УДК 001.6+004

И.А. ГРОМЫКО, канд. техн. наук

ВЛИЯНИЕ КАЧЕСТВА ИНТЕРНЕТ-УСЛУГ НА РИСКИ СОБСТВЕННИКА КОМПЬЮТЕРНОЙ СЕТИ

Введение

В современном мире развитие информационных технологий повлекло за собой не только новые возможности для развития интеллектуальных способностей человечества, но и появление новых видов угроз. В широком философско-социологическом и политологическом контексте эти угрозы были показаны Лиотаром, Бодрияйром и немецкими медиатеоретиками. Эрих Фромм, в свою очередь, еще в конце 70-х годов говорил о возможности возникновения информационного империализма. Философы предостерегают против диктатуры медиакратии превращения информация в средство интеллектуального давления и господства, манипулирования общественным сознанием [1].

В данной работе из всей цветовой гаммы информационного терроризма, как хакерского сознательного злоупотребления цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов [2], будет рассмотрена наиболее простая ситуация, связанная с ухудшением качества передачи сообщений в лини связи (например, в компьютерной сети).

Развитие аппаратурных и программных методов защиты информации еще не достигло такого уровня, когда можно со 100%-й вероятностью определить причину ухудшения качества передачи информации в той или иной компьютерной сети. Пользователя не интересует «по чьей причине отсутствует возможность передачи информации». Его интересует только факт наличия связи с абонентом. Связи, качество которой соответствует его требованиям, которые он оплатил. Если что-либо не соответствует договорным требованиям, то в развитых странах пользователю всегда предоставляется возможность разрыва контракта с поставщиком Интернет-услуг, который не обеспечил необходимое качество трансакций, осуществляемых по компьютерной сети.

В этой ситуации, независимо от характера информационных угроз (например, преднамеренного или непреднамеренного) результаты их реализации влекут за собой нанесение ущерба пользователю и, соответственно владельцу сети. Атаки правонарушителей, например хакеров, способны ухудшить работу аппаратуры линии связи и тогда поставщик Интернет-услуг теряет потенциальных пользователей (клиентуру), профессиональный имидж собственника и, как итог, – деньги, выплачивая штрафы и различные неустойки.

Финансовый эквивалент отношений между пользователями и поставщиками Интернет-услуг, как лакмусовая бумага, напрямую концентрирует внимание на качестве передачи информации, и говорит о способности поставщика услуг защищать информацию, циркулирующую в его компьютерной сети.

Требования государственных стандартов также опираются, на денежный эквивалент, заретушированный под «уровни затрат» на защиту информации [3, 4]. Объемы денежных эквивалентов в виде «минимального, допустимого и необходимого» уровней затрат на защиту информации изложены в государственных стандартах Украины – ДСТУ [3, 4].

Установлено, что возможны три варианта защиты информации:

- достижение необходимого уровня защиты информации с ограниченным доступом (ИСОД) при минимальных затратах и допустимом уровне ограничений видов информационной деятельности (ИД);
- достижение необходимого уровня защиты ИСОД при допустимых затратах и заданном уровне ограничений видов ИД;
- достижение максимального уровня защиты ИСОД при необходимых затратах и минимальном уровне ограничений видов ИД.

Как правило, ориентируясь на финансовое состояние собственника информации, первый и второй уровни относят к защите не государственной тайны, а третий уровень защиты (государственной тайны) принадлежит наиболее обеспеченному в финансовом отношении собственнику информации – государству.

Отсюда применяют либо фрагментарный, либо комплексный способы защиты информации. Необходимый уровень защиты информации обеспечивают ограниченным фрагментарным способом противодействия наиболее вероятной определенной угрозе информации.

Комплексная защита обеспечивает одновременное противодействие множеству угроз информации. Государственная тайна – секретная информация обеспечивается наиболее дорогостоящей – комплексной защитой.

Важно то, чтобы при защите информации стоимость защитных мероприятий не превышала стоимости самой информации [5].

Цель статьи – показ степени взаимосвязанности мероприятий, направленных на повышение качества передачи информации с расходами на эти мероприятия.

