УДК 004:056
ББК 32.81

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ В КИБЕРПРОСТРАНСТВЕ: МОДЕЛИРОВАНИЕ КОАЛИЦИОННЫХ АТАК В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ХОЗЯЙСТВЕННОЙ СИСТЕМЫ

Шипилева Алла Владимировна

Старший преподаватель кафедры экономической информатики и управления
Волгоградского государственного университета
ashipileva@mail.ru
Проспект Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В современном обществе информационные активы являются основным ресурсом и обеспечивают компаниям добавленную стоимость. Сложность и размеры ущерба, вызванного злоумышленными атаками в сети Интернет растут с каждым годом. Для исследования проблем экономической безопасности и защищённости корпоративных и виртуальных сетей предлагается использовать модель коалиционной атаки, построенную на основе ветвящихся процессов с иммиграцией. С помощью модели определяются наиболее вероятные маршруты действий злоумышленников и рекомендации по закрытию уязвимых мест.

Ключевые слова: экономическая безопасность, информационное пространство, информационные активы организации, коалиционная атака, уязвимости, ветвящиеся процессы.

В современных условиях любая компания вынуждена адаптироваться к динамике внешней среды в основном за счет инновационных факторов. Инновационный вектор развития бизнеса обуславливает необходимость комплексного решения проблем обеспечения экономической безопасности, в связи с возможностью усиления известных и появлением новых видов рисков и угроз: потеря предприятием части своих ресурсов, потеря доходов, появление дополнительных расходов в результате осуществления производственной и финансовой деятельности. Экономическая безопасность организаций определяется наличием конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического и организационного потенциалов стратегическим целям и задачам организации. Экономическая безопасность может быть представлена несколькими составляющими: технологической, кадровой, финансовой, политико-правовой, информационной, конкурентной, экологической и другими [2].

В настоящей статье проводится анализ экономической безопасности по одному из функциональных направлений, которое в современных условиях является основным – информационному. Появление глобальных сетей связи, и в первую очередь Интернета, привело к значительным изменениям в организации и ведении коммерческой деятельности. Возникли не только новые направления ведения бизнеса, но и были внесены изменения в уже существующие. Интернет и другие виды электронных коммуникаций стали мощным катализатором развития информационной составляющей бизнеса и создания новой стоимости в результате совершенствования процессов поиска, организации, отбора, синтеза и распро-

странения информации. Однако широкое представление компании в глобальной сети Интернет породило и новые риски, связанные со случайными и преднамеренными воздействиями, направленными на уничтожение, видоизменение тех или иных данных, изменение степени доступности ценных сведений. Если раньше опасность состояла в основном в краже (воровстве, копировании) секретных или конфиденциальных сведений и документов, то сейчас получило развитие незаконное оперирование компьютерными БД, незаконное использование электронных массивов без согласия собственника или владельца и извлечение материальной выгоды.

По данным компании KPMG [1], которая совместно с Symantec, RSA, Checkpoint провела исследования о потерях, возникающих вследствие возникновения различных угроз, только прямые убытки предприятий от нарушения информационной безопасности составляют в среднем 108 тыс. долл. в год. В ходе исследования было опрошено 641 человек из числа старших менеджеров крупнейших корпораций мира – тех, у кого годовой оборот свыше 50 млн долларов США. Примерно четверть выборки составляли госструктуры, 22 % – финансовые организации, 26 % – компании, работающие в потребительском секторе и 27 % – в области информационных технологий и телекоммуникаций. Это были компании, разрабатывающие программное обеспечение всему миру – в Европе, на Ближнем Востоке, в Африке, в странах Азиатско-Тихоокеанского региона, Северной и Южной Америке. Принимали участие и крупнейшие российские компании. Как показало исследование, менее чем в половине компаний решения по вопросам информационной безопасности принимаются на уровне совета директоров. В остальных она возложена на сотрудников отделов информационных технологий. Исключение составляет финансовый сектор, где руководство осознаёт, что информация является стратегическим ресурсом и плохая защита может привести к разрушительным последствиям. Но в этом секторе лишь в 60 % компаний информационной безопасностью озаботилось высшее руководство. В большинстве компаний не ведётся учет нарушений информационной безопасности, нет соответствующей отчетности. Основные потери компаний представлены в таблице 1.

