Способы испытания средств защиты информации

Ляпустин Антон Евгеньевич, Ляпустин Максим Евгеньевич

Раздел 1 Обзор значения средств защиты информации

В современных условиях активного развития информационных технологий сложно представить хотя бы один документ, не имеющий электронного оригинала или копии. С другой стороны, увеличение пропускной способности и доступности глобальной сети Интернет создаёт значительные возможности для злоумышленников. К рискам, которым подвергается информация в электронном виде, как правило, относят [1, 2]:

копирование (хищение) информации;
модификация (искажение) информации;
блокирование информации;
уничтожение информации;
отрицание подлинности информации;
навязывание ложной информации.

С целью защиты информации разрабатываются и применяются средства защиты информации (СЗИ). По способу защиты информации, СЗИ можно классифицировать следующим образом [3]: средства защиты от несанкционированного доступа (НСД):

- авторизация;
- избирательное управление доступом;
- управление доступом на основе ролей;
- мандатное управление доступом;
- журналирование (аудит);
- системы анализа и моделирования информационных потоков (CASE-системы);
- системы мониторинга сетей:
- системы обнаружения и предотвращения вторжений (IDS/IPS);
- системы предотвращения утечек конфиденциальной информации (DLP-системы);
- анализаторы протоколов;
- антивирусные средства;
- межсетевые экраны;
- криптографические средства:
- средства шифрования;
- средства цифровой подписи;
- системы резервного копирования;
- системы бесперебойного питания;
- системы аутентификации (на основе паролей, ключей доступа, сертификатов или биометрических данных);
- инструментальные средства анализа систем защиты.

Поскольку по способу реализации СЗИ можно разделить на программные, аппаратные и программно-аппаратные, при разработке СЗИ можно опираться на ГОСТ 34 серии. В этом случае этапы разработки СЗИ будут следующими [4]:

1. формирование требований к СЗИ;

2. разработка концепции СЗИ;
3. техническое задание;
4. эскизный проект;
5. технический проект;
6. рабочая документация;
7. ввод в действие.

При этом в рамках этапа ввода в действие, должны проводиться испытания средств защиты информации: предварительные испытания, опытная эксплуатация и приемочные испытания. Испытания, как правило, предполагают проверку способности СЗИ выполнять задачи защиты информации в соответствии с техническим заданием. В свою очередь, техническое задание описывает требования к разрабатываемым СЗИ. Отличительной особенностью разработки СЗИ от разработки других автоматизированных систем является их нацеленность на устранение или снижение рисков, связанных с информационной безопасностью, в то время как другие типы автоматизированных систем, как правило, имеют целью эффективное выполнение бизнес-процессов. В соответствии с этим утверждением, особого подхода требует этап испытания СЗИ. Способность СЗИ выполнять поставленные перед ней задачи называется качеством СЗИ.

Выделяют следующие основные принципы информационной безопасности [5]:

1. конфиденциальность;
2. целостность;
3. доступность.

Раздел 2 Обзор основных способов испытания средств защиты информации

Специализированные виды испытаний СЗИ, как правило, направлены на установление факта выполнения испытываемыми СЗИ указанных принципов. Как правило, такие испытания проводятся путем моделирования для СЗИ наиболее распространенных атак. К таким атакам, например, относятся:

- DDOS – вид атаки, нацеленной на перегруз системы путем отправки на её вход значительного количества запросов. Этот вид атаки приводит к временному выходу из строя системы или к значительным задержкам в выполнении ею функций.
- Инъекции кода – вид атаки, заключающейся в исполнении некоего кода, который обеспечивает доступ к системной информации или другой информации клиента.
- Server-Side Includes (SSI) Injection – вид атаки, построенной на вставке серверных команд в код HTML, или запуске их напрямую на стороне сервера.
- XSS (Cross-Site Scripting) – атака заключается в генерации на сформированной сервером странице вредоносного приложения с целью выполнения его на стороне клиента.
- XSRF / CSRF (Cross Site Request Forgery) – атака, строящаяся на недостатках HTTP протокола, позволяющих перенаправлять потенциальную жертву на выбранный злоумышленниками сайт.
- Authorization Bypass – вид атаки, позволяющий несанкционированно получить доступ к сведениям других пользователей, как правило, путем подстановки в URL подложных сведений (например, идентификатора).

Кроме того, можно выделить несколько способов испытания СЗИ, носящих общесистемный характер:

1. нагрузочное тестирование;

2. регрессионное тестирование;
3. системное тестирование.

Нагрузочное тестирование – определение показателей производительности системы или устройства, основанное на сборе времени отклика (выполнения операции) тестируемой системой. Способ нагрузочного тестирования применим к СЗИ с целью определения эффективности защиты от DDOS атак.

Регрессионное тестирование – проверка неизменности поведения тестируемой системы. Этот вид тестирования применяется для контроля за новыми версиями СЗИ. Он обеспечивает неизменность желаемого поведения СЗИ путем защиты от несанкционированных изменений [6].

