценивание уровня функциональной безопасности всего устройства в зависимости от архитектуры построения функциональных подсистем и параметров их настроек.

Для выбора устройства АПМДЗ, предлагаемого к применению в АС ЗИ, будут проводиться испытания на основании разработанной методики, по итогам которых будет выбран показавший наилучшую результативность модуль.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Беляева Е. А.* Разработка методики комплексного тестирования многофункциональных аппаратно-программных средств защиты информации // XIV Международная телекоммуникационная конференция студентов и молодых ученых «Молодежь и наука». Тезисы докладов. Ч. 3. М.: НИЯУ МИФИ, 2010. – С. 223.
2. Системный анализ и принятие решений: словарь-справочник: учеб. пособие для вузов / Под ред. В. Н. Волковой, В. Н. Козлова. М.: Высш. шк., 2004. – 616 с.

*И. С. Боридько, А. А. Забелинский, Ю. И. Коваленко*

## DLP-СИСТЕМЫ: ЗАЩИТА ОТ ИНСАЙДЕРОВ

Современные информационные системы позволяют оперативно собирать информацию, систематизировать и группировать ее, ускоряя процессы принятия управленческих решений и обеспечивая прозрачность деятельности организации и для руководства, и для сотрудников.

Становится очевидным, что большое количество стратегических данных конфиденциального характера является важным информационным ресурсом организации и последствия потенциальной утечки этой информации скажутся на эффективности деятельности организации.

Традиционные средства обеспечения информационной безопасности, такие как системы обнаружения атак, межсетевые экраны, антивирусные программы, выполняют функции защиты информационных активов 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 [1].

Решить проблему случайных и умышленных утечек конфиденциальных данных позволяют DLP-системы (*Data Leak Prevention System*), или системы предотвращения утечек [2,3].

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

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. Защита конфиденциальной информации осуществляется DLP-системой при помощи следующих

основных функций: фильтрация трафика по всем каналам передачи данных, глубокий анализ трафика на уровне контента и контекста.

В DLP-системах конфиденциальная информация может определяться по ряду различных признаков, а также различными способами, например: лингвистический анализ информации, статистический анализ информации; регулярные выражения (шаблоны); метод цифровых отпечатков и т. д. После того как информация найдена, сгруппирована и систематизирована, необходимо предпринять меры по ее дальнейшей обработке, например, произвести ее блокирование.

После внедрения DLP-системы организация получит: защиту информационных активов и важной стратегической информации компании; структурированные и систематизированные данные в организации; прозрачность информационных процессов для руководства и служб безопасности; контроль процессов передачи конфиденциальных данных; снижение рисков, связанных с потерей, кражей и уничтожением важной информации; защиту от вредоносного программного обеспечения, попадающего в организацию изнутри; сохранение и архивацию всех действий, связанных с перемещением данных внутри информационной системы. Кроме того, имеются вторичные плюсы от применения DLP-систем: контроль присутствия персонала на рабочем месте; экономия интернет-трафика; оптимизация работы корпоративной сети; контроль используемых пользователем приложений; повышение эффективности работы персонала.

В настоящее время среди систем внутренней безопасности по-прежнему лидируют решения на базе контентной фильтрации, которые используют 80 % компаний, решившихся внедрить системы защиты от утечек. Вместе с контентной фильтрацией компании используют пассивный мониторинг (77 %), а также внедряют контроль использования портов рабочих станций (75 %).

В качестве примеров DLP-систем можно назвать InfoWatch Traffic Monitor Enterprise — комплексное модульное решение по защите информации от внутренних угроз, которое позволяет контролировать различные каналы утечки данных. В интеграции с устройствами веб-фильтрации и системами электронного документооборота (такими как Blue Coat ProxySG, Cyan Secure Web, Aladdin eSafe, Cisco IronPort, Oracle IRM) InfoWatch Traffic Monitor Enterprise позволяет комплексно обеспечить информационную безопасность компании.

Другим примером DLP-систем является система Zlock — программное обеспечение для разграничения прав доступа пользователей к внешним и внутренним устройствам компьютера и к локальным и сетевым принтерам. Zlock относится к семейству IPC/DLP-систем и позволяет архивировать распечатываемые на принтерах документы и файлы, записываемые на USB-, CD-, DVD-носители и другие устройства. Выпускает данный продукт российская фирма SecurIT.

**Итак, организации практически всех отраслей и масштабов продолжают допускать утечки (только 5 % заявили об отсутствии каких-либо инцидентов).**

Вместе с тем имеются и положительные тенденции — гораздо большее количество специалистов стали осознавать собственную незащищенность и уязвимость своей компании перед действиями инсайдеров, около 40 % российских компаний заявляют о планах внедрения защиты от утечек в ближайшее время.

Следовательно, в процессе подготовки специалистов в области информационной безопасности необходимо больше внимания уделять вопросам, связанным с защитой от утечек, в том числе и DLP-системам.

## СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями от 27 июля 2010 г., 6 апреля, 21 июля 2011 г., 28 июля 2012 г.).

2. *Игнатенко А., Раевский А.* Неосведомленность сотрудников — слабое место защиты информации // Управление персоналом. 2010. № 22. С.46-51.
3. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 4 мая 2012 г. № 240/24/1701 «О работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа».

*С. П. Ботуз, Д. О. Кожедуб, А. Е. Назимкин, А. А. Самошкин*

## МЕТОДЫ И МОДЕЛИ ПРОГРАММНОГО КОМПЛЕКСА ЗАЩИТЫ И СОПРОВОЖДЕНИЯ СУБЪЕКТОВ И ОБЪЕКТОВ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ В СЕТИ ИНТЕРНЕТ/ИНТРАНЕТ

Рассматриваются состав и структура разработанного программного комплекса (ПК) загрузочных модулей защиты и сопровождения субъектов и объектов интеллектуальной собственности (ОИС) в сети Интернет/Интранет на примерах сопровождения таких объектов промышленной собственности (ОПС), как изобретения и полезные модели.

Основная особенность разработанного ПК состоит в том, что в его состав включены кроме таких широко известных методов шифрования, как DES, ГОСТ 28147-89, RSA и др. [1], оригинальные методы когнитивной защиты ОПС: сетевые средства сопровождения и защиты ОПС на основе использования графоаналитического метода / способа кодирования / декодирования измерительной информации о состоянии систем защиты и сопровождения в сети ОИС [2, 3].

Основная цель ПК — автоматизация когнитивных процессов поискового проектирования и экспертизы технически оптимальных позиционных систем защиты и синтеза проблемно-ориентированных стратегий сопровождения ОПС на основе эффективного использования открытых сетевых технологий Интернет/Интранет.

Основные функции ПК:

— синтез персонифицированных / адаптивных электронных / дистанционных курсов обучения с использованием открытых сетевых интернет/интранет-технологий;

— поисковое проектирование средств защиты и активного сопровождения ОПС ограниченной/минимальной сложности;

— синтез стратегий маркетинга и экспертизы состояния соответствующих объектов промышленной собственности (изобретений, полезных моделей и тому подобных инновационных решений в области систем программного управления и контроля на основе использования открытых сетевых технологий Интернет/Интранет) в условиях необходимости обеспечения требований их патентоспособности;

— разработка (автоматизированный синтез), исследование и сопровождение сетевых моделей формирования графоаналитических методов описания основных процессов проектирования, защиты и сопровождения систем/среды взаимодействия субъектов и объектов промышленной собственности;

— многокритериальная графоаналитическая оценка эффективности систем защиты и сопровождения ОПС в сети Интернет/Интранет.