Важное значение для киберпространства имеет информационная составляющая, охва-

Таблица 1

Виды информационных угроз и потери компаний

Виды информационных угроз	Доля в общем числе инцидентов, %	Потери компаний, млн долл.
Инциденты, связанные с компьютерными вирусами	61	10,0
Кражи аппаратного обеспечения (в том числе ноутбуков)	38	3,0
Взлом систем электронной почты	29	0,2
Кражи программного обеспечения	16	3,0
DOS-атаки (действия, вынуждающие систему работать в максимальном режиме нагрузки, что в итоге приводит к отказу)	14	0,5
Взлом Web-сайтов	12	0,2
Отказ информационной системы	12	4,0
Потеря конфиденциальности информации	5	1,5
Искажение вход-выход информации	4	0,1

Примечание. Составлено по данным аналитического исследования компании KPMG [1].

тывающая накопление, защиту информации и ограничение доступа к ней. Обеспечение безопасности корпоративных и виртуальных сетей компаний предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования сети, а также попытках модификации, хищения, вывода из строя или разрушения ее компонентов: аппаратных средств, программного обеспечения, данных и персонала [3].

Для большинства компаний риски информационной безопасности являются наиболее критичными из всего многообразия операционных рисков.

От того, насколько эффективно банки, страховые и инвестиционные компании и другие организации управляют этими рисками, зависит их конкурентноспособность и капитализация. По результатам исследования IT Governance Institute, объявление об инциденте информационной безопасности негативно влияет на рыночную стоимость компании. Организации, в которых произошел инцидент информационной безопасности, в среднем теряют 2,1 % рыночной стоимости. К основным инцидентам информационной безопасности относятся:

– инциденты, связанные с компьютерными вирусами,

– кражи аппаратного обеспечения (в том числе ноутбуков),

– взлом систем электронной почты,

– кражи программного обеспечения,

– DOS-атаки (действия, вынуждающие информационные системы работать в максимальном режиме нагрузки, что в итоге приводит к отказу),

– взлом web-сайтов,

– отказ информационной системы,

– потеря конфиденциальной информации,

– искажение вход-выход информации.

Существует множество подходов к обеспечению информационной безопасности. Часть из них отражена в различных международных, национальных и отраслевых стандартах, в частности, стандарт ISO 207001:2005 «Требования к системе менеджмента информационной безопасности». В соответствии с этим стандартом, должна быть обеспечена систематическая защита всех информационных активов компании. Информационный актив в стандарте определяется таким образом, что к нему относится все связанное с информацией и имеющее ценность для организации – документы, аппаратное и программное обеспечение, базы данных, персонал. Практически все основные бизнес-процессы компаний связаны с информационными активами. Информационная безопасность, согласно стандарту, должна обеспечить сохранение основных свойств информационного актива:

– конфиденциальность – недоступность для неавторизованных пользователей;

– целостность – аккуратность и полнота;

– доступность – получение по требованию авторизованных пользователей.

Также, стандарт рекомендует идентифицировать риски информационной безопасности (инцидент произошел), реализация которых может повлечь наиболее тяжелые последствия – финансовые потери для компании.

Согласно исследованиям CERT [8] количество злоумышленных атак в сети Интернет, их сложность и размер ущерба растет с каждым годом. Основная причина – это слабая защита информационных активов компаний. В настоящее время становится актуальной задача построения интеллектуальных систем анализа защищенности корпоративных сетей, которые содержат компоненты анализа уязвимостей и оценки уровня защищенности на основе моделирования атак [4]. Моделирование атак дает возможность выявлять и устранять потенциальные проблемы информационной составляющей экономической безопасности до того, как произошел инцидент информационной безопасности, когда это относительно просто и не требует значительных затрат.

