Раздел V

Безопасность программного обеспечения

УДК 004.056.53

А.В. Барабанов, М.И. Гришин
Россия, Москва, ЗАО «НПО «Эшелон»

ПРЕДЛОЖЕНИЯ ПО ФОРМИРОВАНИЮ МЕТАБАЗИСА ОЦЕНКИ СООТВЕТСТВИЯ DLP-РЕШЕНИЙ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В статье рассмотрен подход к формированию метабазиса оценки соответствия DLP-решений по требованиям безопасности информации, в основу которого положен подход стандарта «Общие критерии». Представленный метабазис может применяться при сертификации DLP-решений по требованиям безопасности информации для увеличения детерминированности данного процесса.

Сертификация; DLP; оценка соответствия; «Общие критерии».

В последнее время заметен рост популярности и объемов продаж различных DLP-решений (*data loss prevention*). Это связано в первую очередь с ростом количества нарушений информационной безопасности, связанных с утечкой информации и защищаемых информационных систем.

В соответствии со спецификой применения средств защиты информации в Российской Федерации данные решения должны быть сертифицированы ФСТЭК России по требованиям безопасности информации. Но ввиду отсутствия в настоящее время нормативно-методической базы, регламентирующей требования к данным продуктам, сертификация проводиться на соответствие требованиям техническим условиям, что по определению означает полную неопределенность процесса. Поскольку требования к составу функциональных возможностей не формализованы, под определение сертифицированного продукта одного и того же типа попадают решения принципиально различного уровня. Следует отметить, что ведущие мировые компании-разработчики DLP-решений (*Symantec, McAfee*) к 2012 г. получили сертификаты соответствия ФСТЭК России, что, несомненно, способствует их росту продаж на российском рынке.

Таким образом, в настоящее время назрела необходимость формирования нормативных и методических документов, которые могут быть использованы при сертификации DLP-решений для увеличения детерминированности процесса сертификации.

Общие сведения о DLP-решениях

DLP-системы – класс продуктов, используемых в различных информационных системах, которые предназначены для защиты информации от несанкционированной передачи внутренним нарушителем на основе анализа содержимого передаваемых данных и их окружения. Как правило, данные продукты содержат также средства централизованного управления на основе политик.

DLP-системы обеспечивают защиту информации (данных) организации на всех этапах ее жизненного цикла, т.е. на этапах хранения (*Data At Rest*), передачи

(*Data In Motion*), обработки пользователем (*Data In Use*). Таким образом, DLP-система должна выполнять следующие основные функции по защите информации:

– отслеживание действий пользователей на рабочих станциях, связанных с передачей конфиденциальной информации на отчуждаемые носители через сеть, выводом на печать, сохранением на локальные диски и т. д.;

– контроль потоков информации во время передачи через сеть с использованием различных сетевых протоколов (http, ftp, smtp, p2p, im и другие);

– проверка различных хранилищ данных (базы данных, файловые сервера, системы документооборота, почтовые сервера, рабочие станции и т. д.) на предмет несанкционированного хранения конфиденциальных данных (или хранения таких данных в несанкционированных местах).

Функции, указанные выше, могут быть реализованы как в рамках одного комплексного решения, так и в виде отдельных узконаправленных продуктов.

Исходя из основных функций, выполняемых DLP-системами, их можно разделить на три класса:

1. DLP-системы уровня хоста.
2. DLP-системы уровня сети.
3. DLP-системы уровня хранилищ данных.

В DLP-системе уровня хоста основой является модуль (агент), который функционирует на рабочей станции пользователя в фоновом режиме и обеспечивает отслеживание действий пользователя.

DLP-системы уровня сети обеспечивают перехват сетевого трафика, передаваемого по различным каналам, для проведения его последующего анализа. DLP-данного класса может представлять из себя пассивный сетевой монитор, который получает копию сетевого трафика для анализа или решение, устанавливаемое в разрыв сети, что позволяет перехватывать и блокировать трафик при необходимости.

DLP-система уровня хранилищ данных представляет набор сканеров, позволяющих удаленно или локально (используется специальный агент) осуществлять проверку хранилищ данных на предмет несанкционированного хранения конфиденциальных данных.

Основной задачей, которую необходимо решить, для корректного функционирования всей DLP-системы является идентификация конфиденциальной информации (данных). Все методы по идентификации информации можно разделить на два класса: анализ смыслового содержимого информации (контентный анализ), анализ окружения обрабатываемой информации (контекстный анализ).

