УДК 004.056

Р.Муратхан, Д.Ж.Сатыбалдина

Евразийский национальный университет им. Л.Н.Гумилева, Астана
(E-mail:muratkhan_r@enu.kz)

Количественный метод оценки рисков информационной безопасности многокомпонентными угрозами

В статье предложен комбинированный поход к оценке рисков наступления события информационной безопасности на основе онтологического описания предметной области и количественного метода оценивания риска реализации многокомпонентных угроз, использующих более одной уязвимости.

Ключевые слова: риск, информационная безопасность, метод оценки рисков.

Введение

Организации, бизнес которых во многом зависит от информационной сферы, для достижения целей бизнеса должны поддерживать на необходимом уровне систему управления информационной безопасностью (СУИБ) [1]. Многие компании сегодня приходят к тому, что СУИБ должна строиться, исходя из общепринятых норм и с учетом наработанных мировых практик, в том числе международных стандартов [2–4]. В Своде правил по управлению защитой информации [2] для формирования комплексных требований к безопасности информации выделены три основных показателя:

- оценивание рисков, с которыми сталкивается организация (через определение угрозы для активов, уязвимостей активов и вероятности возникновения угроз, а также возможных ущербов);
- соблюдение законодательных, нормативных и договорных требований, которые должны выполняться самой организацией, ее партнерами по бизнесу, подрядчиками и поставщиками услуг;
- формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

Стандарты [3, 4] определяют систему управления информационными рисками как ключевой элемент СУИБ и, используя процессную модель, описывают итерационный подход к проведению оценки рисков. Однако стандарты не содержат рекомендаций по выбору какого-либо аппарата оценки риска, а также по синтезу мер, средств и сервисов безопасности, используемых для минимизации рисков, что снижает полезность стандартов как технологических документов. В связи с этим являются актуальными работы по развитию риск-ориентированных моделей безопасных бизнес-процессов, методов и алгоритмов качественной и количественной оценки рисков информационной безопасности (ИБ) и разработке на их основе программного инструментария.

Математический аппарат оценивания рисков ИБ опирается на методы теории вероятностей, что обусловлено вероятностным характером неопределенности риск-образующих факторов. Формула расчета рисков чаще всего представляет собой произведение трех параметров:

$$R = V \cdot P(T) \cdot AV, \tag{1}$$

где V — мера уязвимости актива к угрозе; AV — ценность актива; $P(T)$ — вероятность реализации угрозы.

Недостатком данного подхода является то, что не учитываются ситуации, когда на один актив действует несколько угроз или одна угроза использует несколько уязвимостей.

В настоящей работе предлагается метод количественной оценки рисков реализации угроз по конфиденциальности, целостности и доступности активов на основе расчета уровней нескольких угроз, использующих несколько конкретных уязвимостей. В работе также используется онтология предметной области управления рисками безопасности информационных систем, которая помогает определить уязвимые активы, цели безопасности, оценивать риски и выявить меры безопасности для смягчения этих рисков.

Онтология предметной области управления рисками

Онтология определяет общий словарь для ученых, которым нужно совместно использовать информацию в предметной области, она включает машинно-интерпретируемые формулировки основных понятий предметной области и отношения между ними [5]. Понятием может быть описание зада-

чи, функция, действие, стратегия и т.п. Отношения между классами и подклассами понятий организуются в виде ориентированного графа, вершины которого соответствуют понятиям предметной области, а дуги (рёбра) задают отношения между ними. Классы и экземпляры имеют свойства (атрибуты).

В настоящей работе используется онтология предметной области управления рисками безопасности информационных систем ISSRM (Information Systems Security Risk Management — Управление рисками безопасности информационных систем), предложенная авторами работы [6].

Онтологическая модель ISSRM (см. рис. 1) описывает три различные концептуальные категории.

