ISSN 2311-8725 (Online)
ISSN 2073-039X (Print)

Математические методы и модели

МЕХАНИЗМЫ СТРАХОВАНИЯ В УПРАВЛЕНИИ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вадим Анатольевич БОРХАЛЕНКО

специалист ООО «ИнфоПроСервис», Москва, Российская Федерация
vadikhide@yandex.ru

История статьи:
Принята 20.10.2016
Принята в доработанном виде 01.11.2016
Одобрена 25.11.2016
Доступна онлайн 27.02.2017

УДК 51-75+004.56
JEL: C02, C61, D81, G22

Ключевые слова:
киберстрахование, теория контрактов, информационная безопасность, DDoS, риски

Аннотация

Предмет. Рассмотрены проблемы обработки рисков информационной безопасности, связанных с реализацией кибератак типа DDoS и отсутствия эффективных технических средств снижения этих рисков. Приводятся основные недостатки организационно-технических мер противодействия DDoS-атакам, а также обосновывается распространенность и выгодность заказа атак данного вида злоумышленниками и недобросовестными конкурентами для нарушения обеспечения непрерывности бизнеса организации, приводятся величины возможных убытков экономических субъектов, потерпевших от реализации DDoS-атаки. Обосновывается необходимость использования экономических методов обеспечения информационной безопасности на примере моделей киберстрахования. Проблема разработки страховых механизмов управления рисками информационной безопасности в настоящее время слабо проработана и является одной из ключевых в области развития экономических методов обеспечения информационной безопасности социально-экономических систем.

Цели. Выявление недостатков существующих организационно-технических мер обеспечения информационной безопасности и обоснование необходимости разработки и использования страховых механизмов управления рисками информационной безопасности.

Методология. С помощью аппарата линейного программирования, теории полезности и актуарной математики разработана математическая модель взаимовыгодного страхового контракта от реализации атаки типа DDoS, которая представляет серьезную угрозу для обеспечения непрерывности бизнеса организации.

Результаты. Разработана страховая модель, обеспечивающая перенос риска, связанного с реализацией DDoS-атак.

Выводы. Предложенный метод киберстрахования от реализации DDoS-атак является более экономичным, нежели большинство существующих технических средств и может применяться для снижения степени возможных финансовых убытков от реализации информационных атак.

Введение

В настоящее время роль информационных технологий в жизни общества приобретает особую значимость. При этом очевиден переход от подходов, сконцентрированных на рутинной поддержке существующих бизнес-процессов, к стратегическому развитию, созданию новых моделей ведения бизнеса и управленческой деятельности, обеспечивающих высокую эффективность инвестиций в данную сферу. Однако высокие темпы информатизации бизнеса и государственных органов неминуемо сопровождаются быстрым ростом рисков, обусловленных появлением новых угроз информационной безопасности, связанных как с действиями злоумышленников, так и со специфическими угрозами, вызванными непосредственно процессами информатизации. В связи с этим возникает потребность в разработке и развитии новых методов и моделей управления рисками информационной безопасности.

Методы обработки рисков информационной безопасности

Систематический подход к менеджменту рисков информационной безопасности необходим для того, чтобы идентифицировать потребности организации, касающиеся требований информационной безопасности, и создать эффективную систему менеджмента[1]. Этот подход должен соответствовать условиям деятельности организации и, в частности, должен быть согласован с общим менеджментом рисков в масштабе организации.

Процесс менеджмента риска информационной безопасности состоит из установления контекста, оценки риска, обработки риска, принятия риска, коммуникаций риска, а также мониторинга и переоценки риска информационной безопасности. В процессе менеджмента риска информационной

[1] ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

безопасности процедуры оценки риска и (или) его обработки могут выполняться итеративно, при этом если удается получить достаточную информацию для эффективного определения действий, требуемых для снижения риска до приемлемого уровня, то задача выполнена, после чего следует обработка риска (рис. 1).

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности. Дополнительные варианты повышения эффективности могут быть неэкономичными, и необходимо принимать решение о целесообразности их применения.

