УДК 001.6+004

И.А. Громыко

Харьковский национальный университет имени В.Н. Каразина, Харьков

ИНФОРМАЦИЯ И ДЕЗИНФОРМАЦИЯ С ТОЧКИ ЗРЕНИЯ ИХ ЦЕННОСТИ

В статье рассмотрен вариант определения ценности информации в её финансовом эквиваленте. Такой подход позволяет перейти (при рассмотрении информационных процессов) от абстрактных рассуждений к реальной практике, которая опирается на теорию финансовой безопасности.

Ключевые слова: *ценность информации, информационная безопасность, финансовая безопасность.*

Введение

На сегодняшний день специалистами в области коммуникационных технологий разработано множество правил и алгоритмов защиты информации. В том числе, в сетях передачи данных. Такое многообразие вариантов построения информационных систем порождает необходимость создания также и систем защиты, учитывающих индивидуальные особенности каждого из вариантов. В то же время, значительный объем имеющихся публикаций, вряд ли, может сформировать чёткое представление о том, как же подойти к созданию системы защиты информации (СЗИ) для конкретной информационной системы, с учётом присущих ей особенностей и условий функционирования [1].

Защита информации должна обеспечиваться комплексом взаимосвязанных мероприятий: правовых, организационных, оперативных, технических, программных, криптографических, психологических и других. Степень влияния мероприятий той или иной группы на различные угрозы информации не является одинаковой. Она зависит от характера угрозы, характеристик среды, в которой эта угроза может осуществляться, личности нарушителя, деловых и моральных качеств сотрудников, которые участвуют в обслуживании компьютерной системы. Поэтому весьма интересной представляется оценка взаимного влияния интересов собственника информации, угроз этой информации и мер противодействия этим угрозам.

В специальной литературе, посвящённой вопросам защиты информации, рассмотрение угроз информации, как правило, ограничивается их определением и более-менее подробным описанием путей осуществления и мер противодействия. Поэтому качественная и, особенно, количественная оценка взаимного влияния указанных выше факторов является весьма важной в теоретическом и практическом плане – как способ оптимизации структуры СЗИ и более эффективного распределения средств, которые расходуются на мероприятия по защите информации [2, 3].

Кроме ответов на вопросы, от кого защищать информацию и как, необходимо ответить также и на вопрос: сколько требуется затратить средств и какова эффективность их отдачи? Следует отметить, что, если на первую часть вопроса можно найти ответы в единичных научных трудах, то общих подходов по поводу ответа на вторую часть вопроса не существует [1].

Исходные предпосылки

Если не концентрировать внимание на физической сущности мероприятий по защите информации и попытаться ответить на вопрос «о возможности существования такой ситуации, в которой информацию можно будет считать защищённой», то окажется, что такая ситуация в принципе возможна, если информацию защитить «от всех видов существующих угроз».

В процессе этого, в зависимости от выбранной классификации атак на информацию, можно выделить от двух и более таких угроз как:

- внутренняя и внешняя;
- нарушения конфиденциальности информации, её целостности или доступности к ней;
- три предыдущие угрозы, плюс угроза отсутствия возможности аудита системы безопасности (и др.);
- более двадцати видов угроз информации в банковских системах и т. д.

Количество и направленность угроз может оказаться настолько большим, что на борьбу с ними нужно будет потратить сумму средств (как первородного базиса в построении системы информационной защиты), нарушающую смысл в необходимости защиты информации.

Стоимость защиты не должна превышать стоимость информации, которую защищают [4].

Важно отметить, что объёмы денежных эквивалентов в виде «минимального, допустимого и необходимого» уровней затрат на защиту информации изложены в государственном стандарте Украины ДСТУ 3396.1-96.

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 определённой угрозе информации.

Комплексная защита обеспечивает одновременное противодействие множеству угроз информации [5, 6]. Государственная тайна – секретная информация обеспечивается наиболее дорогостоящей – комплексной защитой.

Здесь будет уместным рассмотрение ситуации, когда информация переводится в класс «секретной», иначе называемой - «государственная тайна».

Отнесение информации к государственной тайне включает в себя обязательную процедуру обоснования и определения возможного ущерба национальной безопасности государству в случае разглашения этой информации. А ущерб обычно измеряется в финансовом эквиваленте [7, ст.1].

