УДК: 519.862
DOI: 10.34046/aumsuomt91/4

МОДЕЛИРОВАНИЕ БЕЗОПАСНОСТИ В СУДОВЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

А. В. Фролов, начальник класса кафедры АИС
Е. С. Фролова, аспирант
А. А. Антонов, старший преподаватель
А.С. Новак, студент

Эффективность мероприятий по защите компьютерной системы зависит от метода реализации угрозы. Она определяется конкретным средством защиты, конкретной подсистемой безопасности. Средства защиты информационной системы взаимодействуют комплексно. Оценка потенциала защиты информационных систем – задача актуальная. Реализуется различными методами (экспертными, эвристическими, математическими, статистическими, например, классификации угроз по опасности). Учитываются механизмы, конфигурации защитных мер. Кроме проблем идентификации структурных составляющих, подлежащих оценке, формирования комплекса индикаторов, следует иметь обобщающий, интегральный показатель уровня защищенности всей системы. Необходимо учитывать, что класс защищенности системы формально определяется «индексом риска», например, разностью максимального рейтинга степени секретности обрабатываемых системой данных и минимальным рейтингом допуска пользователей. При этом у каждой компании (системы) – свои требования к защищенности: некоторых волнует инсайд, других DDoS-атаки, третьих – аутентификация и др.

В работе осуществлен системный анализ проблемы защищенности компьютерной (информационной) системы. Проведена формализация задачи на языке теории графов и математической логики. Рассмотрена конкретная математическая модель атак информационных систем группового разделения на класс защищенных надежно и класс слабо защищенных. Модель применима к проблемам защиты судовых сетей. Проделан регрессионный, дисперсионный анализ по ряду лет.

Ключевые слова: система, сеть, угроза, защита, уязвимость, математическая модель, киберугроза, дисперсионный анализ

The efficiency of actions for protection of a computer system depends on a threat implementation method. It is defined by a concrete security measure, a concrete subsystem of safety. Means of protection of an information system interact in a complex. Assessment of potential of protection of information systems – a task relevant. Is implemented by various methods (expert, heuristic, mathematical, statistical, for example, classifications of threats by danger). Mechanisms, configurations of protective measures are considered. Except problems of identification of the structural components which are subject to assessment, formations of a complex of indicators it is necessary to have the generalizing, integrated indicator of level of security of all system. It is necessary to consider that the class of security of a system formally is defined by "the index of risk", for example, the difference of the maximum rating of degree of privacy of the data processed by a system and the minimum rating of admission of users. At the same time at each company is (systems) – the requirements to security: some the insider concerns, others the DDoS-attacks, the third – authentication, etc. Formalization of a task in language of the theory of counts and mathematical logic is carried out. The concrete mathematical model of the attacks of the information systems of group division into a class protected reliably and a class of poorly protected is considered. The model is applicable to problems of protection of ship networks. Also regression, dispersive analysis by a row of years is done.

Keywords: system, network, threat, protection, vulnerability, mathematical model, cyber threat, analysis of variance.

Введение

Развитие Е-Навигации повышает необходимость эффективного управления обменом большим количеством информации, как между судами, так и между судами и береговыми службами. Растут не только объемы передаваемых данных, но и расширяется назначение информации. Судовые компьютерные системы становятся все более интегрированными с береговыми и с глобальной сетью Интернет. Обеспечение информационной защищенности становится актуальной проблемой, с которой следует считаться в каждой информационной системе (ИС). Внедрять релевантную политику безопасности, охватывая и компьютерные, и информационные, и технологические, и коммуникационные аспекты, стремятся многие компании, опыт которых может быть полезен морским службам. Каждая со своими спецификациями к степени защищенности, типу защищенности. Одних волнует больше внутренняя информация, других DDoS-атаки, третьих вторичная аутентификация и т.д. Ущерб, риски у всех различные [1, с.37]. Но всех интересуют актуальные задачи:

1) идентификация момента вторжения (увеличения интенсивности входного потока и распределения запросов);

2) изменение протокола (алгоритма) обслуживания, чтобы не обслуживать (игнорировать) искусственно генерируемый злоумышлен-

никами поток задач или прекратить обслуживание, пока не «закроют» уязвимости.

