Формирование требований по безопасности информации к DLP-системам / А.В.Барабанов, М.И.Гришин, А.С.Марков, В.Л.Цирлов // Вопросы радиоэлектроники. 2013. №2. С. 67-76.

УДК 681.3.06

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ К DLP-СИСТЕМАМ

Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л.

Представлен подход к формированию требований и формальных методик сертификационных испытаний DLP-систем на основе стандарта ГОСТ ИСО 15408. Приведен пример требований доверия к классам защиты DLP-систем, предназначенных для защиты персональных данных.

Ключевые слова: *средства защиты информации, средства предотвращения утечек информации, ГОСТ 15408, DLP, Общие критерии, критерии оценки безопасности*

Введение

В настоящее время к современным средствам защиты информации (СЗИ) относят системы предотвращения утечки информации (data leak prevention, DLP), внедряемые с целью выявления и блокирования нелегитимной передачи информации из защищенных автоматизированных систем. К сожалению, анализ и синтез DLP-решений затруднен по причине отсутствия нормативно-методической базы, регламентирующей требования к указанным системам. Например, сегодня сертификация DLP-систем проводится на соответствие техническим условиям, в которых разработчики указывают произвольный набор неформализованных требований. В результате этого под определение сертифицированного СЗИ подпадают решения принципиально различного уровня. Перспективным направлением формирования нормативно-методической базы оценки соответствия является использование аппарата метастандарта ИСО 15408, традиционно

называемого «Общими критериями» [2]. Определение требований к DLP-системам на базе «Общих критериев» и представляет основное содержание работы.

Общие сведения о DLP-системах

DLP-система представляет собой комплекс программно-аппаратных средств, обеспечивающих защищенность информации от угроз нелегитимной передачи из защищенного сегмента автоматизированной системы путем анализа и блокирования исходящего трафика. Условно DLP-системы разделяют на три типа: системные (уровня хоста), сетевые, прикладные (как правило, уровня СУБД). Независимо от типов DLP-систем, используемые методы анализа данных разделяют на атрибутные (например, использующие свойства объектов системы) и семантические (основанные на смысловом анализе информации, как правило, путем выявления сочетаний ключевых данных). В настоящее время большинство корпоративных DLP-систем являются комплексными и включают следующие компоненты: модуль централизованного управления, агенты рабочих станций (серверов), модули анализа протоколов, модули сканирования (поиска) данных.

По аналогии с современными требованиями ФСТЭК России [4], можно предложить подход к формулировке требований к DLP-системам, исходя из типов DLP-систем и категорий защищаемой информации (государственная тайна, информация конфиденциального характера в государственных структурах и информационных системах персональных данных). Такой подход позволяет сформулировать серию *профилей защиты*, на основании которых разработчики (изготовители) СЗИ могут подготовить необходимое *задание по безопасности*. При этом задание по безопасности является основным конструкторским документом для СЗИ, на соответствие которому и проводится сертификация по ИСО 15408 [3].

Напомним, что профили защиты и задание по безопасности представляют собой структурированные формализованные документы, включающие подробное описание (в

нотациях ИСО 15408) функциональных требований к безопасности (ФТБ) и требований доверия к безопасности (ТДБ). Испытательная лаборатория, при проведении оценки соответствия (в форме сертификации), кроме задания по безопасности, использует различного рода свидетельства: конструкторскую и проектную документацию на СЗИ, руководства пользователя и администратора, стандарты предприятия, инструкции, требования к которым также могут быть сформулированы в задании по безопасности.

Метод и процедуры оценки соответствия по требованиям «Общих критериев»

Сформулируем метод, этапы, процедуры и критерии оценки соответствия СЗИ по требованиям ИСО 15408 [3].

Пусть $C = \{c_1, c_2, ..., c_n\}$ - множество компонент требований доверия к безопасности информации, предъявляемых к объекту оценки (ОО) Σ. Множество C формируется с использованием одного из предопределенных оценочных уровней доверия (ОУД) или классов защиты. Для каждой компоненты требования доверия c_i определено множество действий $E^{(i)} = \{e_1^{(i)}, e_2^{(i)}, ..., e_{n_i}^{(i)}\}$ (n_i - число действий оценщика для компоненты c_i), которое должен выполнить оценщик (испытательная лаборатория) для подтверждения соответствия ОО предъявляемой компоненте c_i.

