УДК 621.391 DOI: 10.18698/2541-8009-2019-05-474

СИСТЕМА АНАЛИЗА И ПРЕДУПРЕЖДЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ

А.Т. Левинский adam.levinskiy@yandex.ru
SPIN-код: 2301-6960

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Правила информационной безопасности играют ключевую роль в обеспечении защиты систем и сети. Продуманные, реализованные и внедренные правила информационной безопасности помогут почувствовать разницу между наметками безопасности и организованной системой безопасности, которая эффективно функционирует. Тема данной статьи «Система анализа и предупреждения угроз безопасности персональных данных на предприятии». В результате разработан проект системы анализа и предупреждения угроз безопасности персональных данных на предприятии, приведено его сравнение с действующим аналогами. Безопасность в информационных технологиях понимается как комплекс мер и воспринимается как единая система. Компьютерная безопасность может иметь разные аспекты, среди которых нет более или менее значимых, здесь важно все. Нельзя просто взять и отказаться от части каких-то мер, иначе система просто не заработает.

Ключевые слова

DLP-системы, безопасность, эффективность, Zecurion DLP, HTTP, FTP, блокирование, массив, данные, протокол

Поступила в редакцию 04.04.2019

Введение. Актуальность работы связана с все увеличивающимся количеством утечек информации в организациях и необходимостью защиты от таких утечек. Эти задачи выполняют так называемые DLP-системы.

Сегодня на рынке существует довольно много продуктов, позволяющих детектировать и предотвращать утечку конфиденциальной информации по тем или иным каналам. Однако комплексных решений, покрывающих все существующие каналы, значительно меньше. В этих условиях чрезвычайно важным становится выбор технологии, обеспечивающей защиту от утечек конфиденциальной информации с максимальной эффективностью и минимальным количеством ложных срабатываний.

Цель данной работы — разработка системы анализа и предупреждения угроз безопасности персональных данных на предприятии.

Задачами данной работы являются:

– исследование понятия «информационная безопасность»;

– классификация каналов утечки информации;

– анализ особенностей DLP-систем и их места в системе информационной безопасности компании;

– проведение сравнительного анализа DLP-систем;

– разработка проекта системы анализа и предупреждения угроз безопасности персональных данных на предприятии;

– тестирование проекта в рамках разработанной системы.

Обзор коммерческих систем анализа и предупреждения угроз безопасности персональных данных. Под системой анализа и предупреждения угроз понимается система, которая способна обеспечить контроль возможных угроз информации и предупредить об их появлении.

В качестве таких систем будем рассматривать систему защиты от утечек конфиденциальной информации в результате реализации внутренних угроз — DLP (Data Loss Prevention) [1]. Самые строгие и непротиворечивые критерии принадлежности к DLP-системам представлены исследовательским агентством Forrester Research в ходе их ежегодного исследования этого рынка. Они вывели четыре критерия, на основе которых систему можно отнести к классу DLP [2].

1. *Многоканальность*. Система способна реализовать мониторинг нескольких возможных каналов утечки информации. В сетевом окружении это обычно e-mail, Web и IM (instant messengers), а не только проверка почтового трафика или активности базы данных. На рабочей станции это отслеживание файловых операций, работы с буфером обмена информацией.

2. *Унифицированный менеджмент*. Система имеет привычные средства управления политикой ИБ, анализом и отчетами о событиях по каждому каналу мониторинга.

3. *Активная защита*. Система не только позволяет находить факты нарушения политики безопасности, но и при необходимости поддерживает возможность принуждения к ее соблюдению. Например, она может блокировать подозрительные сообщения или спам.

4. *Учет как содержания, так и контекста*. В процессе описания документов, циркулирующих по определенным каналам утечки данных, важно учитывать не только ключевые слова и регулярные выражения, которые могут присутствовать в этом документе, но и его ключевое содержание. Система также должна обращать внимание и на контекст — тип приложения, протокол, активность, отправитель, адресат и т. п.

Это непростая программная система, которая умеет не только собирать данные, но и распознавать подозрительную активность пользователя (например, ту, которая предшествует «сливу» сведений), а также составлять аналитические отчеты по различным информационным срезам. Если в организации есть настоящий инсайдер, он себя проявит, и тогда архив запротоколированных действий станет основой расследования.

Логика работы DLP вовсе не сложна. Решение объединяет в себе контроль над перемещением информации как на уровне коммуникаций с внешней сетью, так и на уровне оконечных устройств пользователей (рис. 1).