Согласно действующему ГОСТ Р ИСО/МЭК 27005-2010 существуют четыре варианта обработки риска:

- *снижение риска* – уровень риска должен быть снижен путем выбора меры и средства контроля и управления так, чтобы остаточный риск мог быть повторно оценен как допустимый;
- *сохранение риска* – решение сохранить риск, не предпринимая дальнейшего действия, следует принимать в зависимости от оценки риска;
- *предотвращение риска* – отказ от деятельности или условия, вызывающего конкретный риск;
- *перенос риска* – риск должен быть перенесен на сторону, которая может наиболее эффективно осуществлять менеджмент конкретного риска в зависимости от оценки риска.

В результате обработки должны быть выбраны меры и средства контроля и управления для снижения, сохранения, предотвращения или переноса рисков.

В современной литературе основное внимание уделяется организационно-техническому обеспечению информационной безопасности и, в частности, аппаратным и программным средствам защиты информации. Однако экономические методы обеспечения информационной безопасности не менее важны, чем технические. Значительно меньше работ посвящено вопросам, связанным с развитием экономических мер обеспечения информационной безопасности. Поиску величины оптимального объема инвестиций в меры обеспечения безопасности посвящены работы Л.А. Гордона и М.П. Лоуба [1, 2], В.К. Задираки [3], И.Б. Собакина [4], Е.Г. Левченко [5, 6] и И.М. Ажмухамедова [7]. Еще меньше работ посвящено методам киберстрахования. К сожалению, большинство изученных работ по данной тематике, например работы А.Н. Иващенко [8], С.А. Смирнова[2], Н.В. Косыгиной [9], Е.В. Небольсиной [10] посвящены рынку киберстрахования. Напрямую посвящены методике киберстрахования работы Дж. П. Кесана [11] и Н. Шетти [12], Р. Беме [13], Р. Пала [14], М. Элинга [15], а также Н.И. Артамонова [16].

В работах зарубежных авторов по киберстрахованию используются достаточно громоздкие модели нахождения стоимости страхового контракта, а в работах российских авторов указаны только действия по оценке надежности работающей системы риск-менеджмента без описания конкретных математических моделей, как, например, в работе Н.И. Артамонова [16], что и побудило нас к написанию этой статьи.

Согласно Доктрине информационной безопасности Российской Федерации[3] экономические методы ее обеспечения включают:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Рассмотрим подробнее способы реализации DDoS-атак и методы борьбы с ними.

DDoS-атаки и методы борьбы с ними

Ботнет – сеть компьютеров, которая состоит из некоторого количества хостов с запущенными ботами – программами, которые устанавливаются на компьютер жертвы без ее ведома и дают злоумышленнику возможность выполнять некие действия с использованием ресурсов зараженного компьютера. Подключение компьютера к ботнету происходит из-за заражения системы вирусом через уязвимость программного обеспечения, невнимательности пользователя (маскировка под

[2] *Смирнов С.А.* Страхование киберрисков в России: анализ состояния и перспективы развития // Сборник научных работ / под ред. Г.Д. Дроздова. СПб., 2015. С. 303–306.

[3] Доктрина информационной безопасности Российской Федерации: утв. Президентом Российской Федерации 09.09.2000 № Пр-1895.

«полезное содержимое»), использования санкционированного доступа к компьютеру.

Бот, обосновавшись в компьютере своей жертвы, связывается с хостом, управляемым злоумышленником, посылает ему запросы и выполняет ответные команды. Ботнет используется для рассылки спама, хищения личных данных пользователей или осуществления атак типа распределенный отказ в обслуживании (DdoS). Наиболее распространенной атакой злоумышленников на web-сервер является DDoS-атака (рис. 2).

В работе А.К. Гуца [17] описаны три способа, как добиться от сервера отказа в обслуживании.

Первый способ позволяет остановить работу всей атакуемой автоматизированной системы. Для этого злоумышленник посылает серверу-жертве данные или пакеты, которые она не ожидает, и это приводит либо к остановке системы, либо к ее перезагрузке. Атака «хороша» тем, что с помощью нескольких пакетов можно сделать систему неработоспособной.

Второй способ (Flood-атаки) состоит в том, чтобы добиться переполнения очереди на обработку запросов к системе с помощью такого большого количества пакетов, которые невозможно обработать. Например, если система может обработать только 10 пакетов в секунду, а злоумышленник отправляет ей 20 пакетов в секунду, то остальные пользователи при попытке подключиться к системе получают отказ в обслуживании, поскольку все ресурсы системы заняты. При таких атаках значительно снижается производительность компьютерной системы или web-приложений, и наблюдается резкое возрастание входящего трафика.