Основная часть

Будем считать, что информация, в условиях большого количества ее передач от одного носителя информации – источника к другому носителю – получателю, достаточно ординарна и меры по ее защите, предпринимаемые владельцем сети (ВС) – стандартные. В такой ситуации естественно использовать следующие предпосылки:

- стоимость передачи сообщений одинакова, причем она идет в доход ВС;
- в случае некачественной передачи информации ВС выплачивает штраф в размере стоимости сообщения;
- статистика работы сети по передаче сообщений вполне представительна, включая как трафик, так и общую стабильность процесса.

Конечно, актуален вопрос о рентабельности, как экономического показателя сети. Вместе с тем, здесь присутствует также и программно-техническая компонента, поскольку стоимость средств защиты информации (сообщений) и качество ее передачи взаимосвязаны.

В свете сказанного, воспользуемся решением задачи, которую Ричард Беллман [6, с. 307 – 309] рассмотрел, занимаясь вопросами передачи сообщений по каналам связи с привлечением положений теории игр.

Заметим, что постановка этой задачи Беллмана имеет множество предметных интерпретаций. Мы будем вести изложение, придерживаясь своей терминологии. Следует сразу обратить внимание на такие его особенности, как:

- высочайший конструктивизм в плане численной реализации;
- неочевидность результата с позиций соображений эвристического толка;
- замкнутый вид решения, редко встречающийся в задачах теории игр.

Решение базируется на знаменитом принципе оптимальности Беллмана: «Оптимальная политика обладает тем свойством, что каковы бы ни были начальное состояние и начальное решение, последующие решения должны составлять оптимальную политику относительно состояния, получающегося в результате применения первого решения» [6, с. 82]. Этот принцип трактуется в качестве свойства многошаговых процессов решения.

Пусть подсчитанная статистически вероятность качественной передачи сообщения – p, определяет вероятность финансовой потери $q = (1–p)$ для ВС (далее называем его – «игрок»).

В случае, когда игрок стремится максимизировать величину математического ожидания своего капитала после последовательной передачи N сообщений, ему нужно вкладывать в информационный бизнес все имеющиеся средства, если $p > 0{,}5$ и, вообще, приостанавливать деятельность, если $p < 0{,}5$.

Очевидно, такая стратегия таит в себе высокий риск, поскольку в условиях $0{,}5 < p < 1$ вероятность потерять все средства очень велика. Поэтому Беллман предлагает игроку более

осторожный план: максимизация математического ожидания от логарифма, той суммы, которую он будет иметь после передачи N сообщений.

В этом случае, что следует подчеркнуть, полностью исключается принятие любой стратегии, в которой капитал игрока может уменьшиться до нуля.

Если передается всего лишь одно сообщение, процедура определения стратегии приводит к нахождению максимума функции

$$E_1(y) = p\ log\ (x + y) + q\ log\ (x - y) \tag{1}$$

на множестве всех yϵ[0,x].

Когда $p \le q$, функция (1) достигает максимума в точке $y = (p - q)\ x$, принимая значение

$$E_1 = log\ x + log\ 2 + p\ log\ p + q\ log\ q; \tag{2}$$

когда же $p \le q$, $y_{\max} = 0$.

Таким образом, имеет место стратегия:

$$y = \begin{cases} (p - q)x,\ p > q \\ 0,\ p \le q \end{cases} \tag{3}$$

«Нетрудно видеть, что для многошагового процесса такая стратегия также оказывается оптимальной, если потребовать, чтобы на каждом шаге процентное отношение ставки к общей сумме, которой располагает игрок, было постоянным.

Мы же хотим показать, что эта стратегия, смысл которой заключается в том, что на каждом шаге нужно ставить фиксированную долю (p–q) наличного капитала, является оптимальной и в классе *любых* политик заключения пари» [6, с. 308].

Содержание выдержки, подразумевающей азартную игру, легко согласуется с терминологией нашего текста. Тем не менее, важный момент: что применительно к рассматриваемой ситуации означает «любая политика заключения пари»? Конечно, имеется в виду независимость от величины N.