Отсюда можно сказать, что секретная информация, как государственная тайна, относится к разряду самой ценной информации. Её ценность позволяет применить для защиты самые дорогостоящие методы и средства для обеспечения «необходимого, максимального уровня» информационной безопасности.

Цель статьи

Целью статьи является обоснование возможности применения положений теории и практики финансовой безопасности, для описания процессов при обеспечении информационной безопасности.

Основная часть. Ценность информации в ракурсе существующих воззрений

В теории связи ценность информации рассматривают в своеобразном ракурсе. Поэтому Р.Л. Стратонович высказался о ней следующим образом: «Понятие ценности информации … связывает шенноновскую теорию информации с теорией статистических решений. В последней теории основным является понятие средних потерь или риска, которое характеризует качество принимаемых решений. Ценность информации специализируется как та максимальная польза, которую данное количество информации способно принести в деле уменьшения средних потерь.

Такое определение ценности информации оказывается связанным с формулировкой и решением определённых условных вариационных задач» [8, с. 296].

И, тем не менее, «обычная», или же лучше сказать коммерческая сторона вопроса в данной трактовке представляется достаточно очевидной. В самом деле, как за полезностью, так и риском стоят вероятные потери, которые, как правило, могут оцениваться в денежном эквиваленте. Причём упомянутые показатели, естественно взаимосвязаны с качеством принимаемых решений.

Вполне логично считать, что к классу таких решений относятся и процедуры, направленные на предотвращение утечек, а также искажений информации. Иначе говоря, в общем случае, – на её защиту от обесценивания. Что же касается, теории статистических решений и вариационных задач, так это – математический аппарат, используемый для оценивания рисков.

С точки зрения синтеза определений собственно понятия информации в её обычном смысле и кибернетической трактовке, представляют интерес соображения авторов [9, с. 104-105]:

«Наиболее общее определение информации – это сведения об окружающем мире, получаемые в результате взаимодействия с ним. По другому определению под информацией понимается сообщение, устраняющее неопределённость в той области, к которой оно относится.

Академик В. М. Глушков даёт такое определение: информация – это мера неоднородности распределения материи и энергии в пространстве и во времени, показатель изменений, которыми сопровождаются все проистекающие в мире процессы».

Итак, просто получение сведений не гарантирует от потерь, вследствие их неадекватного понимания, или же недостоверности. Поэтому, «устранение неопределённости» будь то на эвристическом уровне, или же с помощью математических методов олицетворяет собой объективно сопровождающий получение информации процесс.

Определение В. М. Глушкова дано с позиций термодинамики (у неё с теорией информации, как известно, тесные взаимосвязи). Вместе с тем, здесь очевиден и прагматический аспект, поскольку от «меры неоднородности» непосредственно зависят размеры потенциальных потерь.

В связи с упоминанием прагматичности, приведём раскрывающую это понятие выдержку:

«Предметом [прагматической теории информации] является определение ценности информации для потребителя. Ценность информации – есть отношение субъекта, информации и цели, где информация выступает как объективный фактор или носитель ценности.

Ценность информации является важной характеристикой для кибернетических систем, так как она связана с их функционированием. Ценностный критерий информации является пригодным, когда сравниваются системы, выполняющие одну и ту же функцию, но имеющие внутреннее разнообразие» [9, с. 136].

Как представляется, характеристика прагматической теории прозрачна, едва ли требует комментариев и весьма актуальна в контексте темы настоящего исследования. В отношении кибернетических систем применимость ценностного критерия кажется излишне суженной. Здесь следовало бы сказать «является пригодным, в частности».

Однако не только сама информация, но и её оценка может трактоваться в ракурсе прагматичности, о чем свидетельствуют следующая выдержка:

«Принятая и понятая информация раньше или позже анализируется, потребляется в деятельности воспринявшего её индивида. … На этом этапе необходима прагматическая оценка информации – её ценности для осуществляемой индивидом деятельности, скажем для разработки плана. Соответственно ошибки такой оценки называют прагматическими.