Для каждого действия оценщика $e_j^{(i)}$ разрабатывается множество $S_j^{(i)} = \left\{ s_{j1}^{(i)}, s_{j2}^{(i)}, \dots, s_{jm_j^{(i)}}^{(i)} \right\}$ шагов оценивания - наименьшей структурной единицы работ по оцениванию ($m_j^{(i)}$ - число шагов оценивания для действия оценщика $e_j^{(i)}$). Разработка шагов оценивания выполняется экспертами испытательной лаборатории на основе «Общей методологии оценки безопасности», представленной в ИСО 18045 с учетом особенностей ОО.

Под *методом* разработки шагов оценивания будем понимать отображение $M : \Sigma \times E \to S$. Функция M на основе действия оценщика $e_j^{(i)}$ и информации о реализации

(свидетельств разработчика) ОО Σ выполняет генерацию множества шагов оценивания $S_j^{(i)}$, выполняемого для проверки удовлетворения ОО множеству C компонент требований доверия к безопасности. Как правило, функция M для данного ОО Σ является биективным отображением [1,5].

Оператором корректности выполнения действия оценщика $e_j^{(i)} \in E^{(i)}$ для ОО Σ назовем $F_S : \Sigma \times E \to \{0,1\}$:

$$F_S(\Sigma, e_j^{(i)}) = \begin{cases} 1, \textit{все шаги оценивания выполнены успешно}, \\ 0, \textit{в противном случае}. \end{cases}$$

Процедурой оценки соответствия назовем набор из четырех объектов $A = \{\Sigma, C, M, F_S\}$, где: C - множество компонент требований доверия к безопасности, предъявляемых к ОО Σ, M - метод разработки шагов оценивания, F_S - оператор корректности выполнения действия оценщика.

Процедура оценки соответствия (в форме сертификационных испытаний) предусматривает наличие трех этапов: планирование, выполнение оценки, анализ и оформление результатов оценки [5]. На стадии планирования решаются задачи получения и анализа исходных данных для проведения оценки. На основании выполненного анализа формируются множества $E^{(i)} = \left\{e_1^{(i)}, e_2^{(i)}, ..., e_{n_i}^{(i)}\right\}$ действий оценщика и соответствующих им шагов оценивания.

Выполнение оценки СЗИ осуществляется с использованием сформированного набора шагов оценивания. Анализ и оформление результатов оценки предполагает выполнение сравнения фактических и эталонных результатов. В результате анализа получаем множество упорядоченных пар вида $(e_j^{(i)}, F_S(\Sigma, e_j^{(i)}))$. Для ОО Σ декларируется соответствие компоненте требования доверия c_i, если в ходе выполнения множества действий оценщика $E^{(i)} = \left\{e_1^{(i)}, e_2^{(i)}, ..., e_{n_i}^{(i)}\right\}$ для каждого получены положительные результаты:

$$\sum_{j=1}^{n_i} F_S(\Sigma, e_j^{(i)}) = n_i .$$

По результатам проведения оценки оформляется технический отчет об оценке. Для ОО декларируется соответствие требованиям доверия к безопасности информации $C = \{c_1, c_2, ..., c_n\}$, если $\forall i \in [1, n] \sum_{j=1}^{n_i} F_S(\Sigma, e_j^{(i)}) = n_i$.

Формирование функциональных требований и требований доверия к DLP-системам

Согласно модели «Общих критериев», объект оценки (в данном случае, DLP-система) рассматривается не сам по себе, а в контексте окружающей среды. При подготовке к оценке соответствия предполагается, что должны быть формализованы следующие так называемые *аспекты среды ОО*:

- *предположения безопасности*, содержащие аспекты безопасности среды, в которой будет использоваться ОО или предполагается к использованию;

- *угрозы безопасности*, включающие все те угрозы активам, против которых требуется защита средствами ОО или его среды;

- *политики безопасности*, идентифицирующие и, при необходимости, объясняющие все положения политики безопасности организации или правила, которым должен подчиняться ОО.

