www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2022.3.2

УДК 004.056:005.521
ББК 32.972.53

ИССЛЕДОВАНИЕ МЕТОДОВ ПРОГНОЗИРОВАНИЯ АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Наталья Алексеевна Головачева

Старший преподаватель, кафедра информационной безопасности,
Волгоградский государственный университет
golovacheva.natalya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Никита Евгеньевич Андрейченко

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBb-191_858111@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе приведена сравнительная характеристика рассмотренных взаимодействий с информационными системами. Для анализа методов прогнозирования введен ряд критериев, на основе которых происходило сравнение и оценка методов. Кроме того, была разработана математическая модель, алгоритм реализации модели для выбора наилучшего метода прогнозирования атак на информационные системы, архитектуры и интерфейса программного средства. Затем были проведены экспериментальные исследования с помощью программного средства, в рамках которых анализировались следующие методы прогнозирования атак на информационные системы. Сделан вывод о наилучшем методе прогнозирования атак на информационные системы и его преимуществе перед другими рассмотренными методами.

Ключевые слова: информационная система, уязвимость информационной системы, атака на информационную систему, угрозы безопасности информации, сетевые атаки, интервальное прогнозирование.

На современном этапе развития общества большое значение во многих направлениях деятельности компаний имеют проблемы информационной безопасности.

Одним из средств их решения является обнаружение компьютерных атак.

Сетевая атака – это злоумышленные воздействия на информационные системы, намеренные действия третьих лиц, направленные на установление контроля над локальным / удаленным компьютером или вычислительной системой [1].

Сетевые атаки по характеру воздействия на сеть можно поделить на активные и пассивные. Активные воздействуют на сеть, из-за чего может быть нарушена работоспособность сети, или же модификация ее настроек [1]. Этот тип воздействия оставляет следы в сети, из-за чего сразу расчет идет на то, что его обнаружат. Пассивная атака проводится без влияния на сеть, но ее работа нарушает сетевую безопасность. Обнаружить ее намного сложнее, чем

активную, из-за отсутствия прямого вмешательства. В основном целью атаки является несанкционированный доступ к защищаемой информации – ее искажение или перехватывание. В первом случае данные изменяются, во втором доступ производится, не вмешиваясь в структуру данных.

Есть несколько разновидностей сетевых атак:

1. DoS- и DDoS-атаки.

DoS-атака обычно производиться одним злоумышленником. Данный тип атаки используется для приостановления работы ИС на короткое время. В основном данное взаимодействие с ИС является тренировочным для хакера. Поэтому не всегда опасно для больших кампаний, из-за чего не часто используется DDoS-атака. Данный тип атаки чуть более опасен, чем предыдущий, для нее потребуется больше средств и злоумышленников, таким способом можно остановить работу большой ИС, что может привести к экстренной ситуации на предприятии. Есть много разновидностей DDoS-атак, самая популярная флуд. Одновременно посылать на ИС огромный поток запросов пустышек. Чаще всего данный вид атаки используют в целях скрыть другие вредоносные воздействия на ИС [3].

2. Компьютерный вирус – вид вредоносного программного обеспечения [1].

Может использоваться как одним злоумышленником, так и группой. Если хакер один, то он просто проверяет работу своего вируса, чтобы в последующие разы усовершенствовать его. Группа хакеров применяет вирусы для более опасных целей. Есть много разновидностей вирусов, но в основном используется «троян», для того чтобы в удобный момент перейти к следующему типу атаки.

3. Технические средства съема информации. Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т. д. [1].

В исполнении это самый сложный способ, так как нужен физический доступ к ИС и специальные знания для грамотного использования технических средств. Но за счет этого данный метод является самым эффективным из всех перечисленных.

В таблице 1 приведена сравнительная характеристика рассмотренных взаимодействий с ИС.

Для анализа методов прогнозирования необходимо ввести ряд критериев (см. табл. 2), на основе которых будет происходить сравнение и оценка методов:

Таблица 1

Сравнительная характеристики злоумышленных взаимодействий

Характеристика	DoS	Вирусы	DDoS	Техсредства съема информации
Количество злоумышленников	Один	Один или группа	Группа	Группа
Технические средства	Персональный компьютер	Персональный компьютер	Собственная ЛВС с большой вычислительной мощью	Клавиатурные жучки, мини-камеры, звукозаписывающие устройства
Для чего используются	Для тренировки	Для устранения изъянов. Для дальнейшего использования при следующей атаке	Для скрытия более опасного взаимодействия с ИС	Для изъятия информации на прямую
Влияние на ИС	Краткое приостановление	Внедрение в ИС с последующем использованием	Полное отключение	Зависит от использующихся техсредств
Получение данных	Нет	При использовании некоторых вирусов	Нет	Да
Компьютерные знания	Недостаточные	Достаточные	Достаточные	Достаточные, разработчик техсредств

Характер воздействия, оказываемого на сеть (К1). Данный вид критерия дает понять, какое воздействие происходит на информационную систему.

