ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ОПРЕДЕЛЕНИЯ ЗАКОНА РАСПРЕДЕЛЕНИЯ АТАК ЗЛОУМЫШЛЕННИКОВ

***Оладько Владлена Сергеевна**, кандидат технических наук, г. Волгоград*

В статье рассмотрена проблема идентификация закона распределения атак злоумышленника. Проведен анализ статистики распространения угроз информационной безопасности и выделены наиболее актуальные атаки злоумышленника на информационные системы и локальные сети предприятий. Проанализированы возможные законы распределений, которым могут соответствовать статистики атак. Показано, что наиболее часто атаки злоумышленника имеют нормальные, показательные и пуассоновский законы распределения вероятностей. Предложен подход к определению закона распределения атак злоумышленника, использующий методы графического и теоретического анализа статистической выборки, содержащей эмпирические данные об атаках злоумышленника. Описана архитектура и функции программного комплекса разработанного для определения закона распределения атак злоумышленника. Описан пример демонстрирующий работу разработанного программного комплекса и прокомментированы результаты. Сделан вывод о возможности его практического применения.

***Ключевые слова**: информационная безопасность, информационная система, прогнозирование, угрозы, инсайдер, система защиты, гипотеза, критерий согласия, статистическая выборка, нормальное распределение, показательное распределение, распределение Пуассона.*

THE SOFTWARE FOR THE IDENTIFICATION DISTRIBUTION LAW OF INTRUDER ATTACKS

***Vladlena Oladko**, Ph.D., Volgograd*

Article is devoted to the identification the distribution law of intruder attacks. Analysis of the statistics dissemination of information security threats is conducted and the most urgent intruder attacks on information systems and local networks of enterprises are selected. The possible distribution of laws, which may correspond to the statistics of attacks, is analyzed. Is shown that intruder attack have normal, exponential and Poisson probability distribution laws. Approach to the identification distribution law of attacks using graphical methods and theoretical analysis of the statistical sample containing empirical data is proposed. Architecture and function of software developed for the identification distribution law of intruder attacks are described. An example demonstrates the developed software and the results are commented. Conclusion about the possibility of practical application of software is made.

***Keywords**: information security, information system, forecasting, threats, insider protection system, hypothesis, goodness of fit, statistical sampling, normal distribution, exponential distribution, the Poisson distribution.*

Введение

Основу любой информационной системы предприятия и организации составляют компьютеры, представляющие собой сервера и автоматизированные рабочие места пользователей, предназначенные для реализации ключевых бизнес-процессов организации. В тоже время, когда пользователь работает на компьютере, то в нем постоянно фиксируется различная информация о его деятельности, накапливаются данные, которые могут быть конфиденциальной информацией, коммерческой тайной, персональными данными пользователей, безопасность которых может быть нарушена вследствие атак злоумышленника. Следовательно, актуальным направлением в области обеспечения информационной безопасности является анализ статистических данных о распределениях атак злоумышленников с целью выявления законов их распределения и дальнейшего прогнозирования. Полученная в результате анализа распределений атак информация может быть использована для составления модели актуальных угроз и выбора наиболее эффективных средств защиты информации, применение которых позволит снизить общий уровень риска.