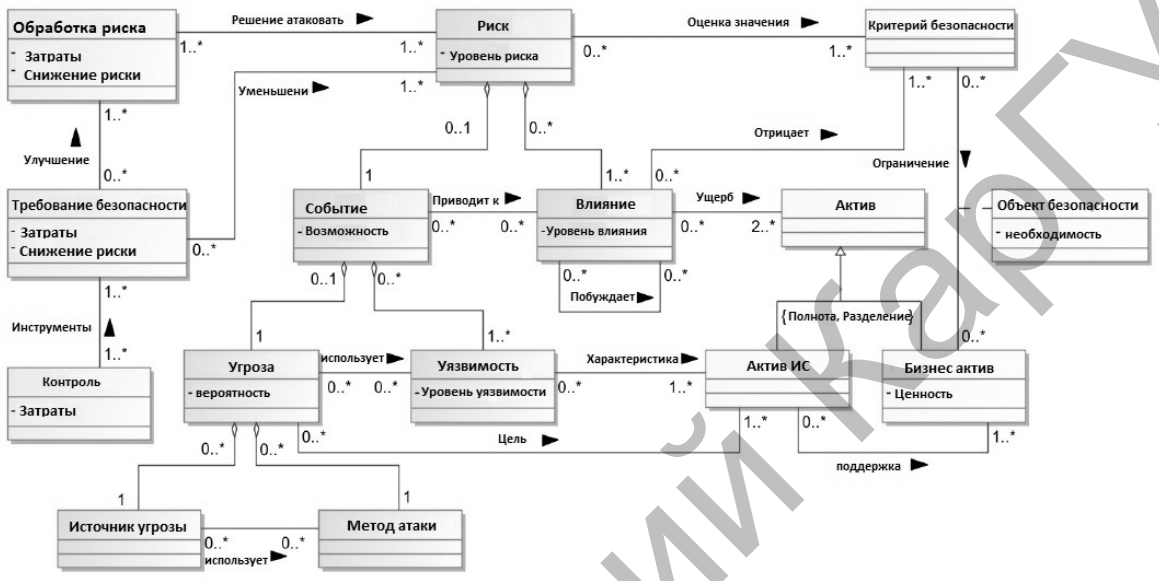

Рисунок 1. Модель ISSRM [Mayer and Dubois et al.]

Понятия, связанные активом, описывают активы организации, подразделяются на бизнес-активы и активы информационных систем (ИС). Они также определяют критерий безопасности, как ограничения бизнес-активов, выраженные как целостность, конфиденциальность и доступность.