Цель оказываемого воздействия (К2). Критерий определяет, учитываются ли цели воздействия на информационную систему.

Наличие обратной связи с сетью (К3). Данный критерий определяет, учитывается ли отклик системы при атаке на информационную систему.

Условия наличия атаки (К4). Данный критерий отражает, определяются ли при создании формальной модели условия, при которых осуществляются переходы от одного узла информационной системы к другому.

Расположение субъекта по отношению к объекту атаки (К5). Критерий определяет, учитываются ли расположения субъектов и объектов.

Нами была разработана математической модели, алгоритма реализации модели для выбора наилучшего метода прогнозирования атак на информационные системы, архитектуры и интерфейса программного средства. Затем были проведены экспериментальные исследования с помощью программного средства, в рамках которых анализировались следующие методы прогнозирования атак на информационные системы:

1. Интервальное прогнозирование (ИП). Суть этого прогнозирования заключается в прогнозировании одного из двух заранее заданных интервалов, в котором будет находиться будущее значение показателя на основе оценок вероятностей этих событий.

2. Полигармонический полином. Эта модель рассчитывалась при помощи формулы:

$$x(t) = a_0 + \sum_{i=1}^{n} [a_i \cdot \cos(2\pi \cdot K_i \cdot t / N) + b_i \cdot \sin(2\pi \cdot K_i \cdot t / N)] + \varepsilon(t) + d_0 + d_1 \cdot t,$$

где N – число элементов исходного ряда; n – число гармоник полигармонического полинома; K_i – коэффициенты, определяющие номер гармонии; ε(t) – прогнозная оценка случайной компоненты; d_0, d_1 – коэффициенты уравнения тренда; t – порядковый номер элементов исходного ряда, $t = 1,2, ...$ [2].

3. Статистический метод основан на построении и анализе динамических рядов характеристик (параметров) объекта прогнозирования.

Основная идея метода состоит в использовании в качестве прогноза линейной комбинации прошлых и текущих наблюдений.

4. Метод экспертных оценок. Этот метод целесообразно применять в том случае, когда отсутствуют статистические данные.

Знания экспертов формируются в базу данных (см. рисунок). Она поможет в поиске аналогичных происшествий и методов их решения, а также минимизации потерь. Главным достоинством такого прогнозирования является отсутствие ложных тревог. Основным недостатком метода экспертных оценок является невозможность отражения неизвестных атак.

5. Метод индуктивного прогнозирования. Он основан на распознавании признаков атак, связанных с запретами.

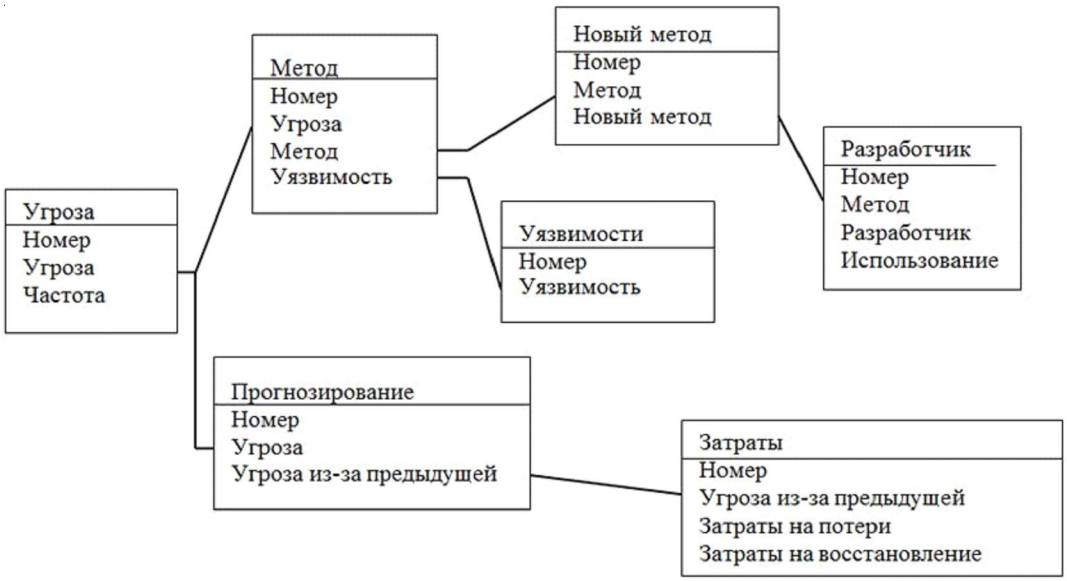
На базе проведенного анализа методов прогнозирования атак необходимо составить сводную таблицу, в которой будут отражены значения критериев для каждого метода.

Так как ни один из методов не обладает наилучшим набором значений критериев, необходимо разработать программу для автоматизации выбора наилучшего метода прогнозирования атак.