Третий способ атаки заключается в резком снижении пропускной способности (переполнении) канала связи.

Атака DDoS на онлайн-ресурс компании влечет убытки в среднем от 52 до 444 тыс. долл. в зависимости от размера компании. Такие данные получены в ходе исследования, проведенного «Лабораторией Касперского» и B2B International. К расходам по устранению последствий подобных атак добавляются репутационные потери и издержки, вызванные недоступностью публичного онлайн-ресурса для партнеров и клиентов[4].

Стоимость реализации DDoS-атаки намного ниже, чем ущерб, получаемый от нее, что зачастую побуждает недобросовестных конкурентов заказывать ее. Например, в работе [18] представлена функция Кобба–Дугласа, описывающая зависимость цены реализации атаки от ее длительности и величины пропускной полосы:

$$C = 0{,}964\ A^{0{,}5869}\ t^{0{,}5903},$$

где C – цена заказа DDoS, долл.;

A – мощность атаки, Мбит/с;

t – длительность атаки, ч.

Потребность в рассмотрении экономических мер обеспечения информационной безопасности также связана с несовершенством некоторых распространенных технических методов. Кратко рассмотрим их основные преимущества и недостатки.

На рынке немало компаний, предлагающих услуги по защите от DDoS-атак. Одни из них предлагают установку программно-аппаратных комплексов в ИТ-инфраструктуре клиента, другие используют возможности провайдера интернет-услуг, а третьи перенаправляют трафик клиента через специальные центры очистки. Однако основной принцип у всех один – фильтрация «мусорного», то есть сгенерированного злоумышленниками, трафика.

Наименее эффективным методом считается установка фильтрующего оборудования на стороне клиента. Во-первых, это требует наличия в защищаемой компании специально обученного персонала, который будет обслуживать и корректировать работу оборудования, что влечет дополнительные расходы. Во-вторых, такой метод эффективен только против атак непосредственно на ресурс и никак не сможет помешать атакам, «забивающим» интернет-канал клиента. Работающий ресурс бесполезен, если к нему нет доступа из сети, а перегрузить интернет-канал жертвы с помощью технологии усиления DDoS-атаки достаточно просто.

Фильтрация трафика провайдером более надежна благодаря наличию широкого интернет-канала, который гораздо сложнее вывести из строя. В то же время, поскольку провайдеры не специализируются на услугах по защите, они фильтруют только самый очевидный «мусорный» трафик, упуская из внимания более изощренные атаки. Для тщательного анализа атаки и

[4] DDoS-атака приводит к убыткам до 444 тыс. евро. URL: http://rus.db.lv/ekonomika/tehnologii/ddos-ataka-privodit-k-ubytkam-do-444-tys-evro-68108

оперативного принятия контрмер необходимы соответствующие знания и опыт. Кроме того, такой тип защиты привязывает клиента к конкретному провайдеру, создавая сложности в случае необходимости использования резервного канала связи или при смене провайдера.

Кластеризация или распределение ресурсов, аренда производительных каналов связи могут помочь, но по этому пути идут единицы, так как такой метод очень дорого обходится. Кроме того, чтобы одолеть созданные дополнительные мощности, злоумышленникам понадобится лишь увеличить масштабы атаки. А с точки зрения вложений злоумышленники потратят на 5–6 порядков меньше средств на увеличение мощности атаки по сравнению с расходами компании на подобную защиту.

Доказательство невыгодности инвестирования в данные методы обеспечения информационной безопасности можно провести с помощью модели Гордона – Лоуба, если известна количественная оценка действия приведенных ранее мер и средств контроля и управления[5].

На основании изложенного рассмотрим предлагаемые нами страховые механизмы противодействия DDoS-атакам.

Моделирование страхового контракта

Предположим, что участники страхового контракта (страхователь и страховщик) имеют различное отношение к риску: несклонность и риск-нейтральность соответственно. Тогда целевая функция страхователя заключается в максимизации его ожидаемой полезности от заключения страхового контракта:

$$Ef = (1 - p)U(H - r) + pU(H - r + h - Q) \to \max, \quad (1)$$

где p – вероятность наступления DDoS-атаки;

$U()$ – функция полезности страхователя;

H – величина капитала страхователя;

r – величина страхового взноса, равная произведению суммы нетто-ставки[6] и коммерческой надбавки ξ_0 на величину страхового возмещения $r = (p + \xi_0) h$;

h – величина страхового возмещения;

Q – величина убытков от последствий DdoS-атаки.