Системное тестирование – оценка выполнения требований (функциональных и не функциональных) системой в целом. Проводится проверка программной части СЗИ, аппаратной части СЗИ (при наличии), их взаимодействия между собой в рамках СЗИ, а также взаимодействие СЗИ с остальной частью системы.

Проведение испытаний СЗИ затруднено, поскольку отсутствуют четкие критерии по защите информации от перспективных видов атак. В связи с этим, к проведению испытаний рекомендуется привлекать экспертное сообщество в задачи которого должны входить поиск новых видов атак на СЗИ и выявление уязвимостей СЗИ.

Непосредственно проведение испытаний может осуществляться экспертами или автоматически с применением средств автоматизированного тестирования. При проведении испытаний экспертами, выводы по итогам испытаний делаются на основании методов экспертных оценок.

Экспертный метод – это метод решения задач, основанный на использовании обобщенного опыта и интуиции специалистов-экспертов [7]. Экспертный метод оценки качества СЗИ используется в тех случаях, когда невозможно или значительно осложнено применение методов объективного определения качества СЗИ. Результат экспертизы может заключаться в ранжировании версии СЗИ по качеству или в измерении по шкале порядка. Процедура ранжирования является наиболее простой при оценке качества СЗИ, но и наименее точной, поскольку разница по качеству между присвоенными рангами R-1, R, R+1 может значительно различаться. Для количественного сравнения качества СЗИ могут обращаться к алгоритмам экспертного ранжирования, которые предполагают наличие следующих этапов:

1. выбор наиболее важных показателей качества, число которых не превосходит 7-10 (большее число показателей приводит к затруднению выставления экспертом оценок);
2. индивидуальное, а затем и групповое ранжирование показателей качества по их важности;
3. оценка СЗИ.

На каждом из указанных этапов проводится оценка согласованности мнений экспертов и отбрасывание, при необходимости, грубых ошибок. Таким образом, с привлечением экспертов могут быть проведены неформализуемые испытания СЗИ, а по результатам таких испытаний получена итоговая согласованная оценка качества СЗИ.

Среди средств автоматизированного тестирования можно выделить следующие наиболее распространенные: QACenter, Mercury, TestComplete и др. Большинство средств автоматизированного тестирования представляют собой некоторую среду разработчика [8], которая обеспечивает написание и исполнение скриптов тестирования. Такие скрипты могут относиться к регрессионному, модульному, системному или другим способам тестирования. Результаты выполнения скриптов (в виде реакции тестируемой программы) могут фиксироваться

средством автоматизированного тестирования для их дальнейшего анализа. Широко распространено применение средств автоматизированного тестирования для нагрузочного тестирования. В этом случае, средство фиксирует параметры производительности тестируемой системы.

Кроме того следует отметить, что особенным испытаниям в соответствии с Постановлением Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» подвергаются средства защиты информации в рамках программных, программно-аппаратных и аппаратных средств предназначенных для обработки данных, отнесённых к государственной тайне, либо отнесённых к служебной тайне, включая персональные данные с классом защищённости К1. Как правило, такие испытания носят комплексный характер. В рамках испытаний оценивается не только средства защиты информации, но и физический защищаемый объект (помещение), аппаратная и программная составляющие системы, а также организационная составляющая (в виде регламентов). В этом случае испытания проводятся с применением специальных средств и техники и заключаются в проверке соответствия показателей защиты информации заданным нормативам. В ряде случаев, оценка может носить экспертный характер (в этом случае оценка получается с применением методов экспертных опросов).

Заключение

Таким образом, можно сделать вывод, что выбор способов испытания СЗИ в значительной степени определяется видом СЗИ, а также способом применения СЗИ, и, как следствие, перечнем угроз или атак, которым подвержен данный тип СЗИ.

Частично испытания могут быть проведены с применением средств автоматизации тестирования, а частично – с привлечением экспертов. В последнем случае результаты испытаний определяются с применением методов экспертных опросов. При разработке СЗИ, предназначенных для защиты информации, отнесенной к государственной тайне, служебной тайне или к персональным данным с классом защищенности К1, испытания должны проводиться, также и по определенным законодательствам регламентам.

Список литературы

1. ГОСТ Р 50922-96 Защита информации. Основные термины и определения
2. Информационные технологии: учебн. пособие / Г.Н. Исаев. – М.: Издательство «Омега-Л», 2012
3. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004.
4. ГОСТ 34.601-90 Автоматизированные системы. Стадии создания.
5. Умников, А. А. Информационная безопасность: учеб.-метод. комплекс / А. А. Умников. – Новосибирск: НГПУ, 2008. – 188 с.
6. Лайза Криспин, Джанет Грегори Гибкое тестирование: практическое руководство для тестировщиков ПО и гибких команд = Agile Testing: A Practical Guide for Testers and Agile Teams. — М.: «Вильямс», 2010.
7. Кириллов В.И. Квалиметрия и системный анализ. Учебное пособие. — Минск : Новое знание ; М. : ИНФРА-М, 2011.
8. Винниченко И.В. Автоматизация процессов тестирования.–СПб.: Питер, 2005