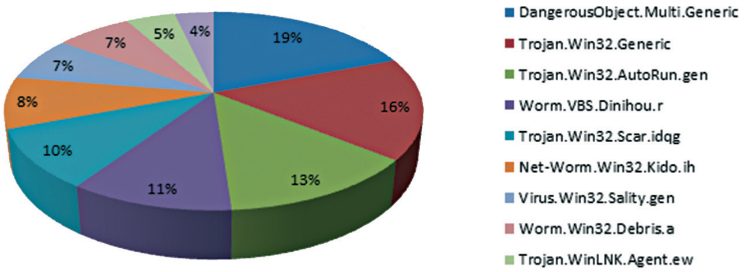

Рис. 1 *– Статистика распространения вредоносного ПО на декабрь 2014 года*

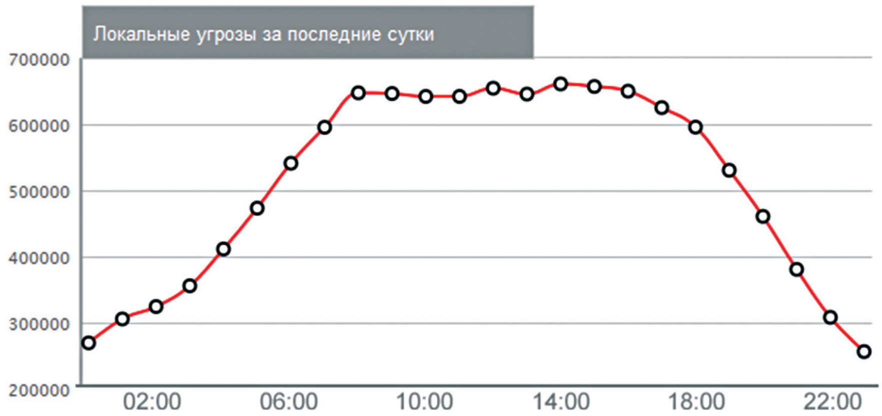

Рис. 2 *– Статистика атак злоумышленников за сутки (экранная копия)*

Распределения атак злоумышленника

Атака - попытка преодоления системы защиты информационной системы (ИС), таким образом можно считать, что атакой злоумышленника является любое действие, которое заключается в поиске и использовании той или иной уязвимости или канала утечки. По данным компании CiscoSystems [1] наиболее атакуемыми элементами в ИС являются: маршрутизаторы, коммутаторы, хосты (серверы и рабочие станции пользователей), сеть, приложения. Причем, как показывают данные исследования проводимого компанией Securitylab[1] за последние несколько лет, более 70% всех нарушений информационной безопасности и утечек данных связано с действиями именно внутренних злоумышленников – сотрудников-инсайдеров предприятия. По своей цели атаки злоумышленников, как правило, направлены на: хищение персональных данных, хищение платежных данных и информации о банковских картах, хищение логинов и паролей пользователей, хищение медицинских данных и карт, адресов электронной почты и т.п.

1 Хакерские атаки в январе: В 2014 году злоумышленники нападают с новой силой//SecurityLab. URL - http://www.securitylab.ru/news/449374.php (дата обращения 24.11.2014)

В соответствии с [2-4] к наиболее распространенным атакам злоумышленника относят:

атаки с помощью вредоносного программного обеспечения;

атаки, осуществляемые через электронную почту;

Dos и DDos-атаки;

прослушивание сети и снифинг;

несанкционированный доступ;

человек посередине (Men-in-middle);

вызов исключительных ситуаций;

хищение оборудования и носителей.

По данным «Лаборатории Касперского» [5, 6] среди локальных атак, проводимых с помощью вредоносного ПО наиболее популярными являются следующие вирусы и трояны: DangerousObject.Multi.Generic, Trojan.Win32.Generic и Trojan.Win32.AutoRun.gen на долю которых приходится 19%, 16% и 13% всех атак соответственно (см. рисунок 2).

Среди сетевых атак наиболее популярными на начало декабря 2014 года являются атаки типа: DoS.Generic.SYNFlood (65%), Intrusion.Win.NETAPI.buffer-overflow.exploit (14%), Bruteforce.Generic.RDP, Scan.Generic.UDP (8%), направленные на отказ в облуживании, перебор паролей и про-