Основные «технические» трудности анализа механизмов страхования возникают из-за нелинейности функции полезности страхователя. В то же время именно эта нелинейность, отражающая несклонность к риску, делает страхование возможным и взаимовыгодным для страхователя и страховщика.

Поэтому для упрощения модели рассмотрим возможные способы учета несклонности к риску, не используя в явном виде функцию полезности. Для этого введем в его целевую функцию рисковую премию, отражающую ценность страхового возмещения, получаемого при наступлении страхового случая, как описано в работе В.Н. Буркова и др. [19].

Тогда ожидаемая полезность страхователя от заключения страхового контракта (1) с учетом сказанного ранее может быть выражена как

$$Ef = H - r + p\left(\Delta h(h) - Q\right) \to \max,$$

где $\Delta h(h)$ – «ценность» страхового возмещения.

Например, положим $\Delta h(h) = he^{\xi}$. Используя разложение экспоненты в ряд Маклорена

$$e^{\xi} = 1 + \frac{\xi}{1!} + \frac{\xi^2}{2!} + \ldots = 1 + \xi + o(\xi),$$

получаем, что для достаточно малых ξ

$$\Delta h \approx h(1 + \xi),$$

где $\xi \geq 0$ – константа, отражающая несклонность страхователя к риску (нейтральности к риску соответствует значение $\xi = 0$).

Ожидаемое значение целевой функции страховщика имеет следующий вид:

$$E\Phi = r - ph \to \max.$$

Таким образом, условие участия (individual rationality) для страхователя имеет вид

$$r \leq p(1 + \xi)h, \quad (2)$$

а для страховщика

$$r \geq ph, \quad (3)$$

Условие «морального риска», отображающее непобуждение страхователя к заинтересованности в страховом случае:

$$(1 + \xi)h \leq Q. \quad (4)$$

[5] *Борхаленко В.А.* Оценка эффективности оптимального инвестирования в систему менеджмента информационной безопасности // Финансовая аналитика: проблемы и решения. 2016. № 10. С. 15–21.

[6] Считается, что величина нетто-ставки равна вероятности наступления страхового случая p.

Выгодность страхования для страховщика оценивается величиной $E\Phi$, так как в отсутствие страхового контракта его полезность равна нулю. Выгодность страхования для страхователя может быть оценена разностью ΔEf между его полезностью в случае заключения страхового контракта и в случае его отсутствия:

$$\Delta Ef = p(1+\xi)h - r.$$

Сумма $\Delta = \Delta Ef + E\Phi$ может рассматриваться, как «мера» взаимовыгодности страхового контракта, тогда целевая функции примет следующий вид:

$$\Delta = \xi ph \to \max. \qquad (5)$$

Задача поиска значений параметров r и h, максимизирующих ожидаемую меру взаимовыгодности с учетом (2)–(5) сводится к задаче линейного программирования, в результате решения которой полученный страховой взнос можно трактовать как аннуитет ренты, выплачиваемой за временной период.

Рассмотрим пример. По данным исследования компании Positive Technologies[7], в 2013 г. DDoS-атаке подверглась практически каждая четвертая из опрошенных компаний (p = 0,23, средняя вероятность реализации[8]). Основываясь на приведенной ранее информации, предположим, что средний ущерб от целенаправленной DDoS-атаки равен 248 тыс. долл. (Q = 16,22168 млн руб.).

Предположим, что объектом атаки является автоматизированная система дистанционного банковского обслуживания. Тогда в соответствии с рекомендациями СТО БР ИББС-2.2-2009 величина потерь является критической (0,054%), исходя из того, что минимальный уставной капитал банка H не менее 300 млн руб.[9]. Также предположим, что ξ = 0,3.

Необходимо найти максимальное значение целевой функции $\Delta = 0,069h \to \max$ при системе ограничений

$$\begin{cases} 0,299h - r \geq 0 \\ r - 0,23h \geq 0 \\ 1,3h - 16,221680 \leq 0 \\ r, h \geq 0 \end{cases}.$$

Решение задачи синтеза страхового контракта средствами Excel представлено на рис. 3.