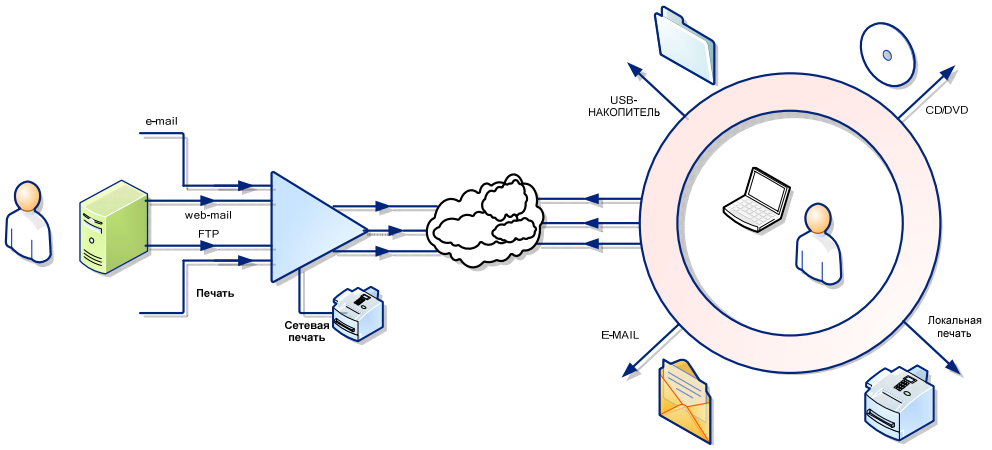

Рис. 1. Контроль утечки информации по сетевым каналам организации и от локальных рабочих станций пользователей с помощью DLP-системы

Важной дополнительной функцией классического решения DLP является возможность сканирования хранящихся файлов и баз данных для обнаружения мест расположения конфиденциальной информации.

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

– перехватчики/контроллеры на разные каналы передачи информации;

– агентские программы, устанавливаемые на оконечные устройства;

– центральный управляющий сервер.

На рис. 2 показан пример схемы развертывания модулей решения DLP в инфраструктуре организации.

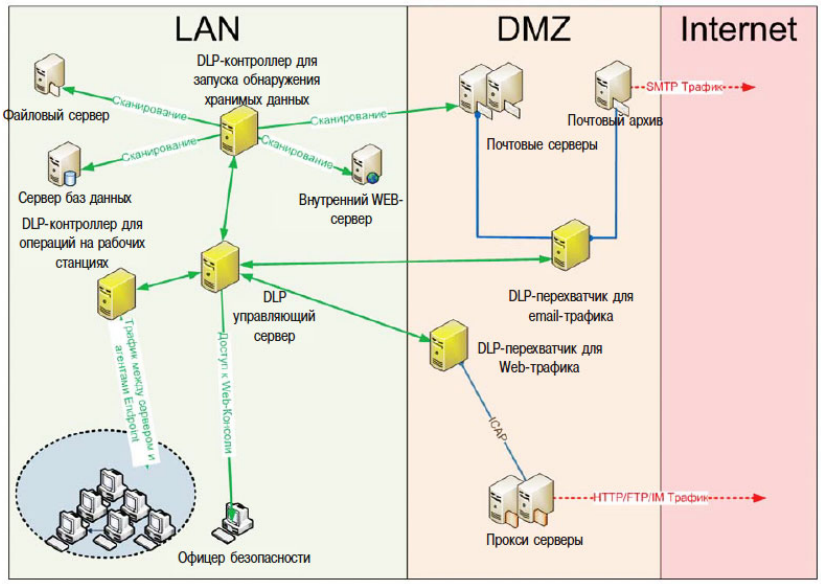

Рис. 2. Типовая архитектура построения системы DLP

Перехватчики исследуют потоки данных, которые могут выводиться из периметра компании, определяют секретные данные, описывают информацию и передают для обработки допустимого инцидента на управляющий сервер. Перехватчики организуются как для копирования исходящего трафика, так и для внедрения в разрыв трафика. В последнем случае утечка данных может быть зафиксирована и остановлена DLP-системой.

Контроллеры для отслеживания хранимых данных активируют процессы поиска в сетевых ресурсах секретной информации. Способы запуска отслеживания могут быть разными: от сканирования сервера контроллера до запуска некоторых программных агентов на установленные серверы или рабочие станции.

Основное назначение DLP — обеспечивать защиту от случайного или намеренного распространения конфиденциальной информации со стороны сотрудников, имеющих доступ к информации в силу своих должностных обязанностей. Помимо того, любая DLP может быть настроена и для борьбы со злонамеренными инсайдерами [3]. Естественно, для того чтобы система DLP достоверно различала конфиденциальную и открытую информацию, необходимо передать в систему логику, на основании которой должна происходить классификация. Встроенные механизмы DLP позволяют максимально автоматизировать и облегчить процессы обучения системы.