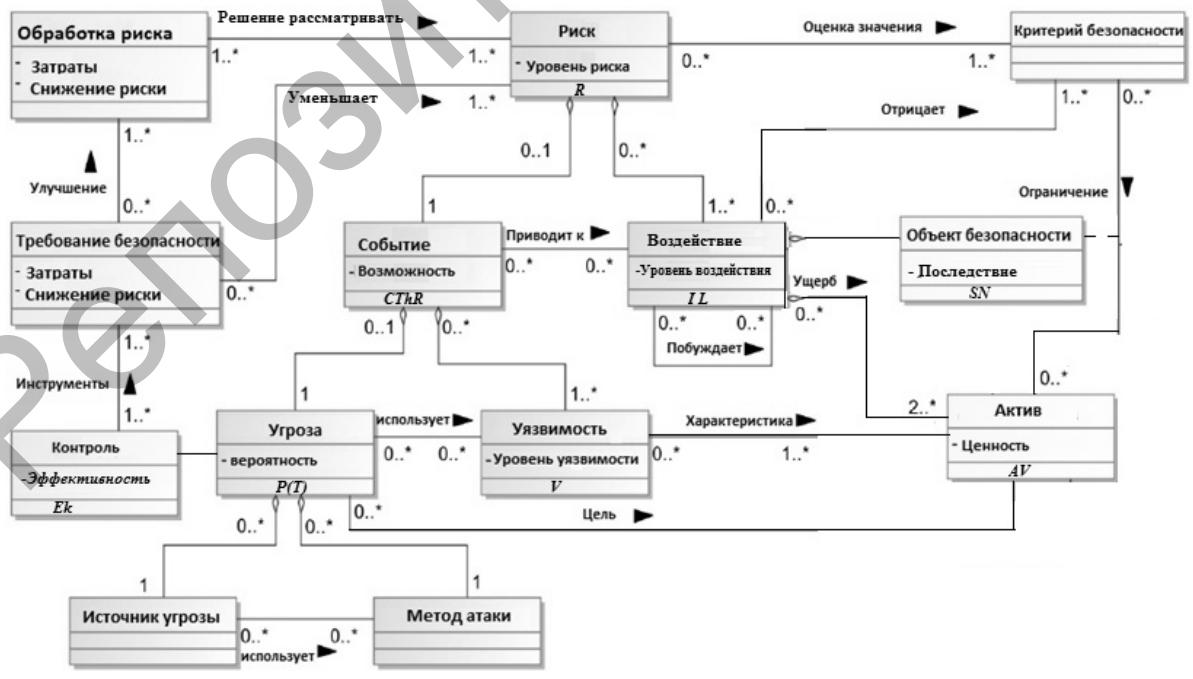

Рисунок 2. Модифицированная модель ISSRM

Понятия, связанные с риском, определяют потенциальный вред для бизнеса. В их состав входят угрозы, которые содержат одну или несколько уязвимостей. В случае их успешного выполнения наносится вред активам системы, оказывается негативное воздействие на активы, определенное в качестве влияния.

Событие — это объединение угрозы и уязвимости, где уязвимость — слабое место системы, которое может быть использовано источником угрозы. Угроза — это способ нанесения атаки. Источник угрозы — это злоумышленник, который инициирует угрозу нанесения вреда активам ИС. Метод атаки является средством, через которое источник осуществляет угрозу.

Понятия, связанные с обработкой рисков, определяют решение обработки рисков, чтобы избежать, уменьшить, сохранить или передать потенциальные риски. Они уточняются требованиями безопасности. Контроль реализуют требования безопасности.

В модифицированной модели ISSRM в каждом понятии написаны на первой строчке название понятий, на второй — мера и на третьей — обозначение расчетных формул.

Предлагаемый метод оценки риска

В основу метода положена модель угроз, используемая в программном продукте «ГРИФ-2006» компании Digital Security [6].

В соответствии с онтологией предметной области (см. рис. 2) уязвимость оценивается мерой уязвимости актива к угрозе, а угроза – вероятностью реализации угрозы через данную уязвимость. Значения меры уязвимости актива к угрозе и вероятности реализации угрозы через данную уязвимость оцениваются экспертом и указываются в уровнях от 0 до 1.

На первом этапе рассчитываем уровень угрозы по уязвимости на основе критичности и вероятности реализации угрозы через уязвимость. Расчет производится по формуле

$$Th = V \cdot P(T), \tag{2}$$

где Th — уровень угрозы по уязвимости.

Значение уровня угрозы по уязвимости получаем в интервале от 0 до 1.

Для того чтобы учесть контроли, модифицируем формулу (2), и вероятность реализации угрозы будем рассчитывать следующим образом:

$$Pk(T) = \frac{P(T)}{C \cdot Ek}, \tag{3}$$

где Ek — уровень эффективности введенных контрмер, который оценивается экспертом и указывается в интервале от 0 до 1. Коэффициент $C = 10$ нужен для того, чтобы получить значение уровня угрозы по уязвимости в интервале от 0 до 1.

Чтобы рассчитать уровень угрозы по всем уязвимостям, через которые возможна реализация данной угрозы на актив, просуммируем полученные уровни угроз через конкретные уязвимости по формуле

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th). \tag{4}$$

Значения уровня угрозы по всем уязвимостям получим в интервале от 0 до 1. Аналогично, учитывая все угрозы, действующие на актив, рассчитываем общий уровень угроз по активу или событие, действующее на актив:

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh). \tag{5}$$

Значение общего уровня угроз по активу получим в интервале от 0 до 1.