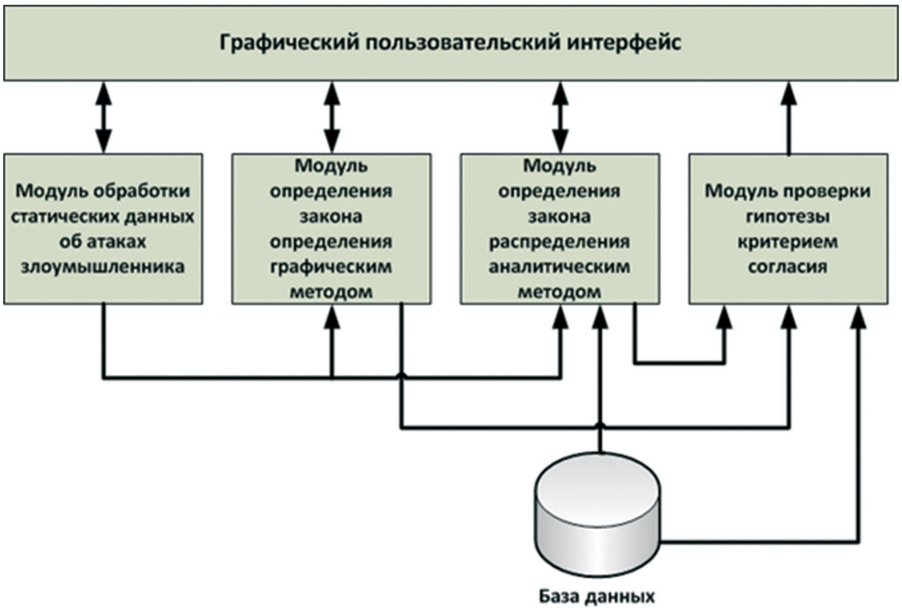

Рис. 3 – Архитектура программного комплекса для определения закона распределения атак злоумышленника

слушивание сети. Также статистические данные ежедневных исследований атак злоумышленников, публикуемые аналитиками SecureList[2] (см. рисунок 2), показывают, что большинство случаев реализации атак приходиться на дневное время суток, принимая пиковые в период с 9-00 до 17-00.

Таким образом, можно сделать вывод о том, что большинство атак злоумышленников происходит во время рабочего дня и скорее всего, направлены именно на ИС и компьютерные сети организаций и предприятий.

Анализ литературных источников [7,8] показывает, что статистические данные об атаках можно представить в виде некоторой случайной величины, которую можно охарактеризовать посредством закона распределения, при этом наиболее часто используются законы нормального распределения, логарифмически-нормального распределения, показательного распределения и распределения Пуассона. Однако, на практике имея информацию о статистике атак, для ее дальнейшей обработки и использования, необходимо точно знать о законе распределении вероятностей случайной величины X, описывающей эту статистику. Следовательно, в этом случае актуальным будет решение проблемы связанной с определением закона распределения атак злоумышленника на основе эмпирической выборки.

2 Статистика//SecureList. URL: https://securelist.ru/statistics/ (дата обращения 04.12.2014)

Программный комплекс для определения закона распределения атак злоумышленника на основе статистических данных об атаках

Для решения задачи определения закона распределения атак злоумышленника автором бы разработан программный комплекс, выполняющий следующие функции:

1. Ввод статистических данных об атаках злоумышленников.
2. Выбор графического или аналитического метода определения закона распределения.
3. Расчет показателей формы распределения для аналитических методов.
4. Построение графиков эмпирических данных об атаках злоумышленника и теоретических распределений и их последующее сопоставление для графических методов.
5. Сравнение показателей формы распределения статистических данных об атаках с допустимыми показателями различных теоретических законов распределений.
6. Выдвижение гипотезы о принадлежности к одному из видов распределений.
7. Проверка гипотезы о принадлежности к выбранному теоретическому закону распределения в соответствии с критерием согласия Пирсона.
8. Принятие решения о совпадении/несовпадении закона распределения статистических данных об атаках и выбранного теоретического закона распределения.
9. Вывод результатов анализа данных.