Решения DLP хорошо подходят для того случая, когда крупная организации ведет активный, но слабо поддающийся управлению обмен документами с внешними контрагентами; а при этом стоит задача обеспечения конфиденциальности этого процесса. Система DLP будет просматривать все информационные потоки и информацию, выводимую на сменные устройства записи, обнаруживать конфиденциальные данные в потоках и активно реагировать на обнаруженные попытки распространения конфиденциальной информации. Например, из медицинского учреждения не сможет беспрепятственно произойти утечка выгрузка историй болезней сразу сотни человек частному лицу, из компании — база кредитных карт и персональные данные клиентов, а из производственного предприятия — случайная копия файла, содержащая внутренние разработки. По результатам перемещений конфиденциальных данных ведется подробная статистика с возможностью отслеживания соответствия требованиям действующих стандартов безопасности.

Основными задачами технической системы защиты от утечек являются:

– получение описания защищаемых данных (настройка системы);

– распознавание защищаемых данные в потоке, исходящем из внутреннего информационного поля компании вовне (распознавание действий, направленных на перемещение конфиденциальных данных);

– своевременная реакция на обнаруженные попытки (формирование доказательной базы для расследования инцидентов).

Решения, наиболее точно соответствующие такому профилю, заслужили высшей оценки в исследовании Gartner.

На сегодняшний день на рынке существует несколько полноценных решений, как отечественных, так и зарубежных. Сравним некоторые из них.

Российские:

– Zecurion DLP;

– Solar Dozor (ранее Dozor Jet).

Зарубежные:

– Symantec Data Loss Prevention (DLP);

– Trend Micro Data Loss Prevention (DLP).

Результаты сравнения этих решений по основным критериям показаны в табл. 1 и на рис. 3 (в баллах).

Таблица 1

Сравнение DLP-систем по основным критериям

Критерий	Zecurion DLP	Solar Dozor	Symantec Data Loss Prevention	Trend Micro Data Loss Prevention
Управление журналами и отчетность по соответствию	3,6	4,1	4,0	2,8
Мониторинг доступа к данным и действий пользователей	2,8	4,7	3,0	2,0
Мониторинг выполнения приложений	3,2	3,1	3,1	2,8
Нормализация и классификация событий безопасности	3,0	4,3	2,6	4,0
Анализ событий безопасности в реальном времени	3,0	3,5	2,0	2,7
Простота развертывания и поддержки	4,2	3,0	3,6	2,6

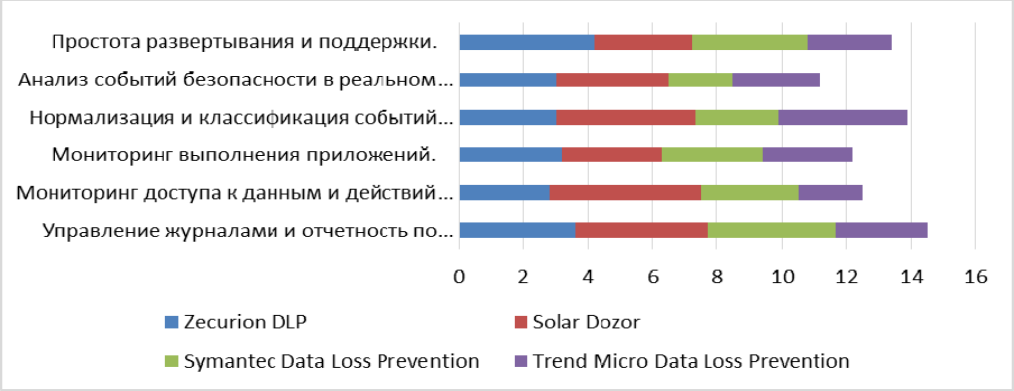

Рис. 3. Сравнение DLP-систем по основным критериям

Сравнение DLP-систем по каналам утечки приведено в табл. 2 и на рис. 4.

Как можно увидеть на рис. 4, все рассматриваемые системы имеют низкий уровень реализации защиты при передаче данных по HTTP, FTP и иным протоколам.

Необходимо разработать решение, которое позволит отслеживать несанкционированную передачу определенных (защищаемых) файлов по сети.

