https://doi.org/10.36719/2789-6919/42/71-76

Замира Ибрагимли
Азербайджанский Университет Нефти и Промышленности
магистрант
https://orcid.org/0009-0009-1136-2094
zamiraibragimova61@gmail.com

Некоторые проблемы информационной безопасности

Резюме

В статье отмечается, что в условиях рыночных отношений товар начинает носить всеобщий характер. По этой причине информация также превращается в объект купли и продажи.

Далее особое внимание отводится раскрытию параметров качества информации, которые должны соответствовать требованиям непосредственных их покупателей и потребителей.

В условиях формирования в станах мира цифровой экономики предлагается принять меры по укреплению законов и порядков, а также воспитанию населения в духе культуры, соответствующему информационному обществу.

В целях эффективного обеспечения информационной безопасности рекомендуется применять алгоритм сквозного и традиционного систем управления информационными потоками.

Безусловно, имеются доступные, фатальные и количественные вызовы и угрозы, вызванные обеспечением информационной безопасности. Однако на практике некоей формулой, используя приведенные параметры безопасности, рассчитывать степень рисковых ситуаций не представляется достаточным. Поэтому рекомендуется применять иную оценку уровня качества информации и, соответственно, информационной безопасности на основе метода «Дельфа». При этом предлагается к исследованиям по данному методу привлекать независимых анонимных специалистов, а также непосредственных покупателей и пользователей информационной продукции.

Ключевые слова: *информация, информационная безопасность, криптография, алгоритм, цифровая экономика, информационные потоки*

Zamirə İbrahimli
Azərbaycan Neft və Sənaye Universiteti
magistrant
https://orcid.org/0009-0009-1136-2094
zamiraibragimova61@gmail.com

İnformasiya təhlükəsizliyinin bəzi problemləri

Xülasə

Məqalədə qeyd olunur ki, bazar münasibətləri şəraitində əmtəələr universal xarakter almağa başlayır. Bu səbəbdən informasiyalar da alqı-satqı obyektinə çevrilir.

Bundan informasiyaların birbaşa alıcılarının və istehlakçılarının tələblərinə cavab verməli olan məlumatların keyfiyyət parametrlərinin açıqlanmasına xüsusi diqqət yetirilir.

Dünyada rəqəmsal iqtisadiyyatın formalaşması kontekstində qanun və sərəncamların gücləndirilməsi, o cümlədən əhalinin informasiya cəmiyyətinə uyğun mədəniyyət ruhunda maarifləndirilməsi istiqamətində tədbirlərin görülməsi təklif edilir.

İnformasiya təhlükəsizliyini səmərəli şəkildə təmin etmək üçün birbaşa və ənənəvi informasiya axınlarının idarəetmə sistemlərinin alqoritmindən istifadə edilməsi tövsiyə olunur.

Əlbəttə, informasiya təhlükəsizliyinin yaratdığı əlçatan, ağır nəticəli və kəmiyyət çağırışları və təhdidləri var. Bununla belə, təcrübədə qeyd edilən təhlükəsizlik parametrlərindən və müəyyən düsturdan istifadə etməklə riskli vəziyyətlərin dərəcəsini hesablamaq kifayət etmir.

Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

Buna görə də "Delfi" metodu əsasında informasiyanın keyfiyyət səviyyəsinin və müvafiq olaraq informasiya təhlükəsizliyinin fərqli qiymətləndirilməsindən istifadə etmək tövsiyə olunur. Eyni zamanda, bu metoddan istifadə etməklə tədqiqata müstəqil anonim mütəxəssislərin, eləcə də informasiya məhsullarının birbaşa alıcıları və istifadəçilərinin cəlb edilməsi təklif olunur.

Açar sözlər: *informasiya, informasiya təhlükəsizliyi, kriptoqrafiya, alqoritm, rəqəmsal iqtisadiyyat, informasiya axınları*

Zamira Ibrahimli
Azerbaijan University of Oil and Industry
master's student
https://orcid.org/0009-0009-1136-2094
zamiraibragimova61@gmail.com

Some Problems of Information Security

Abstract

The article notes that in conditions of market relations, goods begin to be universal. For this reason, information also turns into an object of purchase and sale.

Further, special attention is given to the disclosure of information quality parameters, which must meet the requirements of their direct buyers and consumers.