В самом деле, с использованием метода динамического программирования, показана оптимальность стратегии (3), при которой математическое ожидание логарифма конечного капитала после N игр

$$f_{N+1}(x) = log\ x + (N+1)\ K, \tag{4}$$

где x – начальный капитал;

$$K = \begin{cases} \log 2 + p \log p + q \log q,\ p > q, \\ 0,\ p < q \end{cases}$$

О размерности величин в выражении (4), а также и предыдущих, (1), (2): поскольку x – капитал, естественно измеряемый в денежном эквиваленте – рубли (гривны, доллары); вероятности p и q – безразмерные.

Актуальна ли сама постановка вопроса о стратегии (3), когда пропажа сообщений, например писем, составляет ничтожный процент?

Иначе говоря, вероятность q, ничтожно мала, в отличие от азартной игры, на которую стратегия ориентирована.

По нашему мнению, она очень актуальна в силу следующих соображений:

- штрафы за наносимый ущерб могут существенно превосходить затраты на передачу информационных сообщений;

- по типу умножения q на коэффициент, отражающий моральный ущерб клиента, снижение рейтинга передающей фирмы и т. п.;

- легко представить солидные иски в ситуациях низкого качества передачи рейтинговых программ ТВ, искажения сообщений об аварийной опасности и т. п.;

- значительный процент различного рода неурядиц, включая вызовы скорой помощи, причисляют, как известно, к низкому качеству информационного обмена;

- статистика по информации высокой стоимости также может быть достаточно представительной, наряду с чем, штрафы здесь весьма значительны.

Следует также принять во внимание, что Р. Беллман не предполагает сообщения и штрафы однородными по стоимости. Главное, чтобы был статистический материал, то есть, p и q. Размеры проигрышей (штрафы) значения не имеют.

Мы использовали предпосылку об «однородности» лишь для большей прозрачности изначально поставленной задачи.

Преимущества от использования стратегии (3) в реальных ситуациях получает уже не «игрок», а владелец сети, в плане ее технико-экономического усовершенствования.

Главное из преимуществ состоит в том, что теперь он совсем иначе представляет свой бизнес в целом.

Действительно, если риск потери вложений – q, то на первый взгляд, казалось бы, следует сохранить для подстраховки фонд в размере $(q \cdot x)$, где напомним x – имеющиеся в наличие средства.

Однако, на самом деле, риск потери вложений согласно (3), и с учетом, что $(p+q)=1$, реально составляет

$$x - (p-q)\,x = 2q \cdot x,$$

то есть, вдвое больше и соответственно возникает «финансовая» необходимость повышения качества работы сети. В противном случае необходимо будет сокращать размеры деятельности.

Выводы

Таким образом, экономический стимул повышения качества используемой сети (линии связи) очевиден. Соответственно требуется расширение мероприятий организационной и программно-технической направленности защиты информации от атак правонарушителей, так как термин «качество сети» напрямую связан с интегральным показателем полезности сети для пользователей – финансовым эквивалентом.

Для дальнейших исследований интерес представляют обобщения постановки рассмотренной задачи [6, с. 310 – 317], с учетом того, что:

- характеристики такого носителя информации, как канал связи, изменяются с течением времени (влияние температуры и других факторов среды влияния);

- продолжительность процесса представляет собой стохастическую величину, которая зависит от принимаемых решений и результатов наблюдений и т.п.

Список литературы: 1. *Туронок, С.Г.* Современный терроризм: сущность, причины, модели и механизмы противодействия / С.Г. Туронок // Учеб.-метод. комплекс. – Ч.2. Разд.14. – М. : Изд-во МГУ им. М.В.Ломоносова. – 2008. – 780 с. – Режим доступа: http://lib2.znate.ru/docs/index-322035.html?page=2. 2. *Томас, Т.Л.* Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма : материалы междунар. конф. – М., 2002. 3. *Державний* стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. 4. *Державний* стандарт України ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. 5. *Гроздов Г.Г.* Модифицированный способ решения задачи нормирования эффективной комплексной системы защиты информации автоматизированной системы / Г. Г. Гроздов. – К. : ДУІКТ, 2009. – 32 с. 6. *Беллман, Р.* Процессы регулирования с адаптацией. – М. : Наука, 1964. – 360 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 07.02.2014