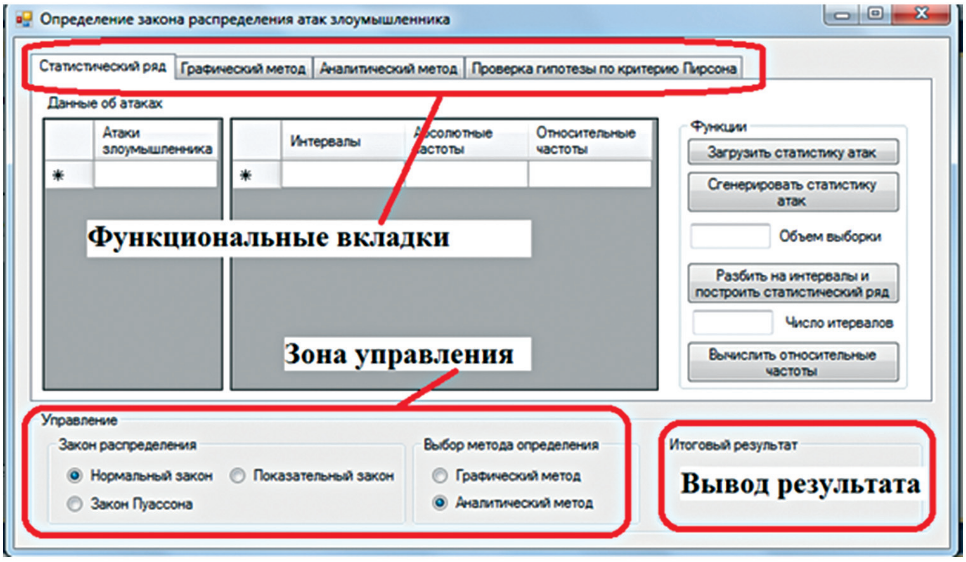

***Рис. 4** – Пользовательский интерфейс. Зоны и функциональные вкладки (экранная копия)*

В качестве входных данных в программный комплекс поступают числовые данные (целого или вещественного типа) о статистики атак злоумышленника, статистические таблицы, а также тип выбранного метода определения закона распределения.

В качестве выходных данных – графики, показатели формы распределения статистических данных об атаках, результат определения закона распределения.

Разработанный программный комплекс, предназначенный для определения закона распределения атак злоумышленника, имеет графический пользовательский интерфейс и модульную архитектуру (см. рисунок 3).

Пользовательский интерфейс (см. рисунок 4), состоит из зоны управления и четырех вкладок, реализующих основные функциональные возможности программного комплекса:

Вкладка «Статистический ряд».
Вкладка «Графический метод».
Вкладка «Аналитический метод»
Вкладка «Проверка гипотезы».

Пример определения закона распределения атак с помощью разработанного программного комплекса

В примере, демонстрирующем работу разработанного программного комплекса, в качестве тестовых данных была использована статистическая выборка, описывающая атаки злоумышленника, распределенные по заранее известному закону. В качестве закона распределения был выбран показательный закон распределения, функция плотности распределения, вероятности которого описывается формулой 1.

$$f(x)=\begin{cases}\lambda e^{-\lambda x} \text{ при } x\geq 0\\ 0 \text{ при } x<0\end{cases} \qquad (1)$$

где λ - параметр обратно-пропорциональный математическому ожиданию.

И выдвинута гипотеза $H0$ о показательном законе распределения и альтернативная ей $H1$- о другом виде закона распределения.

После ввода и обработки статистических данных и расчета в программном комплексе математического ожидания, была построена таблица теоретических вероятностей. И с помощью аналитического метода оценена близость между теоретическими вероятностями и относительными частотами. Поскольку расхождения между ними признаются программой не значительными, то программный комплекс выдвигает гипотезу о близости к показательному закону распределения. Далее по критерию согласия Пирсона проверяется гипотеза $H0$ о показательном законе распределения. Для этого по формуле высчитывается значение наблюдаемого критерия χ^2 Пирсона и сравнивается с критическим значением из таблицы при уровне значимости 0,05 и числе степеней свободы 5. Поскольку наблюдаемое меньше критического то гипотеза считается программой принятой. Результаты представлены на рисунке 5.

Таким образом, можно сделать вывод о работоспособности программного комплекса, правильности выдаваемых результатов и возможности его применения для определения закона распределения атак злоумышленника.