In the context of the formation of a digital economy in the world, it is proposed to take measures to strengthen laws and orders, as well as educate the population in the spirit of culture, corresponding to the information society.

In order to effectively ensure information security, it is recommended to use the algorithm of end-to-end and traditional information flow management systems.

Of course, there are accessible, fatal and quantitative challenges and threats caused by information security. However, in practice, it does not seem sufficient to calculate the degree of risk situations using a certain formula using the given safety parameters.

Therefore, it is recommended to use a different assessment of the level of information quality and, accordingly, information security based on the Delphi method. At the same time, it is proposed to involve independent anonymous specialists, as well as direct buyers and users of information products, in research using this method.

Keywords: *information, information security, cryptography, algorithm, digital economy, information flows*

Введение

В условиях капиталистической системы хозяйствования, т.е. рыночных отношений, товар начинает носить всеобщий характер. С точки зрения известного маркетолога Ф.Котлера и других специалистов в области экономики, товаром становится любая вещь, в том числе услуга, идея или информация, которая может быть востребована со стороны определенного лица в виде конкретного индивида, группы лиц, предприятия, организации или государства за определенное вознаграждение, а также плату (Котлер, Филип, 2012, с.175). Это говорит о том, что создатель товара, конкретнее информации преследует определенную цель, а именно соответствующую выгоду в виде прибыли или достижения чего-то другого. Исходя из приведенных и других соображений информационная безопасность - это не просто «...совокупность защиты информации от случайного или преднамеренного воздействия», а ожидания безвозмездно получателей и покупателей информации, связанные с научной достоверностью, объективностью, полнотой отображения в ней (информации) тех или других объектов, явлений и процессов. Вот почему создатель и продавец информации как особого товара должен заботиться о ее качестве (рис. 1) (5).

Исследование

При этом, качественной считается такая информация, которая на основе проведенного анализа позволяет заблаговременно предвосхитить наступление каких-либо явлений и процессов, например инфляций, землетрясений, войн и т.д.

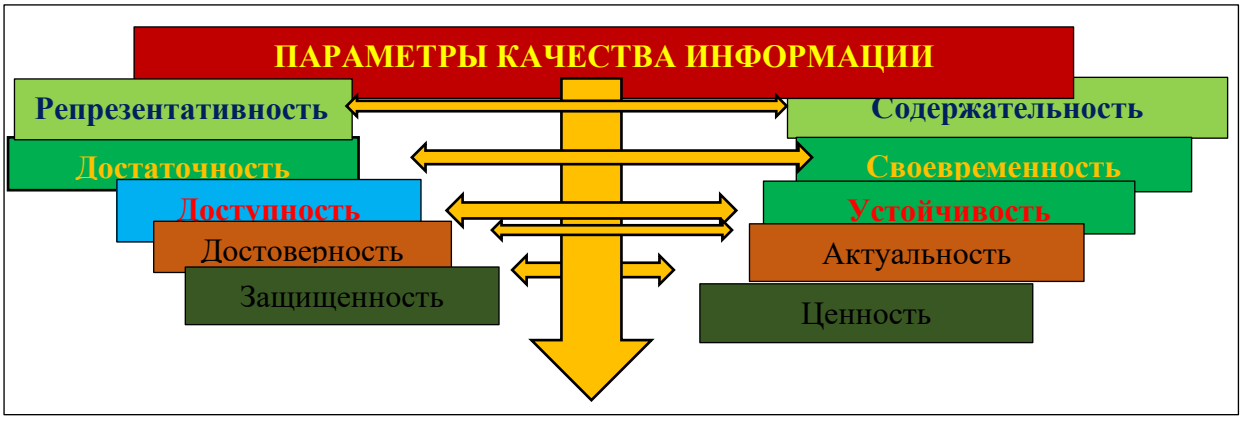

Рисунок 1. Параметры или компоненты качества информации

Из отмеченного следует, что сегодня в понятие информационной безопасности необходимо включать не только факторы ограждения информации от того или другого стороннего воздействия, но также проблемы защиты государственных и общественных устоев, общечеловеческой морали и этики, культуры и национальной идентичности народов мира от вредоносной, совращающей и экстремистской информации (рис.2).