Отнесение определенной информации к конфиденциальной (идентификация) может быть произведено на основе анализа окружения данной информации (контекста информации). В качестве контекста можно рассматривать такие атрибуты как тип, формат и размер файла с данными, приложение, обрабатывающее файл, тип устройства или носителя, на который производится копирование информации, пользователь, обрабатывающий информацию и т. д. Выбор анализируемых атрибутов осуществляется в соответствии с технологией обработки информации в организации, политиками безопасности, описанием бизнес-процессов. Методы контекстного анализа являются важной частью, необходимой для функционирования DLP-систем, однако очень часто их бывает недостаточно.

Для более точной идентификации конфиденциальной информации используется анализ содержимого обрабатываемой или передаваемой информации. В этом случае отнесение информации к конфиденциальной производится путем поиска соответствия непосредственно обрабатываемой информации (а не ее внешних атрибутов или окружения) заданным шаблонам, позволяющим идентифицировать

информацию как конфиденциальную. Среди методов идентификации информации с использованием анализа содержимого можно выделить следующие основные:

– анализ по ключевым словам или фразам (заключается в проверке содержимого на предмет наличия заданных в правилах (словарях) ключевых слов или ключевых фраз; сильной стороной метода является простота создания соответствующих правил обнаружения; метод не подходит для анализа неструктурированных, графических данных, кроме того, характеризуется высоким уровнем ложных срабатываний);

– анализ по регулярным выражениям (поиск соответствия фрагментов данных заданным регулярным выражениям; преимущества и недостатки аналогичны предыдущему методу);

– анализ структурированных данных (метод предназначен для идентификации информации из баз данных и электронных таблиц, в ходе анализа проводится сравнение обрабатываемых структурированных данных с эталонными значениями и выявление соответствия);

– анализ по цифровым отпечаткам (анализ производится на основе предварительно сформированных цифровых отпечатков электронных документов с конфиденциальными данными, создание цифровых отпечатков осуществляется с использованием технологий, специфичных для каждого производителя, в ходе анализа проводится поиск полного или частичного совпадений обрабатываемых документов с цифровыми отпечатками; метод применим для файлов любого формата и любых типов данных – графических, текстовых и т.п., метод характеризуется низким уровнем ложных срабатываний, недостатком метода является возможность обхода путем модификации файлов с конфиденциальной информацией для исключения совпадения с эталонными файлами, с которых снимались отпечатки);

– поиск полного совпадения файла, содержащего информацию (проводится побитовое сравнение обрабатываемых файлов с эталонными файлами для выявления их полного соответствия; метод применяется в основном для неизменяемых файлов, например, бинарных, и характеризуется нулевым уровнем ложных срабатываний; недостатком является возможность обхода путем модификации файлов; метод не подходит для файлов, которые подлежат изменению в процессе обработки).

Большая часть DLP-систем в процессе функционирования использует указанные выше методы (возможно, не все) или комбинации указанных методов. Кроме того, реализация методов идентификации конфиденциальных данных может различаться для различных производителей.

DLP-системы обычно предусматривают несколько способов реакции на обнаружение несанкционированных действий с конфиденциальной информацией:

– регистрация попытки в журнале аудита;

– блокировка попытки совершения несанкционированного действия;

– уведомление пользователя и администратора о попытке нарушения;

– удаление, перемещение или копирование в карантин файлов, с которыми проводились несанкционированные действия.

Управление компонентами DLP-систем осуществляется централизованно с использованием специализированных средств. Как правило, DLP-системы обеспечивают защиту своих средств управления с использованием разграничения доступа на основе ролевой модели, идентификации и аутентификации при доступе к средствам управления и т. д.

Подход к формированию метабазиса оценки соответствия DLP-решений

На сегодняшний день в Российской Федерации существуют два принципиально разных подхода к формированию требований безопасности информации, предъявляемых к изделиям информационных технологий. Первый подход – использование строго заданных требований безопасности информации. Яркими результатами данного подхода являются классические руководящие документы Гостехкомиссии России [2], в основу которых был положен подход, используемый при написании «Оранжевой книги». Второй подход – основан на методологии «Общие критерии», принятого в качестве государственного стандарта Российской Федерации [3]. На основе данного подхода ФСТЭК России уже разработан нормативный документ нового поколения, предъявляемый требования к системам обнаружения вторжений [4]. Второй подход следует признать более перспективным при использовании в формировании и других средств защиты информации, например DLP-решений.

