ступа: http://ru.wikipedia.org/wiki/Контроль_доступа (информатика)/
3. Что такое двухфакторная аутентификация. Юрий Медяков 14.01.2014 / [Электронный ресурс]. – Режим доступа: https://cryptostore.ru/article/obzory/chto_takoe_dvukhfaktornaya_autentifikatsiya/

ПРИМЕНЕНИЕ DATA LOSS PREVENTION ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ОТ ИНСАЙДЕРСКИХ УГРОЗ

И.А. Красников, АлтГТУ, факультет информационных технологий, 5 к.
Научный руководитель – ***Е.В. Шарлаев***, к.т.н., доцент.

Распространение информационных технологий и тенденция подключения государственных информационных систем (ГИС) к информационно-телекомуникационным сетям общего пользования являются порождающим фактором увеличения риска реализации инсайдерских угроз информационной безопасности организаций. Согласно нормативно-правовым актам (НПА) в области обеспечения защиты информации в ГИС, таких как ФЗ №152 «О персональных данных», Постановление правительства 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Приказ ФТЭК от 13.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказ ФСТЭК 18.02.13 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Руководящие документы ФСТЭК, необходимо использование сертифицированных по требованиям безопасности средств защиты информации. Делая акцент на увеличение количества утечек конфиденциальной информации в сеть, следует предпринимать своевременные меры по нейтрализации

данного типа угроз посредством разработки, внедрения и эксплуатации DLP – систем. Использование данной технологии в совокупности с профессиональной настройкой системы, опираясь на перечень сведений конфиденциального характера, выполненной по требованиям НПА, позволяет сократить уровень риска утечки КИ до приемлемого уровня и существенно упростить технические мероприятия по расследованию возможных инцидентов.

Предотвращение утечек (Data Loss Prevention, DLP) – технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек [4]. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется. Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента.

К основным задачам DLP – систем относятся следующие:

1. предотвращение передачи конфиденциальной информации за пределы информационной системы;
2. архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;
3. выявление инсайдеров внутри компании;
4. повышение эффективности работы отдела по защите информации;
5. предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;
6. оптимизация загрузки каналов, экономия трафика;
7. контроль присутствия работников на рабочем месте;
8. отслеживание благонадёжности сотрудников.

Основными методами детектирования конфиденциальной информации являются:

1. Сигнатуры – поиск в потоке данных некоторой последовательности символов. Достоинство: простота пополнения

словаря запрещённых терминов. Недостаток: лингвистическое разнообразие словесных форм.

2. Цифровые отпечатки – детектирование на основе хэшей шаблонов. Достоинство: простота добавления новых шаблонов, высокую степень детектирования и прозрачность алгоритма технологии для сотрудников подразделений по защите информации. Недостаток: необходимость постоянного обновления базы данных «цифровых отпечатков».
3. Метки – расстановка специальных «меток» внутри файлов. Достоинство: высокое качество детектирования. Недостаток: значительная перестройка инфраструктуры внутри сети и введение множества новых правил и форматов файлов для пользователей.
4. Регулярные выражения – нахождение совпадения по форме данных. Достоинства: позволяют детектировать специфичный для каждой организации тип контента. Недостаток: ограниченная сфера применения в рамках DLP – систем и невозможность применения независимо от других технологий.
5. Лингвистические методы – основаны на лингвистическом анализе текста. Достоинства: высокая степень эффективности при намного меньших трудозатратах на внедрение и поддержку. Недостаток: зависимость от языка.
6. Ручное детектирование – фильтрация контента специалистом по защите информации. Достоинства: высокое качество детектирования. Недостаток: ограниченный объём контента.

Современные DLP – системы имеют следующие функции:

1. Контроль доступа к устройствам и интерфейсам. Обеспечение контроля доступа пользователей и групп к портам ввода-вывода, адаптерам WiFi и Bluetooth, любым типам принтеров, мобильным устройствам и дисководам.
2. Контроль сетевых коммуникаций. Обеспечение детектирования коммуникационных приложений и их селективную блокировку.
3. Мониторинг и фильтрация трафика. Информация анализируется на предмет соответствия корпоративным политикам безопасности.

4. Централизованное управление. Полная интеграция централизованного управления в групповые политики Windows.
5. Контроль по типу файлов. Разрешение и запрет доступа к определенным типам файлов.
6. Контроль буфера обмена. Предотвращение утечки данных при намеренном или случайном копировании между различными приложениями и документами через встроенный в ОС Windows буфер обмена.
7. Межсетевое экранирование.
8. Белый список носителей и сетевых протоколов. Для каждого пользователя или группы можно задать свой "белый" список, доступ к которым будет всегда разрешен.
9. Аудит. Протоколирование всех действий пользователей с устройствами и файлами.
10. Централизованное хранение журналов аудита и теневого копирования.