Таблица 2

Сравнение по модели использования

Модель использования	Zecurion DLP	Solar Dozor	Symantec Data Loss Prevention	Trend Micro Data Loss Prevention
Электронная почта (E-mail)	3,3	3,9	2,8	3,1
Интернет-пейджеры	3,4	3,8	2,8	3,7
HTTP, FTP и иные протоколы	1,4	1,2	1,6	1,0
Блокирование	3,4	4,1	2,6	3,2
Скорость анализа сетевого трафика	4,0	5,0	3,0	4,0

Разработка архитектуры системы. Один из вариантов решения данной проблемы — создание анализатора сетевых пакетов (сниффера), который будет просматривать и анализировать сетевой трафик с целью выявления сигнатур защищаемых файлов [5]. Однако данный вариант имеет следующие потенциальные проблемы:

– необходимость встраивания сниффера в структуру сети для обеспечения возможности обработки всех пакетов;

– вынужденная расшифровка зашифрованного трафика (основная проблема).

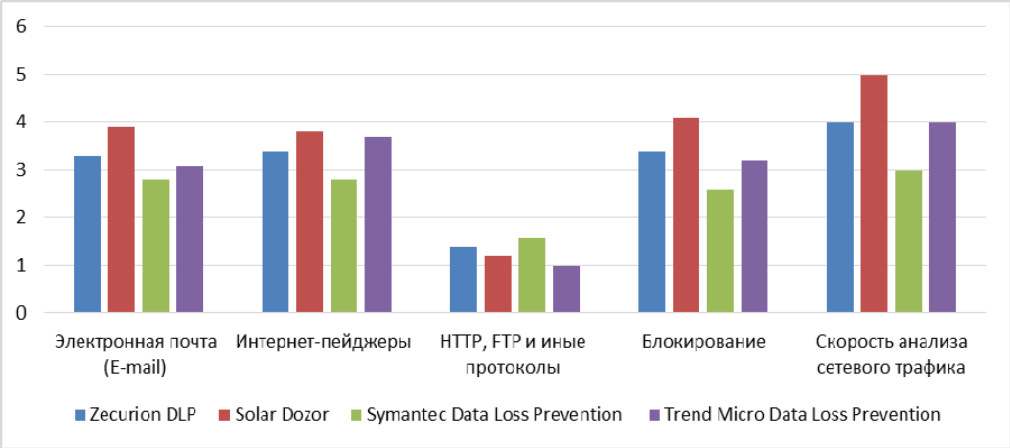

Рис. 4. Сравнение DLP-систем по каналам утечки

Анализаторы сетевых пакетов, или снифферы, первоначально были разработаны как средство решения сетевых проблем. Они умеют перехватывать, интерпретировать и сохранять для последующего анализа пакеты, передаваемые по сети. С одной стороны, это позволяет системным администраторам и инженерам службы технической поддержки наблюдать за тем, как данные передаются по сети, диагностировать и устранять возникающие проблемы. В этом смысле пакетные снифферы представляют собой мощный инструмент диагностики сетевых проблем. С другой стороны, подобно многим другим мощным средствам, изначально предназначавшимся для администрирования,

с течением времени снифферы стали применять абсолютно для других целей. Действительно, сниффер в руках злоумышленника представляет собой довольно опасное средство и может использоваться для завладения паролями и другой конфиденциальной информацией.

Однако не стоит думать, что снифферы — это некий магический инструмент, посредством которого любой хакер сможет легко просматривать конфиденциальную информацию, передаваемую по сети. И прежде чем доказать, что опасность, исходящая от снифферов, не столь велика, как нередко преподносят, рассмотрим более детально принципы их функционирования [6]. В дальнейшем мы будем рассматривать только программные снифферы, предназначенные для сетей Ethernet. Сниффер — это программа, которая работает на уровне сетевого адаптера NIC (Network Interface Card) (канальный уровень) и скрытым образом перехватывает весь трафик. Поскольку снифферы работают на канальном уровне модели OSI, они не должны подчиняться протоколам более высокого уровня. Снифферы обходят механизмы фильтрации (адреса, порты и т. д.), которые драйверы Ethernet и стек TCP/IP используют для интерпретации данных. Пакетные снифферы захватывают всю информацию, проходящую по сети. Снифферы могут сохранять кадры в двоичном формате и позже расшифровывать их, чтобы раскрыть информацию более высокого уровня, спрятанную внутри (рис. 5).