Таблица 2

Критерии оценки

Критерий	Значение		
Характер воздействия, оказываемого на сеть	низкое	среднее	высокое
Цель оказываемого воздействия	не задана	не задана в явном виде	задана
Наличие обратной связи с сетью	не задано	не задано в явном виде	задано
Условия наличия атаки	не заданы	не заданы в явном виде	заданы
Расположение субъекта по отношению к объекту атаки	не задано	не задано в явном виде	задано



База данных для прогнозирования методом экспертных оценок

Таблица 3

Значения критериев оценки

Метод	Критерий оценки				
	К1	К2	К3	К4	К5
Интервальное прогнозирование	высокий	не задан	задан	не задан	задан
Полигармонический полином	средний	не задан в явном виде	не задан	задан	не задан
Статистический метод	средний	не задан	не задан в явном виде	не задан в явном	не задан
Метод экспертных оценок	высокий	не задан в явном виде	не задан	не задан	не задан
Индуктивное прогнозирование	высокий	задан	не задан	не задан в явном виде	не задан

Было проведено 5 экспериментов, в результате которых получены следующие обобщенные оценки методов прогнозирования атак на информационные системы:

– интервальное прогнозирование – 1,414213;

– модель полигармонического полинома – 1,581138;

– статистический метод – 1,658312;

– метод экспертных оценок – 1,802776;

– метод индуктивного прогнозирования – 1,5.

После проведения анализа результатов экспериментов выяснилось, что наилучшим методом прогнозирования атак на информационные системы является метод на основе интервального прогнозирования. Преимущество данного метода в полноте полученных результатов и в точности задания модели информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеева, М. С. Угрозы безопасности локальных вычислительных сетей / М. С. Алексеева, Е. В. Иванова // Молодой ученый. – 2014. – № 18 (77). – С. 212–213.

2. Ларионов, К. О. Разработка системы контроля распределения трафика веб-ресурса на основе прогнозных рядов модели полигармонического полинома / К. О. Ларионов // Молодой ученый. – 2019. – № 35 (273). – С. 5–9.

3. Паюсова, Т. И. Информационные технологии : метод. рекомендации по выполнению лаборатор. работ / Т. И. Паюсова. – Тюмень : ТюмГУ, 2021.

REFERENCES

1. Alexeeva M.S., Ivanova E.V. Ugrozy bezopasnosti lokalnyh vychislitelnyh setej [Local Area Network Security Threats]. *Molodoj uchenyj* [Young Scientist], 2014, no. 18 (77), pp. 212-213.

2. Larionov K.O. Razrabotka sistemy kontrolja raspredelenija trafika veb-resursa na osnove prognoznyh rjadov modeli poligarmonicheskogo polinoma [Development of a System for Controlling the Distribution of Web Resource Traffic Based on Forecast Series of the Polygarmonic Polynomial Model]. *Molodoj uchenyj* [Young Scientist], 2019, no. 35 (273), pp. 5-9.

3. Payusova T.I. *Informacionnye tehnologii: metod. rekomendacii po vypolneniju laborator. rabot* [Information Technology. Recommended Practice for Laboratory Work]. Tyumen, Tyumen State University, 2021.

RESEARCH OF METHODS OF FORECASTING ATTACKS ON INFORMATION SYSTEMS

Natalia A. Golovacheva

Senior Lecturer, Department of Information Security,
Volgograd State University
golovacheva.natalya@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Nikita E. Andreichenko

Student, Department of Information Security,
Volgograd State University
IBb-191_858111@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article analyzes the methods of forecasting attacks on information systems. Within the framework of experimental studies, the best method for predicting attacks on information systems has been identified. At the present stage of society's development, the problems of information security come to the fore in most areas of the company's activities. This is due to a significant number of informatization projects currently being implemented. Most of them are aimed at building a unified information space in order to optimize the processing of large volumes of various kinds of information, including ensuring its reliable storage and prompt access for participants of information exchange. Priority tasks in this direction are: identification, analysis and classification of existing mechanisms for the implementation of threats to information security; assessment of possible damage; identification of basic measures to counter threats; elimination of vulnerabilities; development of security criteria and protection mechanisms. One of the means of solving these problems is the detection of computer attacks. Malicious impacts on information systems can be presented in the form of network attacks. A network attack is an intentional action by third parties aimed at establishing control over a local or remote computer or computer system. As a result of attacks, attackers can disrupt the network, change account rights, receive users' personal data and implement other goals. Network attacks by the nature of the impact on the network can be divided into active and passive. The active ones affect the network, which may cause the network to malfunction, or modification of its settings. This type of exposure leaves traces in the network, which is why it is immediately calculated that it will be detected. A passive attack is carried out without affecting the network. But her work violates network security. It is much more difficult to detect it than the active one due to the lack of direct intervention. Basically, the purpose of the attack is unauthorized access to protected information, distorting it or intercepting it. In the first case, the data is changed, in the second, access is performed without interfering with the data structure.

Key words: information system, vulnerability of the information system, attack on the information system, information security threats, network attacks, interval forecasting.