Обратимся к рисунку 2, откуда видно, что информацию осознанно могут создавать и предлагать любые субъекты, начиная с государственных, производственно- коммерческих структур и прочих структур, кончая соответствующими заказчиками с использованием искусственного интеллекта и других источников. Причем, на каждом из приведенных этапов системы доведения информации до конечных пользователей должны или же могут быть использованы те или другие средства и методы сквозного и поэтапного обеспечения информационной безопасности, в том числе криптографирование.

Рисунок 2.Алгоритм прогрессивной системы глобальной информационной безопасности (*авторская разработка*)

Первая, т.е. сквозная система предполагает заблаговременное продумывание и согласование всех нюансов и проблем обеспечения информационной безопасности между всеми участниками воспроизводственного процесса данной продукции. Вторая же, т.е. практика обеспечения безопасности в данной деятельности возлагается на каждый субъект информационного общества в отдельности. В нынешних условиях развития и становления информационного общества стоит проблема обеспечения законодательной защиты многообразных интересов как производителей и посреднических структур (субъектов), занимающихся распределением, выведением и реализацией информационной продукции на рынке, также непосредственных покупателей и потребителей подобных товаров (Груздева, 2017, с. 53-61).

Упомянутое выше криптографирование, как особая форма оформления и передачи ограниченному кругу лиц скрываемой информации, известна человечеству давно. Криптографирование осуществляется на основе видоизменения той или другой информации с помощью определенных хитроумных правил и алгоритмов с применением специальных ключей для зашифровки и последующей расшифровки (6).

Исследования многих ученых-экономистов мира продолжают подтверждать факты изменчивого, но последовательного стремления мировой экономики к глобализации. В частности, это проявляется: 1) в повышении доли развитых государств мира, а также транснациональных и других компаний в объеме потребления товаров и услуг в менее развитых и отсталых странах мира; 2) в формировании глобальной системы логистики различных видов транспорта; 3) в развитии и стремительном распространении ИКТ во всех континентах, регионах, странах мира и др.

Сегодня многие прогрессивно мыслящие люди различных поколений ясно осмысливают, что развитие и распространение ИКТ и ее программное обеспечение, формирующим искусственный интеллект все более усиливают процессы глобализации в мире, а также, с одной стороны, приносят прогресс, а с другой вызывают новые вызовы и угрозы для всего человечества (Вострецова, 2019).

Безусловно, существуют пределы вызовов и угроз, связанных с информационной безопасностью, которые в одном статье автор делит на три критерия: ***доступность*** **($К_д$),** ***фатальность*** **($К_ф$)** и ***количество*** **($К_к$).** При этом, каждый из предложенных показателей информационной безопасности в виде «...опасности возникновения угрозы и вероятности поломки или обхода защиты информации...» предлагается рассчитать, как среднеарифметическое коэффициентов отдельных уязвимостей (7). Причем, в данной статье считается, что максимальная совокупная уязвимость оценивается показателем 125. Исходя из приведенного, степень информационной опасности (**$К_{(О)}$**) предлагают рассчитывать по формуле:

$$К_{(О)} = (К_д \times К_ф \times К_к) / 125$$

Исходя из приведенных соображений, а также для повышения степени относительной объективности в исследовании степени той или другой информационной безопасности предлагаем использовать не столь распространенный метод «Дельфи», разработанный в США в середине прошлого века (8). Этот метод предусматривает привлечение к исследованиям независимых анонимных экспертов из числа соответствующих специалистов или потребителей тех или других товаров и услуг.

В целях наглядности и научного обоснования степени качества информационной безопасности рекомендуем разработать определенную таблицу, как приведено ниже.

Таблица.

