Шаханова М. В., Кий Ю. А., Шаханова Э. С. Методы анализа защищённости компьютерных сетей // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 22–27

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.7

МЕТОДЫ АНАЛИЗА ЗАЩИЩЁННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Шаханова М. В., Кий Ю. А., Шаханова Э. С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, д.50а), e-mail: marinavl2007@yandex.ru

Повсеместное развитие и интеграция информационных технологий приводит к глобальным трендам цифровой трансформации всех профессиональных областей жизнедеятельности человека. Одним из актуальных вопросов в современных реалиях является обеспечение информационной безопасности используемых на предприятиях компьютерных сетей. Основной целью текущей статьи является исследование методов анализа защищенности компьютерных сетей. Автором предпринимается попытка систематизации знаний, касающихся основных аспектов использования методов анализа защищенности компьютерных сетей. Научная ценность работы заключается в возможности использования полученных материалов в качестве теоретической базы для дальнейших исследований из области разработки методов защиты. В работе применяются теоретические методы исследования, а также используются зарубежные и отечественные научные материалы.

Ключевые слова. Информационные технологии, информационная безопасность, компьютерная сеть, информация, защищенность.

METHODS FOR ANALYZING THE SECURITY OF COMPUTER NETWORKS

Shakhanova M. V., Kiy Yu. A., Shakhanova E.S.

G.I. Nevelsky Maritime State University, Vladivostok, Russia (690003, Vladivostok, st. Verkhneportovaya, 50a), e-mail: marinavl2007@yandex.ru

The widespread development and integration of information technologies leads to global trends in the digital transformation of all professional areas of human activity. One of the urgent issues in modern realities is ensuring information security of computer networks used at enterprises. The main purpose of the current article is to study methods for analyzing the security of computer networks. The author attempts to systematize knowledge concerning the main aspects of using methods of analyzing the security of computer networks. The scientific value of the work lies in the possibility of using the obtained materials as a theoretical basis for further research in the field of developing protection methods. Theoretical research methods are used in the work, as well as foreign and domestic scientific materials are used.

Keywords: Information technology, information security, computer network, information, security.

С помощью информации, непрерывно обрабатываемой и передающейся в различных инфокоммуникационных системах и сетях, происходит обмен конфиденциальными данными, производятся транзакции на различных предприятиях, а также выполняется работа с засекреченной информацией и данными ограниченного доступа. Данный список можно перечислять без конца так как в современном мире все процессы, происходящие в бытовой и

профессиональной сфере жизнедеятельности человека, основываются на использовании информационных технологиях [1].

Ввиду этого, формируется и актуализируется проблема, связанная с обеспечением безопасности работы с информационными ресурсами. Таким образом, вопрос информационной безопасности – это одно из ключевых и приоритетных направлений становления современного технологического прогресса. В современном мире существует большое количество способов и средств защиты информации в различных инфокоммуникационных системах и сетях. Именно способы защиты информации формируют кластер развития средств защиты информации, используемых в современных инфокоммуникационных системах [2].

Исходя из высокой степени необходимости использования компьютерных сетей на современных предприятиях, все большее внимание уделяется в сторону вопросу поддержания их должного уровня информационной безопасности. Непрерывное развитие и повсеместное использование сетей порождает рост уязвимостей программных ресурсов. В свою очередь, широкое распространения средств реализации данных угроз актуализирует применение различных систем анализа защищенности.

Данные системы представляют программно-аппаратные средства, направленные на выявление фактов несанкционированного доступа в компьютерную сеть. При этом выделяется три основных типа атаки. Первый из них является подготовительным и заключается в поиске предпосылок для выполнения той или иной атаки. На данном этапе производится поиск уязвимостей, дальнейшее использование которых и приводит к реализации атаки, что является вторым этапом. На третьем этапе происходит завершение атаки и «заметание» следов. Методы анализа защищенности компьютерных сетей направлены на обеспечение дополнительного уровня защиты компьютерных сетей и разделяются на такие классы относительно позиции в сети, как хостовые и сетевые системы обнаружения вторжений [3].

Необходимо отметить, что обнаружением вторжений занимаются системы анализа защищенности. Таковыми являются различные сканеры безопасности, а также системы поиска уязвимостей. На их основе производятся всесторонние исследования заданных систем для обнаружения уязвимостей, приводящих к нарушениям целостности и информационной безопасности. При этом наибольший уровень угрозы представляют уязвимости проектирования, обнаружение и устранение которых требует большого труда.

Защищенность представляет собой ключевой показатель эффективности функционирования компьютерных сетей, наряду с показателями надежности, отказоустойчивости, производительности и других. Под защищенностью компьютерных сетей обычно понимается степень адекватности реализованных в ней механизмов по обеспечению защиты информации, потенциально подверженной рискам, связанным с осуществлением угроз безопасности. Данные угрозы могут нарушать такие свойства информации, как ее конфиденциальность, целостность и доступность.