Например, успешной является модель уязвимостей Take-Grant [2, с.1] анализа прав доступа с помощью графа доступа, она подтверждает/опровергает степень защищенности системы по регламенту требований: если ресурсы компоненты системы обладают потенциальной опасностью определенного класса, то следует найти удельную эффективность метода (программы, аппаратуры) защиты для конкретной угрозы. Если же рассматривать DDoS-атаки, то к потоку задач пользователей на входе (регулярному потоку) добавляется искусственный, интенсивный поток задач с целью нанесения ущерба за счет снижения эффективности обслуживания (даже блокирования системы) – в системе растет объем отказов (цель атаки – достигнута).

Постановка общей задачи

С каждой задачей важно ассоциировать численные величины, функционалы, модели идентификации искусственного потока по распределению его параметров. Это позволит зафиксировать момент разладки процесса, регулярного потока задач, выделить из смешанного потока и обслужить задачи регулярного потока, или прекратить обслуживание, пока не завершится атака [3, с.34].

Для ситуаций с распределенными системами, можно считать входной поток распределенным по закону Бернулли: поступившая задача с вероятностью α_0 запускается сразу, с вероятностью $1-\alpha_0$ – ставится в очередь. Интенсивность «подмешиваемого» искусственного потока может увеличить вероятность ожидания в очереди.

Разрабатывая политику информационной безопасности значимых ИС (класса защиты А, например), применяют, в частности, тактику мандатного (многоуровневого), ролевого разграничения доступа. В моделях такого рода (Take-Grand, MLS и др.) отражены особенности широко применяемых политик безопасности, механизмов используемых аппаратно-программного окружения, характеристик окружения и другие.

Есть общая теорема [4, с. 462] (Харрисон, Руззо, Ульман, 1976 г., теорема об алгоритмической неразрешимости проблемы компьютерной безопасности). Достоинства модели Take-Grant отмечены многими исследователями (в частности [5, с.53]). Её используют в задачах аутентификации с помощью графа доступа (узлы – объекты/субъекты, дуги – права). Расширенная модель Take-Grant позволяет подтверждать (опровергать) степень защищенности ИС, информационных потоков в системах с разграничением по регламенту требований.

Формализация задачи, ее конкретизация и исследование

Мониторинг осложняется проведением оценки риска, взаимосвязи инициирующих событий, их влияния на уязвимость системы. Логическая модель контроля процессов записывается дизъюнктивной нормальной формой:

$$\bigvee_{j\in\{1,\dots,L\}} y_j$$

Такой формально-алгебраический подход полезен при полной формализации проблемы, системы, среды, что весьма проблематично. Поэтому рассмотрим модель атак ИС, сети, сообщества из n групп в каждой группе i (i=1, 2, …, n), численность защищенных подсистем, пользователей, аккаунтов - Ri, уязвимых - Hi.

Рост защищенных в группе i (j) определим балансовым методом:

$$\Delta A_i \equiv A_i(c - pR_i)A_j$$
$$\Delta R_i \equiv -R_i(m - kA_i)R_j$$

Можно предложить модель:

$$\Delta R_i \equiv -R_i(m - kA_i)R_j$$
$$\frac{dA_i}{dt} = (c - pR_i)A_iA_j$$
$$\frac{dR_i}{dt} = -(m - kA_i)R_iR_j$$
$$\frac{dA_j}{dt} = (c - pR_j)A_iA_j$$
$$\frac{dR_j}{dt} = -(m - kA_j)R_iR_j$$
$$c, p, k, m > 0$$

Состояние равновесия отличное от

$$A_{\downarrow j} = A_{\downarrow j} = R_{\downarrow i} = R_{\downarrow j} = 0$$

определяется из соотношений:

$$c - pR_i = 0$$
$$m - kA_i = 0$$
$$c - pR_j = 0$$
$$m - kA_j = 0$$

или

$$R_i = R_j = \frac{c}{p}, A_i = A_j = \frac{m}{k}$$

Обсуждение результатов

Для эффективной систематизации и формализации, структурирования необходимы группы специалистов (математики, криптоаналитики, сетевые специалисты и др.), способные рассматривать критичность ситуации, оценивать риски, строить и исследовать модели киберугроз, принимать решения, разрабатывать сценарии реализации политики безопасности [6, с.101].