В соответствии с онтологий предметной области, чтобы рассчитать уровень риска по активу, используем возможность события и уровень воздействия (см. рис.2):

$$R = CThR \cdot AV. \tag{6}$$

Здесь IV — величина воздействия, определяемая следующим образом:

$$IV = AV \cdot SN, \tag{7}$$

где AV — ценность актива (см. рис. 2); SN — последствие уязвимости для актива.

Ценность актива и последствие для актива оцениваются экспертом и указываются в интервале от 0 до 1. В результате получим значение риска по активу в интервале от 0 до 1.

Возврат инвестиции, вложенной в ИБ

Управление рисками ИБ сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений, при которых возможно их принятие. Для этого требуется применить контрмеры. Чем сильнее контрмеры безопасности затрудняют вредоносную активность, тем более удачным можно считать их выбор. В качестве формализма, поддерживающего данный подход, целесообразно использовать графы атак, вершины которых помечены возможными контрмерами и их количественной экономической оценкой с точки зрения защищающегося и атакующего [7, 8].

Однократный ущерб на ресурс будем определять по формуле

$$SLE = AV \cdot V, \tag{8}$$

где AV — ценность ресурса, в которую входят все виды затрат на него (установка, сопровождение и т.п.); V — мера уязвимости актива к угрозе.

Поскольку не все угрозы равновероятны, введем вероятность реализации угрозы ($P(T)$). Тогда ожидаемый годовой ущерб от данной угрозы будет вычисляться по формуле

$$ALE = SLE \cdot P(T). \tag{9}$$

Оценка значения $P(T)$ может производиться на основе анализа статистики нарушений информационной безопасности.

Экономический эффект от реализации контрмеры (т.е. от расходов на информационную безопасность) можно оценить по формуле

$$ROSI = \left(ALE \cdot Ek - CSI \right) / CSI, \tag{10}$$

где Ek — коэффициент уменьшения риска в результате реализации контрмеры (лежит в промежутке от 0 до 1), а CSI — стоимость реализации контрмер. При положительном значении $ROSI$ реализация регулятора безопасности является экономически оправданной; в противном случае в ней нет смысла. $ROSI$ — это инструмент экономической оценки эффективности действий (защищающейся) организации в области информационной безопасности. Цель состоит в максимизации значения $ROSI$.

Критерий $ROSI$ позволяет оценивать эффективность как одиночных, так и нескольких мероприятий и способствует снижению рисков ИБ, а также оценивать степень снижения риска по классам угроз.

Результаты и обсуждение

Исходя из введенных владельцем информационной системы данных, можно построить модель угроз и уязвимостей, актуальных для информационной системы компании. На основе полученной модели эксперт оценивает вероятность реализации угрозы, меру уязвимости к угрозе и ценность актива. Исходя из этого будут рассчитаны риски информационной безопасности (табл. 1).

Таблица 1

Введенные данные экспертов и полученный уровень риска ИБ

№	Актив		Угроза		Уязвимость			*R* по формуле (6)	*R* по формуле (1)
	Название	Ценность актива (*AV*)	Название	*P*(*T*)	Название	*V*	Последствие уязвимости (*SN*)		
1	2	3	4	5	6	7	8	9	10
1	Данные, которые передаются между отделами	0,9	Перехват информации	0,2	Незащищенные линии коммуникаций	0,4	0,9	0,285002	0,072
			Изменение информации	0,4	Незащищенная передача информации с ограниченным доступом	0,7	0,2		0,252
2	Данные, которые хранятся на сервере	0,9	Кража в серверных комнатах	0,6	Отсутствие физической защиты окон, дверей	0,3	0,5	0,359454	0,162
			Неавторизованный допуск в помещение с ограниченным доступом	0,9	Отсутствие систем контроля допуска	0,3	0,9		0,243