Решив данную задачу, получаем h = 12,478215 млн руб., r = 3,730986 млн руб. Учитывая, что страховой взнос состоит из нетто-ставки и коммерческой надбавки, величина коммерческой нагрузки равна 0,860997 млн руб. Таким образом, цена страхового контракта, устраивающего обоих участников, равна 3,730986 млн руб. в год, что, например, при номинальной процентной ставке 12,5% эквивалентно ренте пренумерандо с ежемесячными выплатами 0,328940 млн руб. при предположении, что вероятность реализации DDoS-атаки взята за год.

При заданных условиях страхование относится к более экономичным методам обработки рисков, связанных с реализацией DDoS-атак, чем методы, связанные с созданием резервных вычислительных мощностей и их сопровождением, а также другими упомянутыми методами защиты от DDoS.

Заключение

Таким образом, нами рассмотрены страховые методы обработки рисков информационной безопасности на примере рисков, связанных с реализацией DDoS-атак. Предложена математическая модель, описывающая оптимальные условия страхового контракта.

[7] Инциденты в информационной безопасности крупных российских компаний (2013 год). URL: https://www.ptsecurity.com/ru-ru/download/PT_Security_Incidents_2014_rus.pdf

[8] Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» СТО БР ИББС-2.2-2009: распоряжение Банка России от 11.11.2009 № Р-1190.

[9] О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1-ФЗ.

Рисунок 1

Процесс менеджмента риска информационной безопасности

Figure 1

Information security risk management process

Источник: ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

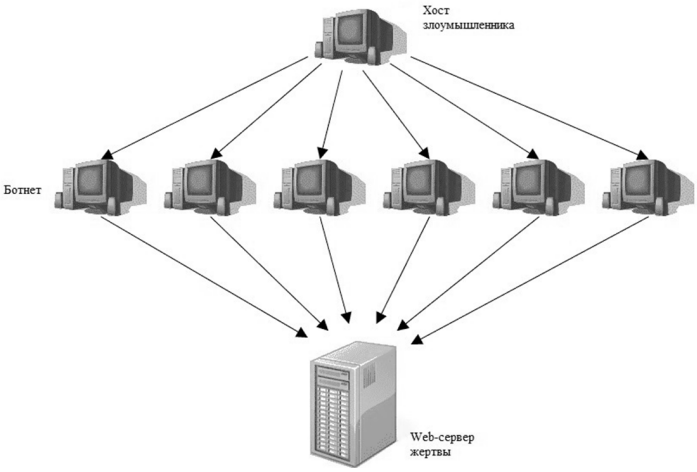
Source: GOST R ISO/IEC 27005-2010 Information Technology. Methods and Means of Ensuring Security. Information Security Risk Management

Рисунок 2

Реализация DDoS-атаки

Figure 2

Realization of a DDoS attack



Источник: авторская разработка

Source: Authoring

Рисунок 3

Решение задачи синтеза страхового контракта

Figure 3

A solution to the problem of synthesis of an insurance contract

Целевая функция			
h	*r*	*f*	
12,478215	3,730986	max	
0,069	0	0,860997	
Система ограничений			
0,299	–1	≥	0
–0,23	1	≥	0
1,3	0	≤	16,22168

