УДК 004.056.52
DOI 10.21685/2587-7704-2018-3-2-6

Open Access RESEARCH ARTICLE

Средства анализа защищенности, применяемые для оценки эффективности функционирования средств защиты информации

В. А. Алькаев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. Г.Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Проведен обзор средств анализа защищенности, применяемых для оценки эффективности функционирования средств защиты информации. Сделан анализ возможности применения средств анализа защищенности, имеющих соответствующие сертификаты ФСТЭК России. Проведенный анализ показал, что существующие средства анализа защищенности позволяют осуществлять оценку эффективности большинства подсистем средств защиты информации, а также реализовывать меры защиты информации, касающиеся анализа защищенности, установленные нормативными и методическими документами ФСТЭК России.

Ключевые слова: информационная безопасность, анализ защищенности, средства защиты информации, средство анализа защищенности, уязвимость.

Security analysis tools for evaluation of performance efficiency of information protection means

V. A. Al'kaev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. A review of security analysis tools used to evaluate the performance efficiency of information protection means was conducted. An analysis of feasibility to use the security analysis tools that have relevant certificates of Federal Service for Technical and Export Control (FSTEC) of Russia has been made. The analysis showed that the existing security analysis tools allow evaluating the effectiveness of most subsystems of information protection means, as well as implementing information protection measures related to security analysis established by regulatory and methodical documents of FSTEC of Russia.

Keywords: information security, security analysis, information protection means, security analysis tools, vulnerability.

Широкое практическое использование электронно-вычислительных машин (ЭВМ), начавшееся в 50-х гг. XX в., потребовало с течением времени применения методов и средств обеспечения информационной безопасности (ИБ). Она достигалась в основном с помощью ограничения физического доступа пользователя к оборудованию, которое содержало или обрабатывало защищаемую информа-

цию. Чуть позже свое развитие получили локальные сети, информационная безопасность которых в основном достигалась путем администрирования и управления доступом к сетевым ресурсам. А с началом использования мобильных коммуникационных устройств угрозы ИБ стали гораздо серьезнее и сложнее. Появились хакеры, целью которых было нанесение ущерба ИБ. Потребовалась разработка новых методов и средств обеспечения ИБ. С тех пор обеспечение ИБ становится важнейшей и обязательной составляющей безопасности вычислительных сетей и систем.

С развитием информационно-коммуникационных технологий, с процессом информатизации общества значительно возросло количество атак на системы и сети. Однако больший интерес для обеспечения ИБ представлял факт постоянного обнаружения новых уязвимостей в программном обеспечении и, как следствие, появление новых видов атак. Для подавления атак и обеспечения ИБ сетей и систем создаются и постоянно совершенствуются программные и программно-аппаратные средства защиты информации (СЗИ) [1].

Существующие в информационной системе уязвимости могут быть использованы при реализации угроз. Средства анализа защищенности используются для поиска уязвимостей в штатном программном обеспечении, которые могли возникать при его разработке и эксплуатации. Сканеры безопасности формируют отчет, в котором предоставляют администратору безопасности сведения о выявленных уязвимостях, их описание, степень опасности и способ устранения.

Средства анализа защищенности являются необходимыми для администраторов безопасности, а также для лиц, занимающихся обеспечением безопасности информационных систем и локальных сетей.

При проведении анализа защищенности реализуются две стратегии. Первая – пассивная, реализуемая на уровне операционной системы, системы управления базой данных (СУБД) и приложений, при которой осуществляется анализ конфигурационных файлов и системного реестра на наличие неправильных параметров; файлов паролей на наличие легко угадываемых паролей, а также других системных объектов на нарушения политики безопасности. Вторая стратегия – активная, осуществляемая в большинстве случаев на сетевом уровне, позволяющая воспроизводить наиболее распространенные сценарии атак и анализировать реакции системы на эти сценарии.

Первоначально сканеры безопасности использовались с целью выявления уязвимостей в локальных сетях. Они были простейшими, имели минимально необходимый набор функций. Например, могли осуществлять сканирование портов для определения номеров открытых портов. В дальнейшем по мере развития и увеличения функциональных возможностей сканеры начали использоваться и нарушителями. На данный момент сканеры безопасности могут представлять собой распределенные программные комплексы, используемые в больших сетях для проверки клиентских компьютеров и серверов, находящихся на больших расстояниях.