В качестве объектов сравнительного анализа были взяты три DLP - системы российских разработчиков: DeviceLock, InfoWatch Traffic Monitor Enterprise и Дозор Джет.

Для проведения сравнительного анализа DLP - систем были выбраны следующие критерии: [5]

1. Позиционирование системы на рынке.
2. Системные требования.
3. Используемые технологии детектирования.
4. Контролируемые каналы передачи данных.
5. Возможности контроля подключаемых внешних устройств.
6. Мониторинг агентов и их защита.
7. Управление системой и обработка инцидентов.
8. Отчетность.
9. Интеграция с решениями сторонних производителей.

Рассмотренные DLP – системы полностью удовлетворяют требованиям российского законодательства и имеют идентичные функциональные возможности по основным критериям анализа. Ключевым фактором выбора средства защиты информации является наличие свободно распространяемой полнофункциональной демонстрационной версии, так как разработка и внедрение проекта системы защиты от утечки конфиденциальной информации будет реализовано в виртуальной среде. Услуга по предоставлению де-

мо-версий доступна только для продуктовой линейки DeviceLock 7 Endpoint DLP Suite. При последующем внедрении проекта в автоматизированную информационную систему важным элементом является стоимость DLP – системы. Очевидное преимущество комплекса DeviceLock заключается в возможности активации лицензий только на необходимые компоненты в зависимости от потребностей организации.

Методика внедрения и эксплуатации DLP – системы имеет следующие этапы:

1. определение целей и задач DLP;
2. классификация данных;
3. определение рисков и каналов утечки данных;
4. разработка политик безопасности;
5. определение компонентов необходимых для построения DLP;
6. определение областей реорганизации существующей структуры сети;
7. техническое внедрение системы;
8. определение необходимых настроек DLP;
9. тестирование;
10. осуществление управления и отчётности.

Проанализировав функционал DLP – систем, можно сделать вывод о том, что данная технология обладает высокой эффективностью и имеет перспективы развития. Становится очевидно, что блокирование доступа в интернет является нерациональным способом ограждения информационных систем от существующих угроз, так как это влечёт за собой усложнение или полный отказ информационного взаимодействия посредством телекоммуникационных сетей общего пользования. Поэтому DLP – системы становятся необходимым элементом в системе защиты информационных систем и используются в совокупности с СЗИ от НСД, МЭ и антивирусными средствами.

Список литературы

1. INFOWATCH TRAFFIC MONITOR ENTERPRISE «Естественное и искусственное освещение» [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/products/ traffic_ monitor_enterprise/

2. Комплекс защиты от утечек информации Дозор Джет [Электронный ресурс]. – Режим доступа: http://www.dozor-jet.ru/
3. DeviceLock защита от инсайдеров [Электронный ресурс]. – Режим доступа: http://www.devicelock.com/ru/
4. DLP – Википедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/DLP
5. Сравнение систем защиты от утечек [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1

ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕЛЕКТИВНЫХ МЕТАЛЛОДЕТЕКТОРОВ НА ОСНОВЕ МИКРОКОНТРОЛЛЕРА

А.Ю. Лаптев, АлтГУ, физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Рост числа объектов информатизации, обрабатывающих и хранящих конфиденциальные данные, ставит жесткие требования к комплексному подходу обеспечения информационной безопасности. Важную роль в решении этой задачи играют различные технические средства, позволяющие выявлять несанкционированные устройства для съема информации [1]. Эффективность такого обнаружения зависит не только от методов измерений, но и от алгоритмов обработки сигналов, регистрируемых измерительными датчиками. В селективных поисковых системах, как правило, приходится определять параметры гармонических сигналов. При этом полезную информацию, как правило, несут не абсолютные значения сигнала, а их небольшие изменения. Из существующих методов обработки широкое применение нашли цифровые методы, использующие аппроксимацию мгновенных значений сигнала исходной модельной функцией. При реализации данного подхода приходится накапливать сумму произведений мгновенных значений сигнала на значения тригонометрических функций, что предъявляет повышенные требования к производительности микроконтроллеров. В настоящей работе для определения комплексной амплитуды гармонического сигнала использовали функции Уолша [2], что позволило существенно снизить вычислительную нагрузку на микроконтроллер без ухудшения точности измерений.