Источник: авторская разработка

Source: Authoring

Список литературы

1. *Gordon L.A., Loeb M.P.* The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 2002, vol. 5, iss. 4, pp. 438–457.
2. *Gordon L.A., Loeb M.P., Lucyshyn W.* Information Security Expenditures and Real Options: A wait-and-see approach. *Computer Security Journal*, 2003, vol. 19, iss. 2, pp. 1–7.
3. *Задірака В.К., Олесюк О.С., Смоленюк Р.П., Штаблюк П.І.* Фінансування витрат на захист інформації в економічній діяльності. *Університетські наукові записи*, 2006, no. 3-4, pp. 479–490.
4. *Собакин И.Б.* Анализ подходов к определению оптимального объема инвестиций в информационную безопасность // Труды ИСА РАН. 2012. Т. 62. № 4. С. 63–68.
5. *Левченко Є.Г., Демчишин М.В., Рабчун А.О*. Математичні моделі економічного менеджменту інформаційної безпеки. *Системні дослідження та інформаційні технології*, 2011, no. 4, pp. 88–96.
6. *Левченко Є.Г., Воробовська Г.В.* Динамічне управління ресурсами захисту інформації. З*ахист Інформації*, 2011, no. 1, pp. 11–17.
7. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник АГТУ. Сер.: Экономика. 2011. № 1. С. 185–190.
8. *Иващенко А.Н., Шарко И.А.* Мировой рынок страхования кибер-рисков: перспективы и препятствия для развития в Республике Беларусь // Материалы IX Международной научно-практической конференции студентов «Национальная экономика Республики Беларусь: проблемы и перспективы развития». Минск: БГЭУ, 2016. С. 196–202.
9. *Косыгина Н.В., Анпилогова В.С.* Киберриски и их страхование в сфере банковского обслуживания // Материалы II Международной научно-практической конференции «Актуальные вопросы экономики и финансов в условиях современных вызовов российского и мирового хозяйства». Самара: Ас Гард, 2014. С. 203–204.
10. *Небольсина Е.В.* Киберриски – глобальная проблема современности // Страховое дело. 2016. № 1. С. 22–28.
11. *Kesan J.P., Majuca R.P., Yurcik W.J.* The Economic Case of Cyberinsurance. URL: http://law.bepress.com/cgi/viewcontent.cgi?article=1001&context=uiuclwps.
12. *Shetty N., Schwartz G., Felegyhazi M., Walrand J.* Competitive Cyber-Insurance and Internet Security. In: Workshop on Economics of Information Security (WEIS). University College London, 2009.

13. *Böhme R., Schwartz G.* Modeling Cyber-Insurance: Towards A Unifying Framework. URL: http://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf.

14. *Pal R., Golubchik L., Psounis K.* A Novel Cyber-Insurance Model. URL: http://www-bcf.usc.edu/~kpsounis/Papers/aegis.pdf.

15. *Biener C., Eling M., Wirfs J.H.* Insurability of Cyber Risk: An Empirical Analysis. *Working Papers on Risk Management and Insurance*, 2015, no. 151. URL: http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf.

16. *Артамонов Н.И.* Управление киберрисками в системе риск-менеджмента предприятий малого и среднего бизнеса // Страховое право. 2015. № 4. С. 53–57.

17. *Гуц А.К., Вахний Т.В.* Теория игр и защита компьютерных систем. Омск: ОмГУ, 2013. 160 с.

18. *Segura V., Lahuerta J.* Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study. URL: http://weis09.infosecon.net/files/113/paper113.pdf.

19. *Бурков В.Н., Заложнев А.Ю., Кулик О.С., Новиков Д.А.* Механизмы страхования в социально-экономических системах. М.: ИПУ РАН, 2001. 109 с.

Информация о конфликте интересов

Я, автор данной статьи, со всей ответственностью заявляю о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

ISSN 2311-8725 (Online)
ISSN 2073-039X (Print)

Mathematical Methods and Models

INSURANCE MECHANISMS IN INFORMATION SECURITY RISK MANAGEMENT

Vadim A. BORKHALENKO

OOO InfoProServis, Moscow, Russian Federation
vadikhide@yandex.ru

Article history:
Received 20 October 2016
Received in revised form
1 November 2016
Accepted 25 November 2016
Available online
27 February 2017

JEL classification: C02, C61, D81, G22

Keywords: cyberinsurance, contract theory, DDoS, information security, risk

Abstract

Subject The article addresses risks of information security.

Objectives The aim of the study is to consider the treatment of information security risks associated with implementation of DDoS-attacks and the lack of efficient technical means to reduce these risks.

Methods I employ methods of linear programming, the theory of utility and actuarial mathematics to develop a mathematical model of a mutually profitable insurance contract.

Results I consider the basic disadvantages of organizational and technical measures against DDoS-attacks realization and describe the prevalence and profitability of using this type of attacks by attackers and dishonest competitors to violate the business continuity of the organization. The paper explains the need for using economic methods to ensure information security, and offers an insurance model that provides for shifting the risk associated with realization of DDoS-attacks.

Conclusions and Relevance The proposed cyberinsurance method of DDoS-attacks resistance is more efficient as compared to many common hardware available, and can be applied to reduce possible financial losses from information attacks.