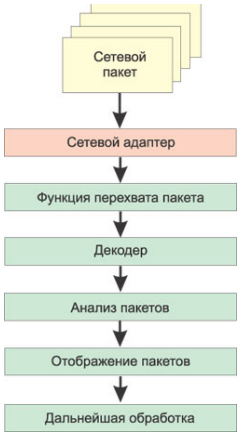

Рис. 5. Схема работы сниффера

Для того чтобы сниффер мог перехватывать все пакеты, проходящие через сетевой адаптер, драйвер сетевого адаптера должен поддерживать режим функционирования promiscuous mode (беспорядочный режим). Именно в этом режиме работы сетевого адаптера сниффер способен перехватывать все пакеты. Данный режим работы автоматически активизируется при запуске сниффера или устанавливается вручную соответствующими настройками сниффера.

Весь перехваченный трафик передается декодеру пакетов, который идентифицирует и расщепляет пакеты по соответствующим уровням иерархии. В зависимости от возможностей конкретного сниффера представленная информация о пакетах может впоследствии дополнительно анализироваться и фильтроваться.

Наибольшую опасность снифферы представляли в те времена, когда информация передавалась по сети в открытом виде (без шифрования), а локальные сети строились на основе концентраторов (хабов — hub). Однако эти времена безвозвратно ушли, и в настоящее время использование снифферов для получения доступа к конфиденциальной информации — задача отнюдь не из простых.

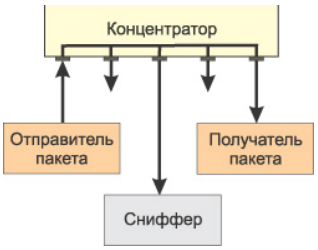

Рис. 6. Работа сниффера при использовании концентраторов (перехват всех пакетов сетевого сегмента)

Дело в том, что при построении локальных сетей на основе концентраторов существует некая общая среда передачи данных (сетевой кабель) и все узлы сети обмениваются пакетами, конкурируя за доступ к этой среде (рис. 6), причем пакет, посылаемый одним узлом сети, передается на все порты концентратора и этот пакет прослушивают все остальные узлы сети, но принимает его только тот узел, которому он адресован. Если на одном из узлов сети установлен пакетный сниффер, то он может перехватывать все сетевые пакеты, относящиеся к данному сегменту сети (сети, образованной концентратором).

Коммутаторы (switch) являются более интеллектуальными устройствами, чем широковещательные концентраторы, и изолируют сетевой трафик. Коммутатор знает адреса устройств, подключенных к каждому порту, и передает пакеты только между нужными портами. Это позволяет разгрузить другие порты, не передавая на них каждый пакет, как это делает концентратор. Таким образом, посланный неким узлом сети пакет передается только на тот порт коммутатора, к которому подключен получатель пакета, а все остальные узлы сети не имеют возможности обнаружить данный пакет (рис. 7).

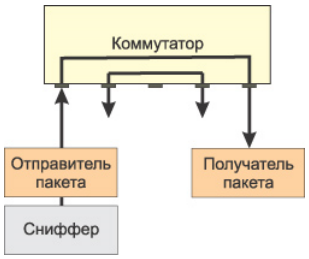

Рис. 7. Работа сниффера при использовании коммутаторов (перехват только входящих и исходящих пакетов одного узла сети)

Поэтому если сеть построена на основе коммутатора, то сниффер, установленный на одном из компьютеров сети, способен перехватывать только те пакеты, которыми обменивается данный компьютер с другими узлами сети. Чтобы иметь возможность перехватывать пакеты, которыми интересующий злоумышленника компьютер или сервер обменивается с остальными узлами сети, необходимо установить сниффер именно на этом компьютере (сервере), что на самом деле не так-то просто. Правда, следует иметь в виду, что некоторые пакетные снифферы запускаются из командной строки и могут не иметь графического интерфейса. Такие снифферы, в принципе, можно устанавливать и запускать удаленно и незаметно для пользователя.

Выбор средств разработки. Для выбора языка программирования сравним языки C++, Delphi и Visual Basic [7]. Сравнение этих языков приведено в табл. 3.

Для разработки информационной системы был выбран язык программирования C++. C++ — это относительно новый язык программирования, который характеризируется следующими преимуществами:

– он спроектирован специально для применения с Microsoft .NET Framework (развитой платформой разработки, развертывания и исполнения распределенных приложений);

– это язык, основанный на современной объектно-ориентированной методологии проектирования, при разработке которого специалисты Microsoft опирались на опыт создания подобных языков, построенных в соответствии с объектно-ориентированными принципами, которые были впервые предложены около 20 лет назад.