На основании угроз и политик, при учете сформулированных предположений безопасности, формулируются *цели безопасности* для ОО и среды, направленные на обеспечение противостояния угрозам и выполнение положений политики безопасности.

Для достижения поставленных целей к ОО предъявляются *требования безопасности*.

В ИСО 15408 (в части 2 и 3) фактически представлены каталоги требований безопасности следующих типов:

- функциональные требования безопасности, предъявляемые к функциям безопасности ОО;

- требования доверия к безопасности, которые предъявляются к технологии и процессу разработки, эксплуатации и оценки ОО и призваны гарантировать адекватность реализации механизмов безопасности.

Результаты анализа существующих DLP-систем позволили сформулировать основные угрозы безопасности (префикс «*T*»), которым данные DLP-системы должны противостоять, положения политики безопасности (префикс «*P*») и предположения безопасности (префикс «*A*») (табл.1).

Таблица 1.

Описание аспектов среды безопасности DLP-систем

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-системы выполняется уполномоченным администратором
A.LOCATE	DLP-средство находится в пределах контролируемой зоны
A.SECCOM	Среда DLP-средств обеспечивает безопасное удаленное взаимодействие распределенных частей DLP-системы между собой и с администратором.

Анализ идентифицированных аспектов среды безопасности позволил сформулировать ФТБ в нотациях ИСО 15408-2 (табл. 2).

Таблица 2.

Функциональные требования безопасности, предъявляемые к DLP-системам

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 указать, что помимо стандартных ФТБ (указанных в ИСО 15408-2), можно предложить ряд дополнительных ФТБ (отмеченных с постфиксом «*EXT*»). Так, 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 носителе 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.

Ориентируясь на подход ФСТЭК России относительно систем обнаружения вторжений [4], можно предположить, что DLP-системы, используемые для защиты информации конфиденциального характера, будут соответствовать ОУД1-ОУД3. При этом для защиты информации в государственных структурах и информационных системах персональных данных (ИСПДн) 1-го уровня защищенности DLP-системы должны пройти контроль на отсутствие недекларированных возможностей.

Пример предлагаемых требований доверия к классам защиты DLP-систем, предназначенных для защиты персональных данных, представлен в табл.3.

Таблица 3

Пример требований доверия к классам защиты DLP-систем

Класс ИСПДн	Требования доверия безопасности DLP-систем		Уровень контроля отсутствия недекларированных возможностей
	ОУД	Дополнительные компоненты доверия к безопасности	
ИСПДн 1 уровня защищённости	3	ALC_FLR.1 «Базовое устранение недостатков» AVA_VLA.3 «Умеренно стойкий»	4
ИСПДн 2 уровня защищённости	2	ALC_FLR.1 «Базовое устранение недостатков»	-
ИСПДн 3 и 4 уровня защищённости	1	AVA_SOF.1 «Оценка стойкости функции безопасности ОО»	-

Выводы

В работе представлен подход к формированию требований к DLP-системам, позволяющий детерминировать процесс оценки соответствия, а также анализа и синтеза указанных систем для применения в защищенных автоматизированных системах. Данный подход гармонизирован с международной нормативной базой и новейшими

нормативными и методическими документами ФСТЭК России по системам обнаружения вторжений и средств антивирусной защиты.

Предложенный способ формирования процедур и критериев проведения сертификационных испытаний СЗИ по линии «Общих критериев» может быть полезен при разработке частных методик проверки механизмов и подсистем безопасности информации.

Литература

1. Барабанов А.В., Гришин М.И., Марков А.С. Формальный базис и метабазис оценки соответствия средств защиты информации объектов информатизации. // Известия института инженерной физики. 2011. № 3. С. 82-88.
2. Бородакий Ю.В., Добродеев А.Ю. Информационное общество и фундаментальные научные проблемы безопасности в компьютерной инфосфере // Информатизация и связь. 2010. № 1. С. 15-19.
3. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1-3. М.: Стандартинформ, 2009. 40, 174, 118 с.
4. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Специальные нормативные документы: официальный сайт ФСТЭК России. URL: http://www.fstec.ru/index.php/ru/dokumenty-po-sertifikatsii-tzi. Дата обращения: 01.04.2013.
5. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под.ред. А.С.Маркова. М.: Радио и связь, 2012. 192 с.