Злоумышленник обычно предваряет свои атаки предварительным зондированием всех компонентов корпоративной и виртуальной сети. На этом этапе он собирает информацию, которая является для него недоступной. На практике злоумышленником определяются роли компьютеров в сети, выделяются файловые сервера и сервера баз данных, маршрутизаторы и интеллектуальные коммутаторы. На основе этой информации злоумышленником строится дерево уязвимостей и выбирается инструментарий для проведения атак непосредственно на узлы корпоративной сети.

В настоящее время существует ряд моделей [7; 9; 10], позволяющих с разной степенью детализации описать процесс сетевой атаки. Большинство моделей основано на конечных автоматах и представляют атаку на автоматизированную систему как последовательность состояний автомата. Все существующие методы моделирования атак направлены на решение задач представления атак, оценки сложности атаки, оценки ущерба от проведенной атаки, но не предоставляют средств для автоматизированного моделирования атак с целью исследования их оптимизации. В работе [5] была разработана математическая модель злоумышленника, описывающая сетевую атаку на основе марковских ветвящихся процессов, в которой предполагается, что действиям злоумышленника соответствует стохастический алгоритм, а не детерминированный.

В данной работе рассматривается другой тип атак – коалиционная атака, когда несколько злоумышленников объединяются для достижения цели. Для построения модели имитирующей действия коалиции злоумышленников, используются ветвящиеся процессы с иммиграцией. При определении вероятности того, что злоумышленник не сможет использовать уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей. Будем рассматривать следующие типы: троичное и m – арное деревья уязвимостей (могут быть использованы и их комбинации):

1. Если дерево уязвимостей является троичным, то злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью P_1, а в правом с P_3. Действия злоумышленника, находящегося с ним в коалиции, описываются известной инфинитезимальной производящей функцией с коэффициентами q_0, q_1, q_2, …:

$$g(z)=\sum_{k=0}^{\infty} q_k z^k = q_0 + q_1 z + q_2 z^2 + \text{K}, \qquad (1)$$

а вероятности P_1 и P_3 находятся из условий [6]:

$$0 < P_1 < 1,$$

$$\frac{1}{2}\frac{P_2^2}{P_1}+\frac{1}{2}\left(\frac{q_1}{q_0}+1\right)P_2 < P_3 < \frac{1}{2}\frac{P_2^2}{P_1}+\frac{1}{2}\left(\frac{q_1}{q_0}+2\right)P_2,$$

где $0 < P_2 < 1$.

2. Если дерево уязвимостей является m-арным (m – количество уязвимостей), то злоумышленник выбирает для атаки уязвимости с порядковыми номерами 0, 1, 2, …, m, соответственно с вероятностями P_0, P_1, ..., P_m, которые определяются из условий [6]:

$$0 < P_0 < 1, 0 < P_1 < 1,$$

$$\frac{1}{2}\frac{P_1^2}{P_0}+\frac{1}{2}\left(\frac{q_1}{q_0}+1\right)P_1 < P_2 < \frac{1}{2}\frac{P_1^2}{P_0}+\frac{1}{2}\left(\frac{q_1}{q_0}+2\right)P_1.$$

Определим коэффициенты $b_2 = P_1(1-\sigma)$, $0 < a_2 < P_1$:

$$\max\left\{0,(n+1)b_n - a_n\right\} \le \omega_n \le b_n,\ n = 2,\text{K}\ ,m-1,$$

$$a_n = a_2 - \sum_{k=2}^{n-1} k\omega_k,\ b_n = b_2 - \sum_{k=2}^{n-1}\omega_k,\ n = 3, 4,\text{K}\ , m,$$

Тогда для уязвимости с номером n вероятность равна:

$$P_n = \omega_n - \left(-\frac{1}{\alpha}\sum_{k=0}^{n} q_k P_{n-k} - (n+1)\sigma P_{n+1} - \right.$$
$$\left. -\frac{1}{P_1}\sum_{k=2}^{n-1}(n-k+1)\omega_k P_{n-k+1}\right)\Big/ n,$$

где $\alpha = \frac{1}{P_1}\left(q_0 P_1 + q_1 P_0 - \frac{2q_0 P_0 P_2}{P_1}\right)$, $\sigma = -\frac{q_0 P_0}{\alpha P_1}$.