На сегодняшний день существует ряд основных методов анализа защищённости компьютерных сетей, предполагающих использование активных и пассивных систем тестирования. В таблице 1 представлен аналитический свод наиболее распространенных методов анализа защищенности сетей [4-5].

Таблица 1 – Методы анализа защищённости компьютерных сетей

Метод	Описание	Преимущества	Недостатки
Анализ механизмов безопасности организационного уровня	Включает в себя анализ политики безопасности организации и документации по обеспечению режима информационной безопасности. Производится оценка их соответствия существующим требованиям и адекватность к реагированию рискам.	Позволяет выявить несоответствия на начальном уровне построения компьютерной сети.	Долгая обработка данных и информации о рисках нарушения безопасности. Недостаточный уровень автоматизации процессов поиска аномалий.
Ручной анализ конфигурационных файлов	Включает в себя анализ межсетевого экрана, прокси-серверов, на основе которых производится управление межсетевыми взаимодействиями, а также иных критических элементов сетевой инфраструктуры.	Может быть полезен при анализе обеспечения информационной безопасности на объектах, где не существует возможности анализа реальных электронно-вычислительных систем.	Низкая эффективность выявления угроз относительно программных методов.
Сканирование внешних сетевых адресов ЛВС из сети Интернет	Основывается на пингах компьютерной сети с целью выявления внешних IP-адресов и отображает распределение типов ресурсов по сети для выявления аномалий.	Позволяет произвести анализ защищенности относительно внешних угроз безопасности. Высокая эффективность и скорость выявления аномалий.	Ограничен сканированием внешних ресурсов. Требует использование платного программного обеспечения.
Сканирование ресурсов ЛВС изнутри	Основывается на пингах компьютерной сети с целью выявления внутренних IP-адресов и отображает распределение типов ресурсов по сети для выявления аномалий.	Позволяет произвести наиболее эффективный анализ защищенности относительно внутренних угроз безопасности.	Ограничен сканированием внутренних ресурсов. Требует использование платного программного обеспечения.

Продолжение Таблицы 1

Метод	Описание	Преимущества	Недостатки
Анализ конфигурации серверов и рабочих станций ЛВС	Производится посредством специализированных программных агентов, выявляющих аномалии и нарушения информационной безопасности сети.	Представляет возможность быстрого и эффективного поиска угроз безопасности на основе использования программных продуктов. Представляет высокую актуальность своего использования для сканирования масштабных и территориально-распределенных компьютерных сетей.	Требует использование дорогостоящего программного обеспечения. Не является рациональным к использованию небольших компьютерных сетей.

Представленные в таблице 1 методы имеют индивидуальные особенности, использование которых в соответствии каждой из них может быть рационально в зависимости от размерности и выполняемых задач компьютерных сетей. Так, к примеру, аппаратные методы анализа защищенности (ручной анализ конфигурационных файлов, анализ механизмов безопасности организационного уровня) являются наиболее эффективным методом сканирования небольших сетей или при решении задач выявления угроз безопасности на этапе проектирования сетей [6-7].

При этом программные методы позволяют произвести более быстрый анализ защищенности масштабных и территориально-распределенных компьютерных сетей, но требуя использование платных программных продуктов. Одними из наиболее распространенных программных продуктов, использующихся при реализации программного анализа защищенности компьютерных сетей являются следующие инструменты, представленные на рисунке 1.