Поскольку теория ценности информации пока разработана весьма слабо, нет и общепринятых подходов к анализу прагматических ошибок. На уровне здравого смысла представляется очевидным, что информация тем ценнее, чем больше приращение эффекта в деятельности использующего её индивида. Тем самым определяется характер и значение прагматической ошибки: индивид неверно оценивает полезность той или иной информации для решения конкретной задачи. По сути дела все подходы в прагматическом анализе информации сводятся к различным вариациям этого достаточно очевидного тезиса» [10, с. 70].

Что же, авторы данной работы вполне отчётливо выразили сформировавшиеся у них соображения. Конечно, они не отрицают возможность построения оценок информационной полезности с помощью различного рода методов, включая математический аппарат, однако хотели бы видеть системность подобного рода процедур.

Как представляется, именно в таком смысле подразумевается «слабость» существующей теории. Оценка прагматических ошибок видится им в качестве своеобразного раздела общей теории ценности. Однако обозначен весьма принципиальный вопрос.

Исчерпывающий, по нашему мнению, ответ на него, за которым видится выдвижение концепции глобального масштаба, дают Р. Беллман и С. Дрейфус:

«Основная проблема нашей цивилизации состоит в передаче информации от одного человека к другому или от одной машины к другой. Возможно, наиболее трудно преодолимой и ставящей в тупик частью этой проблемы является само определение того, что мы понимаем под информацией и как мы договоримся её измерять.

К счастью, в некоторых случаях имеется очень простой способ преодоления этой трудности. Вместо того чтобы пытаться изучать информацию как «улыбку чеширского кота», существовавшую от него отдельно, мы рассмотрим действительный физический процесс, в котором информация используется для выработки решений [11, с. 342].

Тогда, величина информации может быть измерена через эффективность решений.

Таким образом, полезность информации зависит от её применения – это наиболее разумная концепция.

Отношение к понятию «ценность информации» авторов [12], рассуждения которых ведутся с позиций системного анализа, можно охарактеризовать как противоречивые и, тем не менее, они весьма показательны в дискуссионном аспекте. Вначале отмечается:

«Информационная теория систем утверждает, что информация – физическая величина и в этом своём качестве она может быть использована для описания огромного числа процессов, протекающих в естественных или искусственных системах.

Наличие информации в системе может способствовать получению от системы тех или иных эффектов, могущих иметь то или иное значение. Однако выделять в самостоятельную категорию ценность информации – это то же самое, что говорить, например, о ценности (в отличие от калорийности) пищи, которая может по-разному восприниматься различными организмами.

Вообще одна из задач, решаемая в рамках информационной теории систем, состоит в том, чтобы очистить само понятие информации от того налёта субъективизма, которое оно вынесло из ранее развивавшихся теорий, в том числе и шенноновской» [12, с. 6-7].

В общем, здесь подразумевают, что понятие информации фундаментально (полная противоположность мнению авторов [11]), а главное, – единицы её измерения определяются типом конкретно рассматриваемого процесса. В связи с этим, ставить вопрос об информационной ценности считается некорректным.

Если сказать проще, авторы [12] против измерения информационной ценности в денежном экви-

валенте. Вместе с тем, далее, как нетрудно заметить, их позиция претерпевает изменение:

«Сформулируем важный принцип, который необходим практически в любой теории, исследующей ценность количества информации. Вряд ли может вызвать сомнение, следующее неформальное определение: ценностью информации называется величина, характеризующая максимальную пользу, которую можно извлечь из информации при наилучшем её использовании» [12, с. 67].

Однако полезность очень органично сопрягается с суммой прибыли, или же, напротив, убытка. Даже в том случае, когда достижением полезности является выход на некий показатель функционирования технической системы. В самом деле, как без единого эквивалента (денежных средств) определить какой из множества показателей является приоритетным?

В итоге авторы рассматриваемой работы делают вывод:

«Таким образом, понятие ценности количества информации связывает «чистую» теорию информации (вне зависимости от того, какими мерами количества информации мы пользуемся) с теорией принятия оптимальных решений, в которой основным является понятие средних потерь, «риски» [12, с. 69].

Почему бы, не трактовать ситуацию в разрезе использованных здесь понятий: риск – безразмерная величина, или же измеряется в процентах; потери имеют широкий спектр измерений (время, объем продукции, сумма денег). И вновь возникает тот же вопрос: почему не использовать единую единицу измерений, в качестве которой выступает финансовый эквивалент? По нашему мнению, доводы авторов [11], альтернативные [12], что уже отмечалось, представляются гораздо более логичными. В последнее время риски стали оценивать как потери в финансовом эквиваленте.