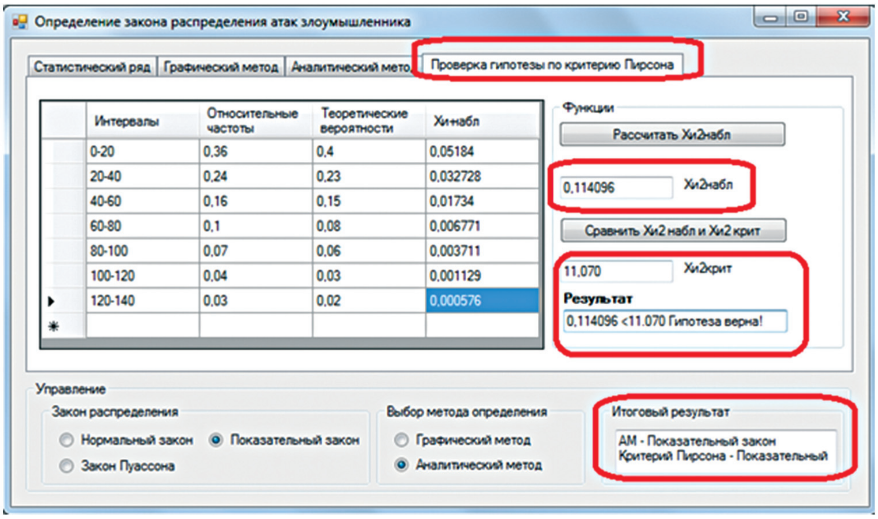

***Рис. 5** – Проверка гипотезы о показательном распределении (экранная копия)*

Вывод

Разработанный программный комплекс для определения законов распределения атак злоумышленника может применяться на практике при анализе атак и инцидентов нарушения информационной безопасности на предприятии, а также в учебном процессе при выполнении лабораторных практикумов в качестве стенда макета при обучении студентов в области информационной безопасности.

Литература:

1. Смирнов Н. Цена инсайдерства//Директор информационной службы. - №7, 2013.URL: http://www.osp.ru/cio/2013/07/13036639/ (дата обращения 24.11.2014)
2. Крошилин С. Инсайдер – внутренний враг информационной безопасности//«Информационные Ресурсы России» . -№4, 2009
3. Вихорев С.В. Классификация угроз информационной безопасности//CNews Аналитика.URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения 03.12.2014)
4. Мошков А.Н. Новые информационные угрозы требуют идти в ногу со временем////Вопросы кибербезопасности. -2013 - № 3(4). – С. 2 – 6.
5. Гарнаева М.А., Функ К. Kaspersky Security Bulletin 2013//Вопросы кибербезопасности. -2013 - № 3(4). – С. 65 – 68.
6. Эмм Д., Гарнаева М., Чевышев В. Развитие информационных угроз в третьем квартале 2014 года// SecureList. URL: https://securelist.ru/analysis/malware-quarterly/24365/razvitie-informacionnyx-ugroz-v-tretem-kvartale-2014-goda/ (дата обращения 04.12.2014).
7. Дрозд А. Виды современных рисков, связанных с утечками данных//SecurityLab. URL - http://www.securitylab.ru/blog/company/securityinform/116908.php (дата обращения 03.12.2014).
8. Меньших В.В., Толстых О.В. Моделирование возникновения угроз информационной безопасности на объекте информатизации//Информационная безопасность. – 2011. – Вып.1 – С. 117-120.

References

1. Smirnov N. Tsena insayderstva//Direktor informatsionnoy sluzhby. - №7, 2013.URL: http://www.osp.ru/cio/2013/07/13036639/ (data obrashcheniya 24.11.2014)
2. Kroshilin S. Insayder – vnutrenniy vrag informatsionnoy bezopasnosti//«Informatsionnyye Resursy Rossii». -№4, 2009
3. Vikhorev S.V. Klassifikatsiya ugroz informatsionnoy bezopasnosti//SNews Analitika.URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (data obrashcheniya 03.12.2014)
4. Moshkov A.N. Novyye informatsionnyye ugrozy trebuyut idti v nogu so vremenem//Voprosy kiberbezopasnosti. -2013 - № 3 (4). - S. 2 - 6
5. Garnayeva M.A., Funk K. Kaspersky Security Bulletin 2013 // Voprosy kiberbezopasnosti . -2013 - № 3 (4).- S. 65 - 68
6. Emm D., Garnayeva M., Chevyshev V. Razvitiye informatsionnykh ugroz v tret'yem kvartale 2014 goda// SecureList. URL: https://securelist.ru/analysis/malware-quarterly/24365/razvitie-informacionnyx-ugroz-v-tretem-kvartale-2014-goda/ (data obrashcheniya 04.12.2014)
7. Drozd A. Vidy sovremennykh riskov, svyazannykh s utechkami dannykh//SecurityLab. URL - http://www.securitylab.ru/blog/company/securityinform/116908.php (data obrashcheniya 03.12.2014)
8. Men'shikh V.V., Tolstykh O.V. Modelirovaniye vozniknoveniya ugroz informatsionnoy bezopasnosti na ob»yekte informatizatsii//Informatsionnaya bezopasnost'. – 2011. – Vyp.1 – S. 117-120