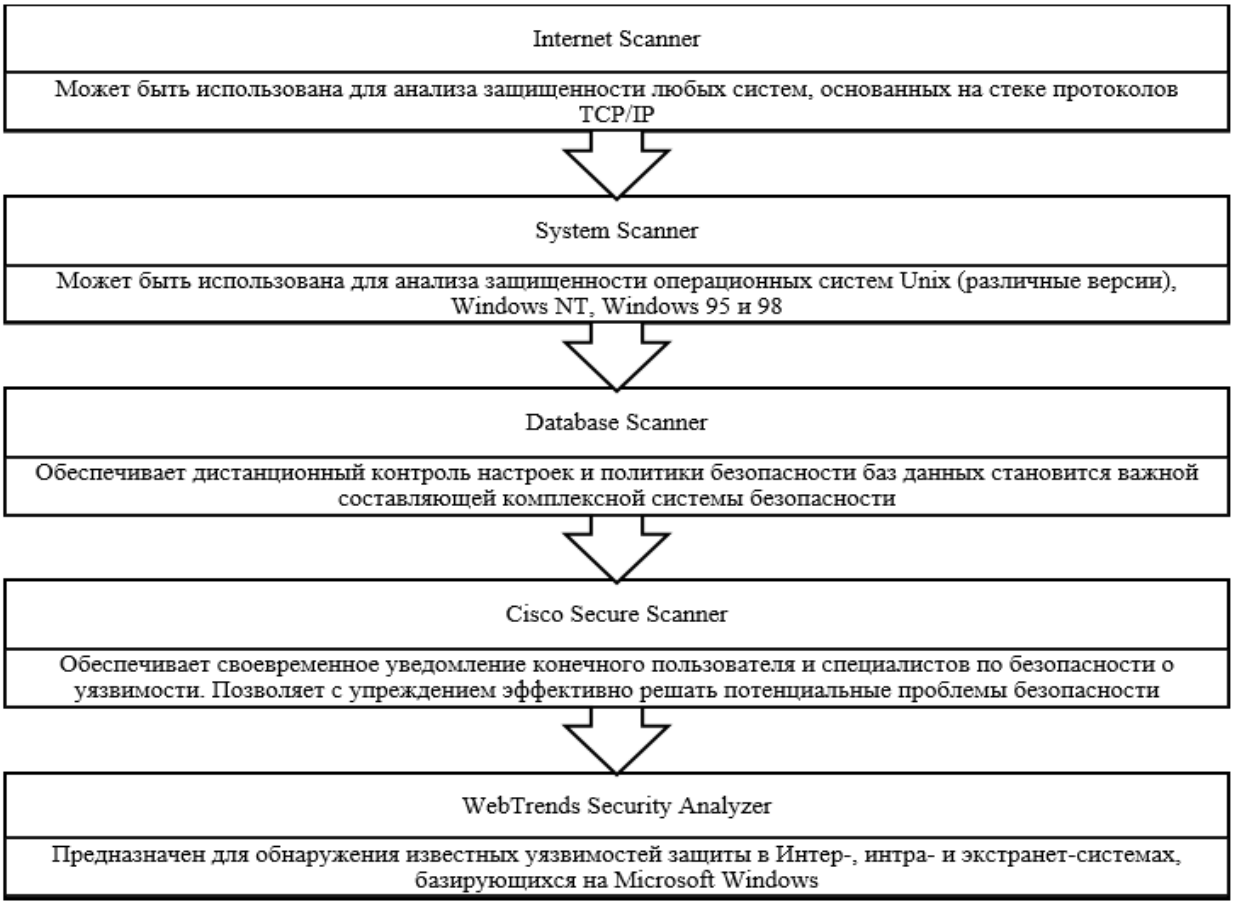

Рисунок 1 – Средства анализа защищенности компьютерных сетей

Таким образом, основной целью представленной статьи являлось исследование методов анализа защищенности компьютерных сетей. В заключение необходимо отметить, что вопрос обеспечения информационной безопасности занимает ключевое место в развитии сегмента информационных технологий. При этом ввиду непрерывного появления новых уязвимостей необходимо разрабатывать новые и повышать эффективность существующих инструментов обнаружения угроз и анализа защищенности компьютерных сетей.

Список литературы

1. Дойникова Е.В., Федорченко А.В., Котенко И.В., Новикова Е.С. Методика оценивания защищенности на основе семантической модели метрик и данных // Вопросы кибербезопасности. 2021.
2. Борзенкова С.Ю., Казарина Е.Е. Анализ методов оценки уровня защищенности информационных систем в процессе их эксплуатации // Известия ТулГУ. Технические науки. 2020.
3. Бутин А.А. Методологии анализа защищенности информации в автоматизированных системах // Достижения науки и образования. 2018.
4. Kotsynyak M.A., Spitsyn O.L., Ivanov D.A. Methodology for assessing network stability in conditions of targeted cybernetic attack // High-tech technologies in Earth space research. 2018.

5. Грушо А. А., Грушо Н. А., Забежайло М. И., Тимонина Е. Е. Методы оценки защищенности компьютерных систем информационной поддержки цифровой экономики // International Journal of Open Information Technologies. 2019.
6. Yuganson A.N., Zakoldaev D.A. An approach to assessing the security of embedded software in the conditions of fuzzy input information. Vestnik AGTU. Series: Management, Computer Engineering and Computer Science. 2020.
7. Шинкаренко А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов // Интеллектуальные технологии на транспорте. 2016.

References

1. Doynikova E.V., Fedorchenko A.V., Kotenko I.V., Novikova E.S. Methodology for evaluating security based on the semantic model of metrics and data // Issues of cybersecurity. 2021.
2. Borzenkova S.Yu., Kazarina E.E. Analysis of methods for assessing the level of security of information systems during their operation. Izvestiya TulGU. Technical science. 2020.
3. Butin A.A. Methodologies for analyzing information security in automated systems // Achievements of science and education. 2018.
4. Kotsynyak M.A., Spitsyn O.L., Ivanov D.A. Methodology for assessing network stability in conditions of targeted cybernetic attack // High-tech technologies in Earth space research. 2018.
5. Grusho A. A., Grusho N. A., Zabezhailo M. I., Timonina E. E. Methods for assessing the security of computer systems for information support of the digital economy // International Journal of Open Information Technologies. 2019.
6. Yuganson A.N., Zakoldaev D.A. An approach to assessing the security of embedded software in the conditions of fuzzy input information. Vestnik AGTU. Series: Management, Computer Engineering and Computer Science. 2020.
7. Shinkarenko A.F. Methods for assessing the security of information and telecommunication nodes // Intelligent technologies in transport. 2016.