На рис. 1 представлена последовательность формирования функциональных требований безопасности (ФТБ) и требований доверия к безопасности (ТДБ) [5].

Изложение среды безопасности объекта оценки ОО должно содержать описание аспектов безопасности среды, в которой предполагается использовать ОО, и ожидаемый способ его применения. Это изложение должно включать:

1) описание предположений безопасности, содержащее аспекты безопасности среды, в которой будет использоваться ОО или предполагается к использованию;

2) описание угроз, включающее все те угрозы активам, против которых требуется защита средствами ОО или его среды;

3) описание политики безопасности организации, идентифицирующее и, при необходимости, объясняющее все положения политики безопасности организации или правила, которым должен подчиняться ОО.

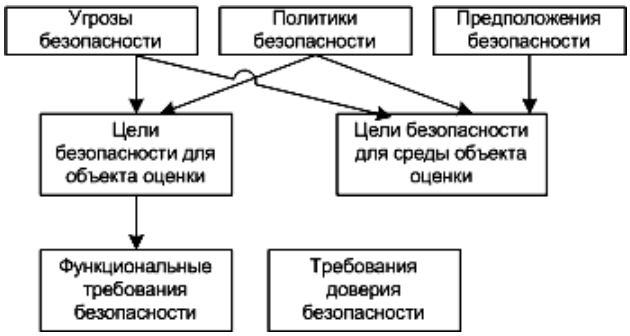

Рис. 1. Последовательность формирования ФТБ и ТДБ

Цели безопасности должны отражать изложенное намерение противостоять всем установленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации. Цели безопасности для ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым необходимо противостоять средствами ОО, или с политикой безопасности организации, которой должен отвечать ОО. Цели безопасности для среды ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым не полностью противостоит ОО, или с политикой безопасности организации и предположениями, не полностью удовле-

творяемыми ОО. При изложении требований безопасности ОО должны быть определены функциональные требования и требования доверия, которым должны удовлетворять ОО.

Результаты анализа существующих DLP-решений позволил сформулировать основные угрозы безопасности (префикс «Т»), которым данные DLP-решения должны противостоять, положения политики безопасности (префикс «Р») и предположения безопасности (префикс «А») (табл. 1).

Таблица 1

Описание аспектов среды безопасности DLP-решений

Обозначение	Описание
T.COMDIS	Неавторизованный пользователь может выполнить попытки раскрытия информации, обрабатываемой DLP-средством, вследствие обхода защитных механизмов
T.SENS_CONTENT	Внутренний нарушитель может выполнить попытки вывода защищаемой информации из информационной системы
P.SENSITIVE_DATA	DLP-средство должно обеспечивать выполнение политики безопасности в части операций с защищаемой информацией
P.MANAGE	DLP-средство должно конфигурироваться уполномоченными администраторами
P.ACCACT	Пользователи DLP-средства должны быть подотчетны
A.NOEVIL	Первоначальная установка и настройка DLP-решения выполняется уполномоченным администратором
A.LOCATE	DLP-средство находится в пределах контролируемой зоны
A.SECCOM	Среда DLP-средств обеспечивает безопасное удаленное взаимодействие распределенных частей DLP-решения между собой и с администратором

Анализ идентифицированных аспектов среды безопасности позволил сформулировать ФТБ (табл. 2).

Таблица 2

Функциональные требования безопасности, предъявляемые к DLP-решениям

Условное обозначение семейства	Наименование функциональной возможности
FMT_MOF	Управление отдельными функциями безопасности DLP-системы
FMT_MTD	Управление данными функций безопасности DLP-системы
FMT_SMR	Роли управления безопасностью
FMT_MOF	Управление отдельными функциями безопасности DLP-системы
FMT_MTD	Управление данными функций безопасности DLP-системы
FAU_GEN	Генерация данных аудита безопасности
FAU_SAR	Просмотр аудита безопасности
FIA_UAU	Определение атрибутов пользователя
FIA_ATD	Аутентификация пользователя
FIA_UID	Идентификация пользователя
FLP_ANL_EXT	Методы анализа информации
FLP_LFC_EXT	Политика управления операциями над информацией
FLP_LFF_EXT	Правила управления операциями над информацией

Следует отметить, что помимо стандартных ФТБ, сформулированных на основе 2 части стандарта «Общие критерии», разработаны специальные ФТБ (с постфиксом «EXT»).

