Бобрышева Г.В., Звозникова А.О. Методы оценки информационной безопасности. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 123-127.

УДК 004.056.53

МЕТОДЫ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г.В. Бобрышева, А.О. Звозникова

EVALUATION METHODS OF INFORMATION SECURITY

G.V. Bobrysheva, A.O. Zvoznikova

Аннотация. Рассматривается обеспечение информационной безопасности компьютерных сетей на основе использования эффективных методов и средств защиты информации, для оценки эффективности которых применяются качественные и количественные показатели.

Ключевые слова: информационная безопасность, защита информации, компьютерная сеть.

Abstract. The article deals with the information security of computer networks through the use of effective methods and means of information security, to assess the effectiveness of which are used qualitative and quantitative indicators.

Keywords: information security, information protection, computer network.

В настоящее время существует острая потребность в защите информации и, в частности, информации, передаваемой в компьютерных сетях. Необходимость защиты информации подтверждается Федеральным законом «Об информации, информационных технологиях и защите информации» и другими нормативно-правовыми документами Российской Федерации [1].

Поэтому одним из основных требований при построении компьютерных сетей является обеспечение ее информационной безопасности.

Под информационной безопасностью понимают состояние защищенности информации от несанкционированного использования и модификации. При этом информационная безопасность компьютерной сети во многом определяется уязвимостью хранимой, обрабатываемой и передаваемой в ней информации.

Уязвимость информации возможна при возникновении таких состояний компьютерной сети, при которых создаются условия для реализации угроз безопасности информации, наиболее опасными среди которых являются преднамеренные угрозы, которые могут быть реализованы аппаратными, программными и аппаратно-программными средствами.

Решение вопросов и эффективность обеспечения информационной безопасности компьютерной сети достигается за счет использования методов и средств защиты информации и, в частности, криптографических методов.

Для оценки эффективности методов и средств защиты информации применяют качественные и количественные методы оценки информационной безопасности.

Качественные методы оценки информационной безопасности предполагают:

- оценку уровня информационной безопасности;
- анализ рисков;

тестирование методов и средств защиты информации.

К количественным методам относятся:

- метод экспертных оценок;
- метод информационных потоков;
- графовый метод;
- метод весовых коэффициентов.

Наиболее эффективным методом оценки информационной безопасности компьютерной сети является тестирование предполагаемых для использования или используемых методов и средств защиты информации. Тестирование позволяет оценить эффективность методов и средств защиты информации и их устойчивость к атакам, выявить недостатки в организации защиты информации (системы защиты) компьютерной сети с точки зрения третьего лица (взломщика) и ее уязвимые места путем имитации различных атак.

Для оценки методов и средств защиты информации чаще всего используют три метода тестирования: по методу "черного ящика", по методу "белого ящика", тестирование на проникновение [2].

Использование метода "черного ящика" предполагает, что команда тестирования не знает конфигурацию и внутреннюю структуру системы защиты компьютерной сети. В процессе тестирования происходит эмуляция действий потенциальных злоумышленников, пытающихся взломать систему защиты. Тестирование заключается в наблюдении за реакциями механизмов защиты на различного рода атаки злоумышленника.

Использование метода "белого ящика" предполагает, что команда тестирования знает конфигурацию и внутреннюю структуру системы защиты в компьютерной сети. В процессе тестирования происходит проверка наличия и работоспособности механизмов безопасности системы защиты, соответствия состава и конфигурации системы защиты требованиям безопасности и существующим рискам. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного программного обеспечения, а затем проверяются на практике. В данном случае основным инструментом анализа являются программные средства анализа защищенности системного уровня.

Тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) заключается в санкционированной попытке обойти предполагаемый для использования комплекс средств защи-

ты компьютерной сети. В ходе тестирования команда выполняет роль злоумышленника, мотивированного на нарушение информационной безопасности компьютерной сети [3-6].

Тестирование на проникновение осуществляется в соответствии со стандартами и руководствами по обеспечению информационной безопасности и может быть проведено с использованием следующих подходов:

ручное тестирование;

автоматическое тестирование, наиболее популярными инструментами для которого являются: Nmap, Nessus, Metasploit, Wireshark, OpenSSL, Cain & Abel, THC Hydra, w3af;

сочетание ручного и автоматического тестирования, являющееся наиболее оптимальным подходом.

В процессе аналитического анализа подходов тестирования на проникновение выделены их сильные и слабые стороны (см. таблицу).

Методы тестирования на проникновение

Метод тестирования	Сильные стороны	Слабые стороны
1	2	3
Метод "черного ящика"	– возможность выявления дефектов, которые невозможно найти методом «белого ящика», например, отсутствие некоторой функциональности СИБ; – возможность подготовки тестовых данных и составления тест-кейсов сразу после подготовки документации на СИБ; – тестирование проходит «с позиции пользователя»	– необходимость большого количества тестов из-за множества тестовых данных, вследствие чего часто тесты могут быть избыточными, так как неизвестна конфигурация и структура СИБ; – сложность составления тестов при отсутствии полной документации на СИБ; – возможность пропустить граничные значения при составлении тестовых данных из-за неочевидной документации
Метод «белого ящика»	– знание внутренней логики и структуры кода помогает подготовить тестовые данные, которые позволяют эффек-тивное тестирование СИБ; – позволяет оптимизировать код путем удаления дополнительных строк кода, которые могут привести к дефектам в коде	– требуются квалифицированные и опытные специалисты, так как знание кода и внутренней структуры являются необходимыми условиями для данного вида тестирования; – почти невозможно проверить каждый кусок кода, чтобы выяснить скрытые ошибки

Продолжение таблицы.

1	2	3
Тестирование на проникновение	– позволяет обнаружить недостатки защиты, которые не были учтены при выборе политики безопасности – имеется возможность имитации реализации различных угроз – имеется возможность рассмотреть действия нарушителя – имеется возможность использования для тестирования инструментария	– не позволяет проверить код; – требует большого количества тестовых данных

Результаты аналитического анализа рекомендуется учитывать при выборе метода и подхода тестирования системы защиты компьютерной сети.

Библиографический список

1. Информационно-правовое обеспечение «ГАРАНТ». Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации» [Электронный ресурс]. URL: http://base.garant.ru/12148555/ (дата обращения: 21.09.2018)

2. Полянский Д.А. Оценка защищенности: учеб. пособие. Владимир: Изд-во Владим. гос. ун-та, 2005. 80 с.

3. OWASP Testing Project. [Электронный ресурс]. URL: https://www.owasp.org/index.php/OWASP_Testing_Project (дата обращения: 16.09.2018)

4. OWASP Top Ten Project. [Электронный ресурс]. URL: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (дата обращения: 16.09.2018)

5. The Web Application Security Consortium / Threat Classification. [Электронный ресурс]. URL: https://www.owasp.org/index.php/OWASP_Testing_Project (дата обращения: 17.09.2018)

6. Стандарты. ISO 27000. Международные стандарты управления информационной безопасностью. Общие сведения о стандартах серии ISO 27000. [Электронный ресурс]. URL: http://iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu/ (дата обращения: 18.09.2018)

Бобрышева Галина Владимировна
Пензенский государственный университет,
г. Пенза, Россия
E-mail: g_bobr@mail.ru

Bobrysheva G.V.
Penza State University,
Penza, Russia

Звозникова Анна Олеговна
Пензенский государственный университет,
г. Пенза, Россия

Zvoznikova A.O.
Penza State University,
Penza, Russia