Для проведения специальных видов испытаний средств защиты информации, например сертификационных, инспекционных и др., в Российской Федерации разработаны средства анализа защищенности, применение и набор функций которых отличается от распространенных сетевых сканеров уязвимостей. Такие средства анализа защищенности, как СЗИ от НСД, должны проходить обязательную процедуру оценки соответствия требованиям по безопасности информации и получения сертификата государственной системы сертификации средств защиты информации, регулируемой ФСТЭК России [2–4]. Сертифицированные сканеры безопасности могут применяться администраторами безопасности для оценки эффективности установленных и используемых в информационных системах средств защиты информации.

Средства анализа защищенности классифицируются с учетом того, какие подсистемы СЗИ являются объектом исследования, а именно:

– средства проверки подсистемы идентификации и аутентификации;
– средства проверки подсистемы обеспечения целостности;
– средства проверки подсистемы гарантированного удаления информации;
– средства проверки подсистемы регистрации событий.

Был рассмотрен Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 [5]. Проведен анализ возможности реализации проверки подсистем средствами анализа защищенности, имеющими сертификаты соответствия требованиям обеспечения безопасности информации, регулируемым ФСТЭК России.

Анализ показал, что для проверки подсистемы идентификации и аутентификации возможно использование такого средства анализа защищенности, как «Сканер-ВС». Осуществить проверку подсистемы обеспечения целостности могут такие средства, как «ФИКС», «Трафарет 2.0» и «Сканер-ВС». Проверка подсистемы гарантированного удаления информации возможна средствами анализа

защищенности «TERRIER 3.0», «Ревизор Сети 3.0» и «Сканер-ВС». А подсистему регистрации событий возможно проверить средствами «Трафарет 2.0», «ФИКС», «TERRIER 3.0», «Ревизор Сети 3.0» и «Сканер-ВС».

Таким образом, существующие сертифицированные средства анализа защищенности позволяют реализовать проверку защищенности всех информационных подсистем.

В связи с широким применением средств анализа защищенности стали разрабатываться нормативные документы, устанавливающие требования к обеспечению ИБ. Так, ФСТЭК России разработала несколько положений, устанавливающих требования по обеспечению ИБ информационных и автоматизированных систем, в составе которых могут использоваться средства анализа защищенности [2–4]. В этих положениях определен перечень мер защиты, которые должны применяться для контроля (анализа) защищенности информации. Далее рассмотрен обобщенный перечень мер контроля защищенности информации.

Нормативными документами ФСТЭК России установлен следующий перечень мер контроля защищенности информации:

– АНЗ.0 Разработка правил и процедур (политик) контроля (анализа) защищенности;

– АНЗ.1 Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей;

– АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

– АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

– АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации;

– АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей.

Проведен анализ возможности реализации мер контроля защищенности информации при использовании средств анализа защищенности. Рассмотрению подлежали только те программные средства, которые имеют действующий сертификат соответствия требованиям по безопасности информации.

Анализ показал, что для реализации меры контроля защищенности АНЗ.0 можно использовать средства анализа защищенности «Трафарет 2.0», «ФИКС», «TERRIER 3.0», «Ревизор Сети 3.0» и «Сканер-ВС». Для меры контроля защищенности АНЗ.1 – «Сканер-ВС», для АНЗ.2 – «Ревизор Сети 3.0» и «Сканер-ВС», для АНЗ.3 и АНЗ.4 – «Трафарет 2.0», «ФИКС» и «Сканер-ВС», для АНЗ.5 – «Сканер-ВС».

В результате проведенного анализа возможности реализации мер контроля защищенности информации можно сделать вывод о том, что существующие средства анализа защищенности позволяют реализовать все меры защиты, установленные нормативными документами ФСТЭК России [2–4]. Количество таких программных средств, прошедших оценку соответствия требования по безопасности информации и имеющих сертификат ФСТЭК России, небольшое. Однако использование таких средств является необходимым.

Библиографический список

1. Справочник24. Информационная безопасность. Основы и методы защиты информации. – URL: https://spravochnick.ru/informacionnaya_bezopasnost/informacionnaya_bezopasnost_osnovy_i_metody_zaschity_informacii/#istoriya-vozniknoveniya-i-razvitiya-informacionnoy-bezopasnosti (дата обращения: 28.10.2018).
2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608).
3. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (Зарегистрировано в Минюсте России 14.05.2013 № 28375).
4. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : Приказ ФСТЭК России от 14 февраля 2014 г. № 31 (Зарегистрировано в Минюсте России 30.06.2014 № 32919).
5. Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-

gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения: 21.09.2018).

Алькаев, В. А.
Средства анализа защищенности, применяемые для оценки эффективности функционирования средств защиты информации/ В. А. Алькаев, А. Г. Фатеев// Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-6.