Таблица 3

Сравнение языков программирования

Параметр	Степень соответствия, %		
	C++	Delphi	Visual Basic
Возможность компиляции	8	8	4
Многопоточная компиляция	8	0	8
Интерпретатор командной строки	6	4	0
Многомерные массивы	8	0	8
Динамические массивы	8	8	0
Ассоциативные массивы	4	0	0
Интерфейсы	8	0	4
Мультиметоды	8	0	0
Общая оценка	7,25	2,5	3

Проект реализации системы. Перед запуском процесса захвата пакетов нам необходимо выбрать устройство, с которого будет осуществляться захват. Устройство описывается классом LivePacketDevice. После этого для выбранного устройства создается коммуникатор (объект класса PacketCommunicator) — это объект, который выполняет захват пакетов. Объекты данного класса имеют ряд методов, которые выполняют захват: ReceivePackets — захват пакетов, ReceiveStatistics — захват статистики получаемых пакетов. Перечисленные метод являются блокирующими (они блокируют поток, в котором запускаются и принимают пакеты до тех пор, пока не будет вызван метод Break-коммуникатора) и потому метод захвата пакетов запускается в методе DoWork компонента BackgroundWorker (фоновый поток). Методы ReceivePackets в качестве параметра принимает процедуру обратного вызова, в теле которой и выполняется анализ пакета и его сохранение в базе данных. Анализ пакетов выполняется методами класса PacketManager. Основной метод класса, AddPacket, осуществляет сохранение пакета в базе данных и запускает процедуру поиска данных в файлах заданных каталогов. Поиск по двоичным данным защищаемых файлов выполняет объект класса DataScanner, который принимает содержимое пакета и проверяет вхождения содержимого в сигнатуры защищаемых файлов [8]. За обновление статистики и списка захваченных пакетов отвечает таймер, который располагается на главной форме приложение (класс MainForm).

Все данные захваченных пакетов сохраняются в базе данных SQLite.

Схема базы данных представлена на рис. 8, диаграмма классов приложения — на рис. 9.