Тогда, если ценность информации имеет денежный эквивалент, то и дезинформация можно представить денежным эквивалентом, взятым с обратным знаком.

А. Ефимов говорит о том, что «… дезинформация, увеличивая исходную неопределённость, уменьшает вероятность достижения цели, причём её ценность является отрицательной» [13, с. 8]. При этом автор предполагает, что ценность информации измеряется приращением вероятности достижения цели (по А. А. Харкевичу).

Отмечается также возможность использования в качестве меры ценности некоторой функции от близости к цели – «суммы штрафов» (по Р. Л. Стратоновичу).

Представляет интерес выдержка:

«Проблема старения информации, для которой не нашлось места в теории Шеннона, постоянно давала о себе знать на практике, выдвигая с древнейших времён задачи оперативного управления войсками, флотом, а позднее – экономикой и торговлей. …

Шеннон в работе о системах секретной связи указывал, что быстро стареющие сообщения можно зашифровать более простым шифром, чтобы время возможной расшифровки его противником было сравнимо со «сроком жизни» сообщения» [13, с. 27].

Суть такова. Если, например, $x(t) = a \sin\omega t$, то информация о детерминированном процессе для наблюдателя, который имеет возможность производить экстраполяцию, не устаревает. Однако когда измеряемый процесс случаен во времени t, его экстраполяция становится принципиально невозможной.

Результат представляет суперпозицию точной функции $y(t)$ и ошибки вида εt, где ε – малая величина дезинформации, возрастающей с течением времени. Иначе говоря, достоверность восстановленной функции уменьшается, результат поступательно «наполняется» дезинформацией - устаревает [13, с. 28-29].

Далее речь идёт об особенностях передачи стареющей информации, что встречает существенные осложнения, вплоть до полной невозможности её идентифицировать [13, с. 37-45]. Здесь возникает ситуация, принципиально отличающаяся от традиционного для теории связи приёма сигналов с помехами [14, с. 163-165]. Естественно, дезинформационный процесс «искусственного старения» должен быть достаточно правдоподобен.

Исходя из этого, вполне очевидным представляется такой метод защиты информации от несанкционированного доступа путём её «искусственного старения»? Фактически ценность информации можно свести к нулю, внедрив в сообщение «элементы прогрессирующей дезинформации».

Важно отметить, что такой подход характерен для упреждающих систем защиты информации [15].

Зная возможности современных компьютеров можно определить величину интервала времени, необходимого для расшифровки того или иного нашего сообщения, полученного конкурентом незаконным путём. К концу этого интервала времени «изначально достоверное сообщение» будет представлять собой дезинформацию для конкурента.

Действительно, законный получатель информации быстро справится с «отключением» накапливающейся ошибки, тогда как в противном случае через какой-то промежуток времени информация придёт в негодность.

Однако такой приём, в первую очередь, касающийся электронных носителей, является также и элементом общего подхода, а именно – прогрессирующей (или динамической) дезинформации.

В самом деле, пусть потенциальный конкурент знает конечный результат, условно назовём, проек-

та, а также некоторые сведения о его промежуточных этапах (являющиеся достоверными), имея при этом два неидентичных варианта. Попытка несанкционированного получения третьего варианта проекта приведёт к наличию у правонарушителя трёх различных проектов.

На то, чтобы разобраться в них по существу, особенно если проект дорогостоящий (а значит, риск высок), понадобится достаточно много времени и информация устареет. Конечно, каждый дезинформационный вариант должен быть «качественным».

Выводы

На основании вышеизложенного сделаны следующие выводы:

- надёжная передача информации, а соответственно – недопущение несанкционированного доступа, искажений и т. п., представляет собой чрезвычайно важную проблему;
- базисом надёжной передачи информации может выступать не только и, даже, не столько, теория информации, представления о которой достаточно абстрактны, а коммерческая эффективность процесса передачи;
- более того, не только лишь для упомянутой теории, но и самого понятия информации её прагматическая ценность является первичным существенным базовым моментом;
- обратим внимание, это относится также и к понятию количества информации, которое на протяжении продолжительного периода времени привлекает внимание учёных;
- защищая информацию от негативных воздействий, мы фактически занимаемся экономией финансовых ресурсов, которая может быть весьма значительной;
- прогрессирующая (динамическая) дезинформация, снижающая со временем стоимость переданной (принятой) информации является одним из способов защиты информации, для развития которого потребуется отдельная теория и практика, базирующаяся на принципах работы систем с элементами искусственного интеллекта.