Действия злоумышленника, находящегося с ним в коалиции, описываются заданной инфинитезимальной производящей функцией (1).

Автором реализована программа моделирования деревьев уязвимостей для коалиционных атак в корпоративной сети в Microsoft Visual Studio NET 2010 на языке C#. Основные результаты компьютерного моделирования коалиционной атаки следующие:

– максимальная вероятность достижения злоумышленником цели за заданное время;

– время, затраченное злоумышленником на достижение цели;

– рекомендации по модернизации средств защиты уязвимостей.

Таким образом, предлагаемые модели коалиционной атаки при организации информационной безопасности на предприятии позволят значительно сократить потери, связанные с незаконным проникновением злоумышленников в корпоративную сеть, при этом нет необходимости нести дополнительные финансовые затраты на приобретение специального программного обеспечения. Расчет проникновения при сетевой атаке позволяет определить наиболее уязвимые места и целенаправленно организовать дополнительную защиту соответствующих узлов. Предложенные модели целесообразно использовать при организации рациональной защиты корпоративных информационных ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Аналитический отчет по информационной безопасности KPMG совместно с Symantec, RSA, Checkpoint. – Электрон. текстовые дан. – Режим доступа: http://www.kpmg.com/RU/ru/IssuesAndInsights/ArticlesPublications. – Загл. с экрана.

2. Габети, А. В. Обеспечение экономической безопасности малых и средних предприятий / А. В. Габети, Е. В. Песоцкая // Экономика и управление : сб. науч. тр. Ч. IV. – СПб. : СПбГУЭФ, 2010. – С. 161–169.

3. Курило, А. П. Обеспечение информационной безопасности бизнеса / А. П. Курило. – М. : Альпина Паблишер, 2011. – 392 с.

4. Степашин, М. В. Моделирование атак для активного анализа уязвимостей компьютерных сетей / М. В. Степашин // Сборник докладов научно-практической конференции по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика». – 2005. – С. 269–273.

5. Шипилева, А. В. Математическая модель злоумышленника в корпоративной сети /А. В. Шипилева // Сборник трудов. Управление большими системами ИПУ им. В. А. Трапезникова РАН. – 2007. – Вып. 19. – С. 127–133.

6. Шипилева, А. В. Предельные распределения для ветвящихся процессов с иммиграцией / А. В. Шипилева // Журн. Известия высших учебных заведений. Математика. – 2000. – № 1 (452). – С. 77– 83.

7. Camtepe, S. A. Modeling and detection of complex attacks / S. A. Camtepe, B. Yener // In Proceedings of the Third International Conference on Security and Privacy in Communications Networks and the Workshops. – IEEE Conference Publications, Nice, France. – 2007. – P. 234–243.

8. CERT/CC Statistics. – Mode of access : http://www.cert.org/stats/cert_stats.html. – Tittle from screen.

9. Sheyner, O. Automated generation and analysis of attack graphs / O. Sheyner // Proceedings of the IEEE Symposium on Security and Privacy. – Oakland, CA, USA – 2002. – P. 273–284.

10. Von Ohiemb, D. Formal security analysis with Interacting state machines / D. Von Ohiemb, L. Volkmar, D. Gollmann // Lecture Notes in Computer Science. – 2002. – № 2502. – P. 212–228.

ECONOMIC SECURITY IN CYBERSPACE: SIMULATION OF THE COALITION ATTACKS ON THE INFORMATION SPACE OF AN ECONOMIC SYSTEM

Shipileva Alla Vladimirovna

Senior Lecturer, Department of Economic Informatics and Management,
Volgograd State University
ashipileva@mail.ru
Prospect Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. In modern society, information assets are a major resource and provide companies with added value. The complexity and size accept damage caused by malicious attacks on the Internet that are increasing every year. To research the problems of the economic security, corporate and virtual networks protection the author suggests using the coalition attack model built on the basis of branching processes with immigration. The model identifies the most likely routes that intruders may use as well as recommends how to protect vulnerabilities.

Key words: economic security, information space, information assets of an organization, coalition attack, vulnerability, branching processes.