Экспертная оценка уровня качества предлагаемой на рынке информации*

Оценки экспертов по 10-тибалльной системе

№ п/п	Показатели качества информации	1	2	3	4	5	6	7	8	9	10	Средний балл
1	*Репрезентативность*	*3*	*3*	*8*	*7*	*8*	*3*	*9*	*1*	*5*	...	*5,5*
2	*Доступность*	*5*	*1*	*9*	*2*	*3*	*6*	*3*	*7*	*7*	...	5,0
3	*Достаточность*	*8*	*6*	*7*	*5*	*5*	*1*	*4*	*7*	*2*	...	5,3
4	*Достоверность*	*7*	*3*	*4*	*4*	*8*	*7*	*2*	*4*	*8*	...	5,3
5	*Содержательность*	*9*	*3*	*2*	*3*	*4*	*8*	*3*	*3*	*7*	...	5,0
6	*Своевременность*	*4*	*8*	*4*	*3*	*3*	*7*	*3*	*8*	*5*	...	5,4
7	*Защищенность*	*7*	*2*	*9*	*6*	*3*	*9*	*8*	*10*	*8*	...	7,1
8	*Устойчивость*	*1*	*6*	*3*	*8*	*6*	*9*	*2*	*6*	*8*	...	5,2
9	*Актуальность*	*4*	*8*	*6*	*2*	*1*	*5*	*9*	*3*	*2*	...	4,7
10	*Ценность*	...	...	...	...	...	...	...	...	...	...	5,2
	Средние баллы экспертов	*5,3*	*4,5*	*5,2*	*4,9*	*4,7*	*6,5*	*4,6*	*5,4*	*5,6*	*7,0*	53,7

Показатели экспертных оценок условны.

Далее на эту таблицу наносятся экспертные оценки параметров качества информации, поступающей от создателей, возможно различных каналов их распространения и реализации.

В условиях рыночных отношений производители информации должны учитывать покупательские приоритеты их продукции. Поэтому в качестве экспертов оценки качества информации также могут выступать их покупатели и потребители, а в части показателей качества могут ставиться приоритеты заказчиков данной информации.

Заключение

В условиях капиталистической системы хозяйствования информация, как и обычная вещь становится объектом купли и продажи. Поэтому, производители информации, а также физические и юридические лица, занимающиеся выведением данной продукции на мировые и другие рынки, должны нести ответственность не только за их количественную и качественную сохранность, но также ограждать потребителей от тех или других вызовов и угроз, обеспечивая информационную безопасность в обществе в целом.

Каждая информация имеет как коммуникативную, так и экономическую эффективность. Первая из этих информационных эффектов может определяться на основе выяснения того, насколько опрашиваемые помнят о той или другой информации. Экономический же эффект устанавливается тем, на сколько полученная информация смогла повысить продажи или увеличить отдачу от вложений и т.д.

Информационная безопасность – это не просто защита информации от каких-либо случайностей или сторонних негативных действий, а системное обеспечение защиты создателей, каналов легального распространения и пользователей информации от злонамеренных атак, а также прямых вызовов и угроз.

В целях всестороннего обеспечения информационной безопасности рекомендуем пользоваться сквозной и обычной, т.е. структизированной системой управления информационными потоками.

Информационная безопасность напрямую зависит от качества создаваемых информаций, используемых при этом технических средств, а также выбранных вариантов коммуникаций - общего пользования Интернета, внутрикорпоративного Интернета и межсетевого Экстернета.

В настоящее время нет абсолютно лучшей общепризнанной практики расчета степени информационной опасности. Поэтому предлагаем данный показатель определять используя метод «Дельфи», как это приводится в данной статье.

Литература

1. Вострецова, Е.В. (2019). *Основы информационной безопасности*. Учебное пособие для студентов вузов. Изд-во Урал. ун-та. https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
2. Груздева, Л.М. (2017). *Основы информационной безопасности*. Учеб. пособие в двух частях. Ч. 1. Юридический институт МИИТа.
3. Котлер, Ф. (2012). *Основы маркетинга*. *Краткий курс*. «ООО «И. Д. Вильямс».
4. Родкина, Т.А. (2001). *Информационная логистика*. «Экзамен».
5.https://prezi.com/p/vyn13cuazox9/presentation/#:~:text=Возможность%20и%20эффективность%20использования%20информации,%2C%20актуальность%2C%20защищенность%20и%20ценность.
6.https://web.flow.opera.com/ext/v1/index21c8bdcfe5fd72f585dc62c8d79b752805c79ba8b55588fbecce8ec6333a0915.html
7.https://web.flow.opera.com/ext/v1/index-21c8bdcfe5fd72f585dc62c8d79b752805c79ba8b55588fbecce8ec6333a0915.html
8. https://ru.wikipedia.org/wiki/Метод_«Дельфи»

Поступило: 17.11.2024
Принято: 19.02.2025