1	2	3	4	5	6	7	8	9	10
3	Информация, которая хранится в файлах	0,7	Неавторизованный доступ к резервным копиям конфигурационной информации	0,4	Отсутствие контроля доступа к файловому серверу	0,8	0,5	0,112	0,224
4	Сервис, который предоставляет услуги	0,7	Интернет атаки (DOS или DDOS атака)	0,4	Неэффективная фильтрация входящего трафика	0,3	0,2	0,0168	0,084
5	Информация или бизнес-планы	0,5	Обсуждение конфиденциальной информации в незащищенных помещениях или вне помещений	0,6	Отсутствие политик, правил обращения с информацией с ограниченным доступом	0,8	0,1	0,024	0,24

Для снижения уровня риска предлагается применить контрмеры уменьшения вероятности реализации угрозы через уязвимости. После введения контрмер эксперт оценивает их эффективность (табл. 2, столбец 7) и по формуле (3) рассчитывает вероятность реализации угрозы после введенных контрмер. Затем по формуле (6) и (1) заново будем рассчитывать уровень риска информационной безопасности.

Таблица 2

Уровень риска после введения контрмер

№	Актив	Угроза	Уязвимость	Контрмеры		*R1* по формуле (6)	*R1* по формуле (1)
				Название	*Ek*		
1	2	3	4	5	6	7	8
1	Данные, которые передаются между отделами	Перехват информации	Незащищенные линии коммуникаций	Физически поставлять данные	0,9	0,241779	0,036
		Изменение информации	Незащищенная передача информации с ограниченным доступом	При передаче использовать алгоритмы шифрования	0,1		0,126
2	Данные, которые хранятся на сервере	Кража в серверных комнатах	Отсутствие физической защиты окон, дверей	Установить металлическую дверь и решетки на окна	0,2	0,099186	0,081
		Неавторизованный допуск в помещение с ограниченным доступом	Отсутствие систем контроля допуска	Установить дополнительные камеры видеонаблюдения	0,5		0,135
3	Информация, которая хранится в файлах	Неавторизованный доступ к резервным копиям конфигурационной информации	Отсутствие контроля доступа к файловому серверу	Перенести файловое хранилище в виртуальную среду	0,2	0,056	0,112
4	Сервис, который предоставляет услуги	Интернет атаки (DOS или DDOS атака)	Неэффективная фильтрация входящего трафика	Производить фильтрацию входящего трафика	0,9	0,001867	0,042

1	2	3	4	5	6	7	8
5	Информация или бизнес-планы	Обсуждение конфиденциальной информации в незащищенных помещениях или вне помещений	Отсутствие политик, правил обращения с информацией с ограниченным доступом	Обучение персонала по вопросам о мерах предосторожности при работе с конфиденциальной информацией	0,5	0,0048	0,12

Как видно из таблицы 1, если на один актив действует несколько угроз и одна угроза использует несколько уязвимостей, тогда получить реальный уровень риска актива по формуле (1) трудно (см. табл. 1, пересечение строк 1,2, столбец 9). Таким образом, по классическому методу на один актив получаем два риска. Так как на один актив действует две угрозы, то по предлагаемому нами методу получаем один риск для одного актива (см. табл. 1, пересечение строк 1,2, столбец 8). Если на один актив действует только одна угроза, и она использует только одну уязвимость, тогда предложенный нами метод соответствует классическому методу оценки рисков (см. табл. 1, пересечение строк 3,4,5 столбцами 8,9).