Семейство *FLP_ANL_EXT* содержит требования к методам, применяемым DLP-системой при анализе информации и процесса передачи информации из защищенного сегмента информационной системы в сети связи общего пользования или на носители информации. Результатом анализа является обнаружение информации ограниченного доступа.

Семейство *FLP_LFC_EXT* идентифицирует политики управления операциями над информацией, устанавливая им имена, и определяет области действия политик, образующих идентифицированную часть управления информационными потоками. Эти области действия можно характеризовать тремя множествами: субъекты под управлением политики, информация под управлением политики и операции перемещения информации, на которые распространяется политика. Механизм функций безопасности DLP-систем управляет передачей информации в соответствии с политикой управления операциями над информацией.

Семейство *FLP_LFF_EXT* описывает правила для конкретных функций, которые могут реализовать политики управления операциями над информацией, именованные в FLP_LFC_EXT, где также определена область действия соответствующей политики.

Для формирования классов защиты и ТДБ к данным классам следует использовать подход, приведенных в нормативном документе ФСТЭК России «Требования к системам обнаружения вторжений» (табл. 3).

Таблица 3

Требования доверия к классам защиты DLP-решениям

Класс защиты DLP-системы	Требования доверия безопасности DLP-систем		Уровень контроля отсутствия НДВ
	Оценочный уровень доверия	Дополнительные компоненты доверия к безопасности	
4	ОУД3	ALC_FLR.1 «Базовое устранение недостатков» AVA_VLA.3 «Умеренно стойкий»	4
5	ОУД2	ALC_FLR.1 «Базовое устранение недостатков»	-
6	ОУД1	AVA_SOF.1 «Оценка стойкости функции безопасности ОО»	-

Для высоких классов защиты (1-3) необходимо применять более высокие оценочные уровни доверия (ОУД) и уровни контроля отсутствия недекларированных возможностей [6]. Для каждого типа и класса защиты DLP-решений должны быть разработаны профили защиты (всего – 18 штук), содержащие ФТБ и ТДБ для определенного класса защиты.

Общий алгоритм сертификации DLP-решений в соответствии с предлагаемым метабазисом оценки соответствия представлен на рис. 2.

Как видим, испытания ОО – в нашем случае это DLP-решение – проводятся на соответствие заданию по безопасности, которое представляет собой структурированный и строго формализованный документ, включающий подробное описание ФТБ к DLP-решению и среде его функционирования, а также ТДБ к процессу разработки и эксплуатации DLP-решения. При разработке задания по безопасности DLP-решения определенного класса защиты необходимо использовать типовые

наборы требований – профиль защиты определенного класса защиты. Испытательная лаборатория и орган по сертификации, в свою очередь, при проведении оценки используют различного рода свидетельства – конструкторскую и проектную документацию на изделие, руководства пользователя и администратора, корпоративные стандарты, руководства и процедуры, требования к которым также могут быть сформулированы в задании по безопасности.