Список литературы

1. Гарасимчук О.І. Оцінка ефективності систем захисту інформації / О.І. Гарасимчук, Ю.М. Костів // Вісник КНУ ім. М. Остроградського. – Вип. 1/2011 (66). – Ч. 1. – Львів: Нац. ун-т "Львівська політехніка", 2011. – С. 16-20. – [Електронний ресурс]. – Режим доступу: http://www.kdu.edu.ua/statti/2011-1-1(66)/16.pdf [in Ukr.].

2. Horev A.A. Evaluating the effectiveness of information protection against leakage via technical channels // Special vehicle / A.A. Horev. – 2006. – №6. – P. 53-61.

3. Korolev V.I. Methods of assessing the quality of protection for information in its automated processing bath / V.I. Korolev, E.V. Morozova // Safety of information technology. – 1995. – № 2. – 215 p. [in Russian].

4. Грездов Г.Г. Модифицированный способ решения задачи нормирования эффективной комплексной системы защиты информации автоматизированной системы / Г.Г. Грездов // Монография. – К.: ДУІКТ, 2009. – 32 с.

5. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

6. Державний стандарт України ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

7. Закон України «Про державну таємницю» Відомості Верховної Ради України (ВВР), 1994, N 16, ст.93.

8. Стратонович Р.Л. Теория информации / Р.Л. Стратонович. – М.: Сов. радио, 1975.– 424 с.

9. Браславец М.Е. Кибернетика / М.Е. Браславец, Т.Ф. Гуревич. – К.: Вища школа, 1977. – 326 с.

10. Вилкас Э.Й. Решения: теория, информация, моделирование / Э.Й. Вилкас, Е.З. Майминас. – М.: Радио и связь, 1981.– 328 с.

11. Áåëëìàí Ð. Ïðèêëàäíûå çàäà÷è äèíàìè÷åñêîãî ïðîãðàììèðîâàíèÿ / Ð. Áåëëìàí, Ñ.. Äðåéôóñ. – Ì.: Íàóêà, 1965. – 458 ñ.

12. Øèëäåéò À.Â. Ââåäåíèå â èíòåðíàöèîíàëüíóþ òåõíèêó ñèñòåì / À.Â. Øèëäåéò, Â.Ô. Êî÷íåâ, Ô.Ô. Õèíóøèí. – Ì.: Ðàäèî è ñâÿçü, 1985. – 279 ñ.

13. Ефимов А.Н. Информация: ценность, старение, рассеяние / А.Н. Ефимов. – М.: Знание, 1978. – 64 с.

14. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования. – К.: Вища школа, 1986. – 239 с.

15. Громыко И.А. Будущее за упреждающими системами защиты / И.А. Громыко, С.Ю. Кильмаев, Е.Я. Оспищев // Защита информации. INSIDE. – 2007. – №2 (14) – 2007. – С. 14-18.

Поступила в редколлегию 11.12.2013

Рецензент: д-р техн. наук, проф. С.Г. Рассомахин, Харьковский национальный университет им. В.Н. Каразіна, Харьков.

ІНФОРМАЦІЯ ТА ДЕЗІНФОРМАЦІЯ З ТОЧКИ ЗОРУ ЇХ ЦІННОСТІ

І.О. Громико

У статті розглянуто варіант оцінки цінності інформації в її фінансовому еквіваленті. Такий підхід дозволяє перейти (при розгляді інформаційних процесів) від абстрактних міркувань до реальної практики, яка спирається на теорію фінансової безпеки.

Ключові слова: *цінність інформації, інформаційна безпека, фінансова безпека.*

INFORMATION AND DISINFORMATION TERMS OF THEIR VALUE

I.O. Gromyko

In this article the value of information is considered in its financial equivalent. This approach allows us to pass (when considering the information processes) from abstract reasoning to actual practice, which is based on the theory of financial security.

Keywords: *value of information, information security, financial security.*