Таблица 3

Пример расчета возврата инвестиции, вложенной в ИБ

#	Актив		Угроза	Уязвимость	Контрмеры			ROSI
	Название	Ценность актива, у.е.			Название	*Ek*	Цена, у.е.	
1	Данные, которые передаются между отделами	3000	Перехват информации	Незащищенные линии коммуникаций	Физически поставлять данные	0,9	40	4,4
			Изменение информации	Незащищенная передача информации с ограниченным доступом	При передаче использовать алгоритмы шифрования	0,1	30	1,8
2	Данные, которые хранятся на сервере	3000	Кража в серверных комнатах	Отсутствие физической защиты окон, дверей	Установить металлическую дверь и решетки на окна	0,3	120	0,35
			Неавторизованный допуск в помещение с ограниченным доступом	Отсутствие систем контроля допуска	Установить дополнительные камеры видеонаблюдения	0,5	90	3,5
3	Информация, которая хранится в файлах	2500	Неавторизованный доступ к резервным копиям конфигурационной информации	Отсутствие контроля доступа к файловому серверу	Перенести файловое хранилище в виртуальную среду	0,2	50	2,2
4	Сервис, который предоставляет услуги	2500	Интернет атаки (DOS или DDOS атака)	Неэффективная фильтрация входящего трафика	Производить фильтрацию входящего трафика	0,9	50	4,4
5	Информация или бизнес-планы	2000	Обсуждение конфиденциальной информации в незащищенных помещениях или вне помещений	Отсутствие политик, правил обращения с информацией с ограниченным доступом	Обучение персонала по вопросам о мерах предосторожности при работе с конфиденциальной информацией	0,5	100	3,8

Предложенная нами формула расчета вероятности реализации угрозы через уязвимость учитывает эффективность введенных контрмер, которая играет важную роль для снижения рисков. При введении контрмер надо учитывать не только снижение рисков, но и возврат инвестиций, вложенных в ИБ (см. табл. 3). Это позволит получить экономическое обоснование целесообразности применения защитных мер, что в конечном итоге приведет к экономии бюджета организации и предприятия.

Полученные результаты могут быть расширены на следующих этапах исследования путем анализа большого количества бизнес-моделей и событий безопасности. Будущие исследования связаны с разработкой специального программного инструментария оценки рисков. Экспертные оценки будут обрабатываться методами статистической обработки нечетких данных [9, 10].

Список литературы

1 *Koller G., Koller R.* Modern Corporate Risk Management: Blueprint for Positive Change and Effectiveness. — New York: J. Ross Publishing, 2007. — 272 p.

2 ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.

3 ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

4 ISO/IEC 27005:2008. Information technology. — Security techniques. — Information security risk management.

5 *Gruber T.R.* Toward principles for the design of ontologies used for knowledge sharing. International // J. of Human-Computer Studies. — 1195. — Vol. 43 (5–6). —P. 907–928.

6 *Mayer N.* Model-based Management of Information System Security Risk. [PhD thesis] University of Namur, 2009.

7 *Куканова Н.* Методика оценки риска ГРИФ-2006 из состава Digital Security Office, [ЭР]. Режим доступа: http://dsec.ru/ipm-research_center/article/risk_assessment_method_vulture_2006_from_the_composition-_of_the_digital_security_office/?sphrase_id=406

8 *Кащенко А.Г.* Оценка эффективности мероприятий по снижению рисков информационной безопасности // Информация и безопасность. — 2007. — № 3 — С. 511–513.

9 *Bojadziev G., Bojadziev M.* Fuzzy Logic for Business, Finance and Management. Singapore: World Scientific, 1997.

10 *Ngai E.W.T., Wat F.K.T.* Fuzzy decision support system for risk analysis in e-commerce development, Decision Support Systems 40. — 2005. — P. 235–255.

Р.Мұратхан, Д.Ж.Сатыбалдина

Көп компонентті қатері бар ақпараттық қауіпсіздіктің тәуекелін бағалаудың сандық әдісі

Мақалада ақпараттық қауіпсіздіктің тәуекелін бағалау үшін пәндік облысты сипаттаудың онтологиясы негізінде және бір немесе бірнеше әлсіздігі бар, көп компонентті қатердің тәуекелін бағалаудың құрама әдісі келтірілген.