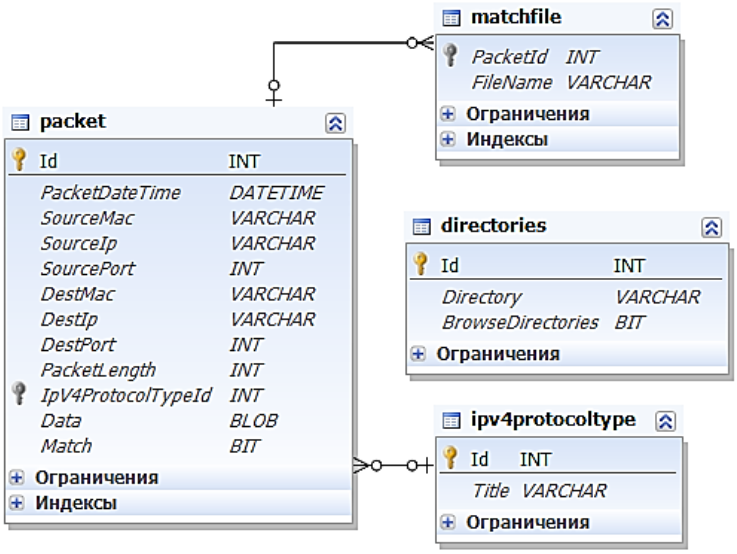

Рис. 8. Схема базы данных

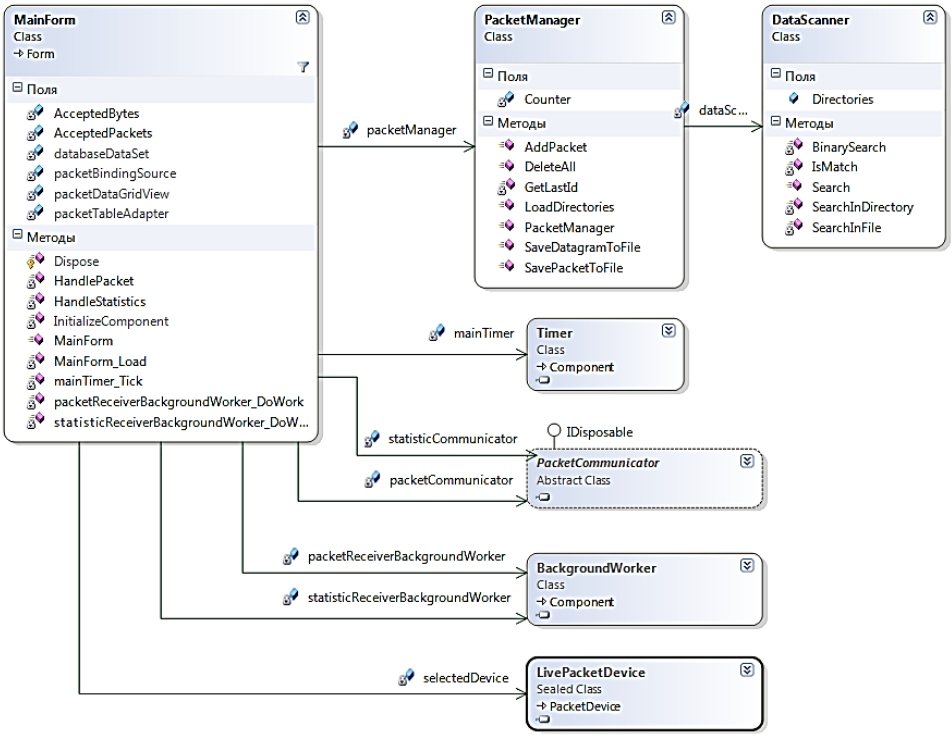

Рис. 9. Диаграмма классов приложения

Класс MainForm — это класс главной формы приложения. Является основой всего приложения и служит основной точкой пользовательского интерфейса приложения.

Тестирование системы. Данные, которые необходимы эксперту для определения функциональности каждой из систем, для настоящего сравнения получены с сайтов производителей, из документации и по результатам тестирования ознакомительных версий программ [9]. Для определения приоритетов составляются матрицы попарных сравнений:

	Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6	Сертификат
Канал 1	1	1/3	1/5	1	1	1	1	1	1	1/3
Канал 2	3	1	1/3	1	1	1	1	1	1	1/3
Канал 3	5	3	1	1	1	1	1	1	1	1/3
Метод 1	1	1	1	1	1/9	1/7	1/7	1/7	1/7	1/3
Метод 2	1	1	1	9	1	5	3	1	3	1/3
Метод 3	1	1	1	7	1/5	1	1	1/5	1/7	1/3
Метод 4	1	1	1	7	1/3	1	1	1/5	1/7	1/3
Метод 5	1	1	1	7	1	5	5	1	1/3	1/3
Метод 6	1	1	1	7	1/3	7	7	3	1	1/3

Экспертные данные сформулированы на основании изложенной выше информации (характеристиках сравниваемых DLP-систем и представлениях об объекте защиты). Сравнения проводились по шкале значимости от 1 до 9 (1 — одинаковая значимость, 3 — незначительное превосходство и т. д., обратные величины — если сравниваемый объект уступает в данной характеристике) [10].

Для каждой из матриц N определяется нормализованный вектор локальных приоритетов со следующими компонентами:

$$\sqrt{\prod_{i=1}^{n} a_{ij}} = a_j,$$

где n — размерность матрицы; a_j — элемент i-й строки матрицы. Таким образом, матрице N сопоставляется вектор a.

Нормирование компонент осуществляется путем деления каждой компоненты вектора a на сумму всех компонент этого вектора:

$$b_j = \frac{a_j}{\sum_{j=1}^{n} ja_j}.$$

Далее определяются приоритеты для сравнения альтернатив по всем критериям:

	Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6
Zecurion DLP	0,08	0,33	0,26	0,33	0,14	0,08	0,08	0,33	0,09
Solar Dozor	0,46	0,33	0,1	0,33	0,72	0,46	0,46	0,33	0,45
Symantec Data Loss Prevention	0,46	0,33	0,64	0,33	0,14	0,46	0,46	0,33	0,45
Trend Micro Data Loss Prevention	0,33	0,1	0,33	0,33	0,1	0,33	0,33	0,1	0,33
Разработанная DLP	0,08	0,33	0,26	0,33	0,14	0,08	0,08	0,33	0,09

Полученный вектор приоритетов для сравнения значимости критериев между собой показан ниже:

Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6
0,059	0,077	0,1	0,02	0,13	0,057	0,059	0,116	0,139

Перемножив матрицы, получим итоговый вектор приоритетов для альтернатив (A — 0,17; B — 0,36; C — 0,46, D — 0,32; E — 0,49). По результатам проведенных вычислений получаем значения общего ранжирования альтернатив: A — 0,17; B — 0,36; C — 0,46, D — 0,32; E — 0,49. Таким образом, наиболее приемлемой альтернативой для оценивающего эксперта является разработанная DLP-система.