References

1. Gordon L.A., Loeb M.P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 2002, vol. 5, iss. 4, pp. 438–457.
2. Gordon L.A., Loeb M.P., Lucyshyn W. Information Security Expenditures and Real Options: A wait-and-see approach. *Computer Security Journal*, 2003, vol. 19, iss. 2, pp. 1–7.
3. Задірака В.К., Олесюк О.С., Смоленюк Р.П., Штаблюк П.І. Фінансування витрат на захист інформації в економічній діяльності. *Університетські наукові записи*, 2006, no. 3-4, pp. 479–490.
4. Sobakin I.B. [Analyzing the approaches to determination of optimal investment in information security]. *Trudy ISA RAN = Proceedings of Institute for Systems Analysis of RAS*, 2012, vol. 62, no. 3, pp. 63–68. (In Russ.)
5. Левченко Є.Г., Демчишин М.В., Рабчун А.О. Математичні моделі економічного менеджменту інформаційної безпеки. *Системні дослідження та інформаційні технології*, 2011, no. 4, pp. 88–96.
6. Левченко Є.Г., Воробовська Г.В. Динамічне управління ресурсами захисту інформації. *Захист Інформації*, 2011, no. 1, pp. 11–17.
7. Azhmukhamedov I.M., Khanzhina T.B. [Assessment of the cost-effectiveness of information security measures]. *Vestnik Astrakhanskogo GTU. Ser. Ekonomika = Vestnik of Astrakhan State Technical University. Series: Economics*, 2011, no. 1, pp. 185–190.
8. Ivashchenko A.N., Sharko I.A. [The world cyber risk insurance market: Opportunities and obstacles for development in the Republic of Belarus]. *Materialy IX Mezhdunarodnoi nauchno-prakticheskoi konferentsii studentov "Natsional'naya ekonomika Respubliki Belarus': problemy i perspektivy razvitiya"* [Proc. 9th Int. Sci. Conf. The National Economy of the Republic of Belarus: Problems and Development Prospects]. Minsk, BSEU Publ., 2016, pp. 196–202.
9. Kosygina N.V., Anpilogova V.S. [Cyber risks and their insurance in the sphere of banking services]. *Materialy II Mezhdunarodnoi nauchno-prakticheskoi konferentsii "Aktual'nye voprosy ekonomiki i finansov v usloviyakh sovremennykh vyzovov rossiiskogo i mirovogo khozyaistva"* [Proc. 2nd Int. Sci. Conf. Topical Issues of Economy and Finance under Contemporary Challenges of Russian and Global Economy]. Samara, As Gard Publ., 2014, pp. 203–204.

10. Nebol'sina E.V. [Cyber risks as a global problem of the modern world]. *Strakhovoe delo = Insurance Business*, 2016, no. 1, pp. 22–28. (In Russ.)

11. Kesan J.P., Majuca R.P., Yurcik W.J. The Economic Case of Cyberinsurance. Available at: http://law.bepress.com/cgi/viewcontent.cgi?article=1001&context=uiuclwps.

12. Shetty N., Schwartz G., Felegyhazi M., Walrand J. Competitive Cyber-Insurance and Internet Security. In: Workshop on Economics of Information Security (WEIS). University College London, 2009.

13. Böhme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. Available at: http://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf.

14. Pal R., Golubchik L., Psounis K. A Novel Cyber-Insurance Model. Available at: http://www-bcf.usc.edu/~kpsounis/Papers/aegis.pdf.

15. Biener C., Eling M., Wirfs J.H. Insurability of Cyber Risk: An Empirical Analysis. *Working Papers on Risk Management and Insurance*, 2015, no. 151. Available at: http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf.

16. Artamonov N.I. [Management of cyber risks in the risk management system for small and medium-sized businesses]. *Strakhovoe pravo = Insurance Law*, 2015, no. 4, pp. 53–57. (In Russ.)

17. Guts A.K., Vakhnii T.V. *Teoriya igr i zashchita komp'yuternykh sistem* [The games theory and computer systems protection]. Omsk, OmSU Publ., 2013, 160 p.

18. Segura V., Lahuerta J. Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study. Available at: http://weis09.infosecon.net/files/113/paper113.pdf.

19. Burkov V.N., Zalozhnev A.Yu., Kulik O.S., Novikov D.A. *Mekhanizmy strakhovaniya v sotsial'no-ekonomicheskikh sistemakh* [Insurance arrangements in socio-economic systems]. Moscow, Institute of Control Sciences of RAS Publ., 2001, 109 p.

Conflict-of-interest notification

I, the author of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.