R.Muratkhan, D.Zh.Satybaldina

Quantitative method of risks assessment of information security for multi component threats

The paper proposes a combined approach to assess the risk of information security events based on ontological domain description, business processes modeling language and quantitative method of risk assessment for multi component threats implementation using more than one vulnerability.

References

1 Koller G., Koller R. *Modern Corporate Risk Management*: Blueprint for Positive Change and Effectiveness, New York: J. Ross Publ., 2007, 272 p.

2 *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*.

3 *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.*

4 *ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management*.

5 Gruber T.R. *J. of Human-Computer Studies*, 43 (5–6), (1195), p. 907–928.

6 Mayer N. *Model-based Management of Information System Security Risk*. [Ph.D. thesis] University of Namur, 2009.

7 Kukanova N. *Metodika ocenki riska GRIF 2006 iz sostava Digital Security Office*, [ER]. Access mode: http://dsec.ru/ipm-research_center/article/risk_assessment_method_vulture_2006_from_the_composition-_of_the_digital_security_office/?sphrase_id=406

8 Kachshhenko A.G. *Information and Security*, 3, 2007, p. 511–513.

9 *Bojadziev G., Bojadziev M.* Fuzzy Logic for Business, Finance and Management, Singapore: World scientific, 1997.

10 Ngai E.W.T., Wat F.K.T., *Fuzzy decision support system for risk analysis in e-commerce development*, Decision Support Systems 40 (2005), p. 235–255.

UDC 378.004

B.M.Nurlanova

Ye.A.Buketov Karaganda State University (E-mail: b.nurlanova@mail.ru)

Assessment of consumers satisfaction by quality of information telecommunication educational technologies

In article the system of estimation containing a method of an assessment and the corresponding questionnaire, is developed for determination of satisfaction of consumers. The assessment of quality of information and telecommunication educational technologies is defined on the basis of processing of results of questioning.

Key words: educational information and telecommunication technologies, assessment of consumers satisfaction, a method of an assessment, anonymous survey, electronic educational resources.

The modern education system uses information technologies and computer telecommunications more actively. The education system that promoted especially dynamically by a number of factors, and first of all — equipment of educational institutions by the powerful computer equipment and development of community of the Internet develops.

Information technology — this is another marketing channel. It is necessary to know their opportunities and laws and to apply to destination. It is necessary to try, it is necessary to set real tasks and to apply appropriate means.

Thus, innovative learning technologies have a number of good points as adaptability, mobility, democracy, and the end result of improving the quality of education.

Use of information and telecommunication technologies gives the chance to build extremely favorably for the user an individual trajectory of training. Student can personally specify the time and sequence of study subjects, as well as the students are given several opportunities to perform laboratory work to realize practical tasks that actually it is impossible. Essential also is that application of information and telecommunication technologies in training gives the chance to the student to carry out at distance communication with the teacher in time convenient for, applying for this purpose a forum, a chat, e-mail [1].

Use of technologies allows the teacher always update the content of education; to carry out any kind of occupation, also to realize control and self-checking of results of students educational activity.

In parallel with the benefits of information and telecommunication technologies and their use in many universities of our country has a lot of problems, such as, first, inadequate resourcing and weak material and technical equipment of the schools; Second, as noted I.V.Popova and V.I.Zhiltsova, insufficient didactic component of electronic educational resources determines that no technological approach to learning in many distance learning courses, besides the direction of the educational process mainly on the reproductive nature of the activity [2]. It is possible to call one more of burning issues of higher education institutions is a weak level of information competences of the teachers, not allowing them actively and productively to apply in educational process of information and telecommunication technologies. A significant problem is the lack of a comprehensive evaluation system and criteria developed quality of electronic educational resources.

To solve this problem it is necessary to evaluate the electronic educational resources for these resources to develop a simplified method costs, the cost of equipment such as computer classes, Internet connection and installation of furniture, salary staff (teaching, administration, repairs, utilities, office supplies, etc.).