Кроме рассмотренной математической модели проведен статистико-математический анализ. Общее количество компьютерных преступлений (табл. 1) при этом имеют некоторую периодичность (рис.1).

Проведенный статистико-регрессионный анализ дает следующие результаты: множественный коэффициент R=0,389654, R-квадрат – 0,15183, нормированный R-квадрат – п 0,098819, стандартная ошибка – 5,067904.

Проведенный дисперсионный анализ дал результаты (критерий Фишера):

F=2,86414, значимость – 0,109953,
остатки – SS=410,9384,
MS=25,68365,
коэффициенты равны 2003,676+/–3,09071, 0,000725+/–0,000428,
t-статистика – 648,2899 и 1,692377,
нижние и верхние 95%-значения соответственно равны 1997,124; 2010,228 и –0,00018; 0,001633.

Таблица 1 –Общее количество компьютерных преступлений

Год	Общее количество компьютерных преступлений
2000	843
2001	2066
2002	4122
2003	7782
2004	9092
2005	10612
2006	9333
2007	5215
2008	4387
2009	4697
2010	5679
2011	7087
2012	8665
2013	10857
2014	9567
2015	8546
2016	6086
2017	5121

Рисунок 1 – Общее количество компьютерных преступников за 2000-2017 гг.

Заключение

Современная компьютерная (информационная) сеть, связывающая суда между собой и с берегом, формируется и функционирует, развивается из множества элементов, подсистем. Уровень ее безопасности не только диктуется сложностью структурной, но и растущим разнообразием угроз окружения. Развитие Е-Навигации повышает требования к безопасности систем в целях защиты от злоумышленников. Для оценки риска и противодействия угрозам необходимо прогнозирование (моделирование) рисков, уязвимостей системы.

Литература

1.Щеглов К.А, Щеглов А.Ю. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации.–2013.–вып.101.– №2.–С.36-43.
2.Разграничение доступа к информации в компьютерных системах. URL: http://lib2.znate.ru/docs/index-323588.html?page=8 (дата доступа: 02.12.2018).
3.Цирлов В.Л. Основы информационной безопасности автоматизированных систем. – Ростов-на-Дону: Феникс, 2008. – 173 с.

4. Harrison M., Ruzzo W., Ullman J. ESIGN: Protection in operating systems, 1976, vol.19, №8. - pp.461-471.
5. Девянин П.Н. Модели безопасности компьютерных систем: учеб.пособие для студ. высш. учеб. заведений. – М.: Изд. центр «Академия», 2005. – 144 с.
6. Казиев В.М., Казиева Б.В., Казиев К.В. Основы правовой информатики и информатизации правовых систем.– М.: Инфра-М. Вузовский учебник (2-ое изд.),2017. – 336 с.

References

1. Shcheglov K.A Shcheglov A.Y. Zashchita ot atak na uyazvimosti prilozhenij modeli kotrolya dostupa voprosy zashchity informacii vyp 101, №2, 2013 p.36-43
2. Razgranichenie dostupa k informacii v kompyuternyh sistemah URL http://lib2.znate.ru/docs/index-323588.html?page=8 02.12.2018
3. Cirlov V.L. Osnovy informacionnoj bezopasnosti avtomatizirovannyh system. Rostov-na-Donu - Feniks-2008-173 p
4. Harrison M., Ruzzo W., Ullman J. ESIGN: Protection in operating systems. 1976, vol.19, №8. - pp.461–471.
5. Devyanin P.N. Modeli bezopasnosti kompyuternyh system. Ucheb posobie dlya stud.vyssh.ucheb.zavedenij. M.: izd.centr “Akademiya” 2005-144 p.
6. Kaziev V.M. Kazieva B.V. Kaziev K.V. Osnovy pravovoj informatiki I informatizacii pravovyh system. M.: Infra M. Vuzovskij uchebnik 2-oe izd 2017-336p.