Заключение. Каждое из предприятий — разработчиков систем защиты от утечек (DLP) предлагает, как правило, аналогичную структуру системы, отличающуюся только в деталях. Основными модулями такой системы являются:

– контролирующие модули для каждого канала, по которому возможна утечка;

– агентские модули, устанавливаемые на рабочих местах конечных пользователей;

– управляющее звено с панелью управления для администратора системы.

Таким образом, DLP эффективно обеспечивает защиту информации от намеренного несанкционированного распространения как сотрудниками, так и посторонними лицами, имеющими какие-то права доступа в систему.

Литература

[1] Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. СПб., СПбНИУ ИТМО, 2012.

[2] Cser A. The Forrester Wave™: cloud security gateways, Q4 2016. Forrester, 2016.

[3] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М., Форум, Инфра-М, 2017.

[4] Reed B., Wynne N. Magic quadrant for enterprise data loss prevention. Gartner, 2016.

[5] Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность. М., Академия, 2017.

[6] Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах. М., Форум, 2015.

[7] Рассел Д., Кон Р. Сравнение языков программирования. М., Буквика, 2012.

[8] Баранов Ю.Г. Методы принятия управленческих решений. Псков, ПГУ, 2013.

[9] Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб., Наука и техника, 2004.

[10] Ховард М., Лебланк Д., Вьега Дж. 24 смертных греха компьютерной безопасности. СПб., Питер, 2010.

Левинский Адам Тагирович — магистрант кафедры «Информационные системы и телекоммуникации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

SYSTEM FOR ANALYZING AND PREVENTING THREATS TO THE SECURITY OF PERSONAL DATA IN AN ENTERPRISE

A.T. Levinsky
adam.levinskiy@yandex.ru
SPIN-code: 2301-6960

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Information security rules play a key role in ensuring the protection of systems and networks. Sophisticated, implemented, and realized information security rules will help to feel the difference between safety tips and an organized security system that functions effectively. The topic of this article is "System for analyzing and preventing threats to the security of personal data in an enterprise". As a result, a draft system for analyzing and preventing threats to the security of personal data in an enterprise has been developed, and a comparison with the existing analogs is given. Security in information technology is understood as a set of measures and is perceived as a single system. Computer security can have different aspects, among which there is no more or less significant, everything is important here. One can not just give up some measures, otherwise, the system simply will not start working.

Keywords

DLP-systems, safety, efficiency, Zecurion DLP, HTTP, FTP, blocking, array, data, protocol

Received 04.04.2019

References

[1] Katorin Yu.F., Razumovskiy A.V., Spivak A.I. Zashchita informatsii tekhnicheskimi sredstvami [Hardware information protection]. Sankt-Petersburg, SPbNIU ITMO Publ., 2012 (in Russ.).
[2] Cser A. The Forrester Wave™: cloud security gateways, Q4 2016. Forrester, 2016.
[3] Shan'gin V.F. Informatsionnaya bezopasnost' komp'yuternykh sistem i setey [Information security of computer systems and networks]. Moscow, Forum Publ., Infra-M Publ., 2017 (in Russ.).
[4] Reed B., Wynne N. Magic quadrant for enterprise data loss prevention. Gartner, 2016.
[5] Mel'nikov V.P., Kleymenov S.A., Petrakov A.M. Informatsionnaya bezopasnost' [Information security]. Moscow, Akademiya Publ., 2017 (in Russ.).
[6] Vasil'kov A.V., Vasil'kov I.A. Bezopasnost' i upravlenie dostupom v informatsionnykh sistemakh [Safety and access control in information systems]. Moscow, Forum Publ., 2015 (in Russ.).
[7] Russell J. Cohn R., Programming language. VSD, 2012. (Russ. ed.: Sravnenie yazykov programmirovaniya. Moscow, Bukvika Publ., 2012.)
[8] Baranov Yu.G. Metody prinyatiya upravlencheskikh resheniy [Management decision-making technique]. Pskov, PGUPubl., 2013 (in Russ.).

[9] Shcheglov A.Yu. Zashchita komp'yuternoy informatsii ot nesanktsionirovannogo dostupa [Computer information protection from unauthorized access]. Sankt-Petersburg, Nauka i tekhnika Publ., 2004 (in Russ.).

[10] Howard M., LeBlanc D., Viega J. 24 deadly sins of software security. McGraw-Hill, 2009. (Russ. ed.: 24 smertnykh grekha komp'yuternoy bezopasnosti. Sankt-Petersburg, Piter Publ., 2010.)

Levinsky A.T. — Master's Degree Student, Department of Information Systems and Telecommunications, Bauman Moscow State Technical University, Moscow, Russian Federation.