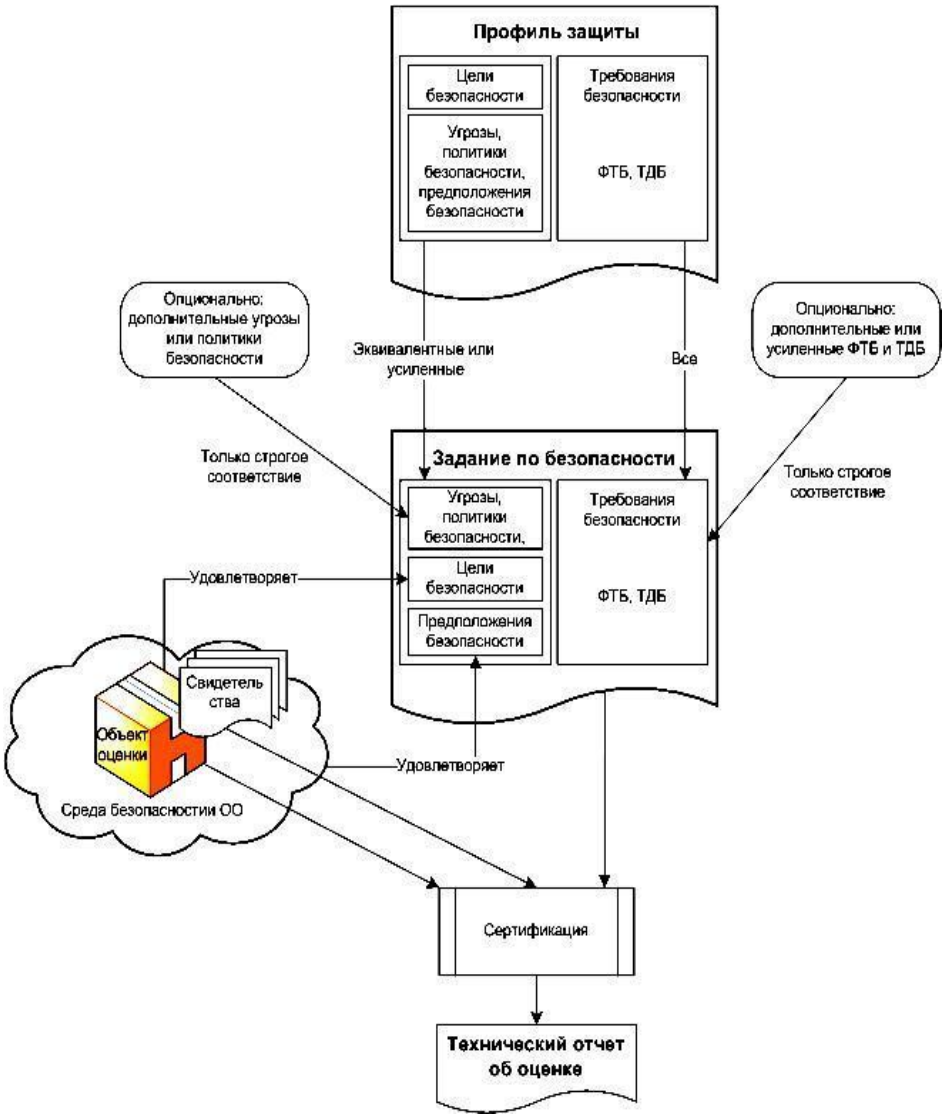

Рис. 2. Порядок проведения сертификации DLP-решений

Предложенный в настоящей работе перечень требований позволяет детерминировать процесс оценки соответствия DLP-решений по требованиям безопасности информации. Представленный подход к формированию метабазиса оценки соответствия DLP-решений требованиям по безопасности информации может най-

ти практическое применение в процессе проведения сертификационных испытаний в системе сертификации средств защиты информации ФСТЭК России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Understanding and Selecting a Data Loss Prevention Solution // Официальный сайт компании Securosis, L.L.C.. URL: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf (дата обращения: 01.05.2012).

2. Сборник руководящих документов по защите информации от несанкционированного доступа. – М.: Гостехкомиссия России, 1998. – 74 с.

3. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1-3. – М.: Стандартинформ, 2009.

4. *Барабанов А.В., Марков А.С., Цирлов В.Л.* Сертификация систем обнаружения вторжений // Открытые системы. СУБД. – 2012. – № 3.

5. *Цирлов В. Л.* Основы информационной безопасности: краткий курс. – Ростов н/Д: Феникс, 2008. – 253 с.

6. *Марков А.С., Миронов С.В., Цирлов В.Л.* Выявление уязвимостей программного обеспечения в процессе сертификации // Известия Южного федерального университета. – Технические науки. – 2006. – Т. 62. – № 7. – С. 82–87.

УДК 681.3.06

Е.А. Ларионцева, Н.Н. Стельмашук
Россия, г. Москва, ЗАО «НПО «Эшелон»

РАЗРАБОТКА МЕТОДИКИ ИСПЫТАНИЙ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СООТВЕТСТВИИ С ПОЛОЖЕНИЯМИ НОВОЙ НОРМАТИВНОЙ БАЗЫ

В статье разработана методика сертификационных испытаний систем обнаружения вторжений. Разработана математическая модель оценки соответствия системы обнаружения вторжений 6-го класса уровня узла.

Сертификация; системы обнаружения вторжений; оценка соответствия; «Общие критерии».

Система обнаружения вторжений (СОВ) – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней [1,2].

Обычно выделяют следующие типы СОВ:

1) узловые– располагаются на отдельном узле и отслеживают признаки атак и других видов несанкционированных действий на него;

2) сетевые – находятся на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети.

Поэтому при проведении оценки соответствия СОВ определенному классу требований соответствующим органам, проводящим испытания, необходимо учитывать не только определенный класс защиты СОВ, но и ее тип, возможность обнаружения/предотвращения вторжений и так далее. Требования к СОВ претерпели некоторые изменения в последнее время, и целью данной работы является, во-