УДК 658.29-049.5

КОМПЛЕКСНЫЙ МЕТОДИЧЕСКИЙ ПОДХОД ОПЕРАТИВНОЙ ОЦЕНКИ УРОВНЯ КИБЕРПРЕСТУПЛЕНИЙ

канд. техн. наук В.В. МАЛИКОВ
(Центр повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь, Минск);
канд. техн. наук Е.А. КРИШТОПОВА
(Белорусский государственный университет информатики и радиоэлектроники, Минск)

Предложен комплексный методический подход по оценке уровня киберпреступлений, учитывающий нормативно-правовые, технологические, экономические критерии и параметры. Рассматриваются принципы, реализующие оценку уровня киберпреступлений. Показана совокупная экономическая оценка прибыли от реализации атак, учитывающая величину уровня доходности по критерию близости риска совершения киберпреступлений, основанному на оценках технико-экономического потенциала рынка и уровня наказания в соответствии с нормативно-правовыми актами. Классифицируется рынок киберпреступности.

Введение. В настоящее время использование информационно-коммуникационных технологий со стороны организаций различных форм собственности, а также физических лиц приобрело трансграничный характер. Государства, на территории (или через территории) которых осуществляется активное использование таких технологий, должны принимать меры для нормативно-правового, организационно-технического и технического регулирования в данной сфере. Обеспечение внутригосударственного регулирования невозможно без учета аспектов международного законодательства и сотрудничества между ведущими индустриально развитыми странами.

Глобальный рынок киберпреступности активно развивается и совершенствуется в соответствии с передовыми направлениями информатизации общества, внедрением электронных систем коммуникаций, электронных платежных систем [1].

В целях организации действенной системы противостояния современным вызовам и угрозам, реализуемым для противоправной деятельности со стороны преступного сообщества, необходима разработка методической базы, способствующей пресечению и раскрытию киберпреступлений.

Методика исследований. Для оценки состояния рынка киберпреступности, устанавливающего уровень его соответствия определенным критериям и показателям, необходимо проведение совокупного экономического анализа прибыли от реализации атак с учетом величины уровня доходности по критерию близости риска совершения киберпреступлений, который базируется на оценках технико-экономического потенциала рынка и уровня наказания в соответствии с нормативно-правовыми актами. Существующие в настоящее время методы оценки, а также программные комплексы, разработанные на их основе, имеют определенный перечень недостатков и уязвимостей, а также значительную (во многих случаях избыточную) стоимость и низкую функциональность [2].

Для достижения цели, заключающейся в разработке методического подхода по технической и экономической оценке уровня киберпреступлений, необходимо задаться перечнем принципов, его реализующих. В качестве *основополагающих принципов* выделим следующие: цели, согласования критериев, равнопрочности оценки.

Под *принципом цели* будем понимать следующее: все решения при проведении оценки ориентированы на главную цель – обеспечение требуемого уровня достоверности информации для принятия управленческих решений.

Под *принципом согласования критериев* будем понимать то, что оценки состояния киберперступности на всех уровнях иерархии анализируемой структуры должны быть согласованы и базироваться на оценках состояния элементов нижнего уровня иерархии.

Под *принципом равнопрочности оценки* будем понимать следующее: оценка риска совершения комплесной кибератаки в целом и отдельных технологических атак в частности равна величине максимального риска совершения преступления, т.е. оценка риска производится по наиболее уязвимому элементу.

Будем считать, что логически законченные подсистемы структуры рынка киберпреступности P_m являются независимыми модулями, т.е. вероятность реализации атаки подсистемой O_A не влияет на вероятность реализации атаки подсистемой O_B, т.е. $P_{OA}(O_B) = P_B$.

Однако известно, что каждая подсистема множества O определяется множеством $R = \{R_1, R_2, \dots, R_n\}$ признаков, которые будем называть *показателями атакующей системы*.

Таким образом, для рынка киберпреступности требуется определить множества $P = \{P_1, P_2, \dots, P_m\}$, общий риск для каждой атакующей подсистемы множества O с учетом множества показателей атакующей системы $R = \{R_1, R_2, \dots, R_n\}$ как по уровню структуры киберпреступлений, так и всей структуры киберпреступлений в целом [3].

Результаты и обсуждение. Оценка технического и экономического уровня киберпреступлений была проведена через определенные действия.

1. *Декомпозиция рынка киберпреступности на законченные функциональные уровни и модули* (рис. 1). Предлагается использование варианта декомпозиции, который учитывает полный технологический цикл осуществления атак, включающий как разработку вредоносного программного обеспечения, так и непосредственно его использование в преступных целях. В качестве *базовых уровней* предлагаются следующие: интернет-мошенничество; спам; DDos-атаки; рынок криминальных средств систем и услуг [2; 4; 5].

Рис. 1. Классификация рынка киберпреступности

2. Следующий этап – *проведение уровневой технико-экономической оценки потенциала модулей рынка киберпреступности*.

Техническую оценку будем проводить на основе параметра технологичности атаки – $K_{техн}$, показатели которого будут иметь следующие возможные значения:

- высокотехнологичная атака/услуга (H): не описана в базах знаний по уязвимостям и сборниках эксплойтов – является таргетированной (0-day, Watering Hole, social engineering и др.) [4; 5];
- низко технологичная атака/услуга (L): описана в базах знаний по уязвимостям и сборниках эксплойтов – не является таргетированной.

Экономическую оценку будем проводить на основе параметра потенциального объема рынка $P_{пот}$, показатели которого будут иметь следующие возможные значения:

- высокий объем рынка (H): потенциальный объем ≥ 1 млн. долларов США;
- низкий объем рынка (L): потенциальный объем менее 1 млн. долларов США.

Таким образом, представление уровневой технико-экономической оценки потенциала рынка киберпреступности $У_{кибер}$ с учетом описанных параметров оценки будет иметь вид:

$$У_{кибер} = \{K_{техн}, P_{пот}\}. \quad (1)$$

В качестве базовых уровней технико-экономической оценки потенциала рынка киберпреступности $У_{кибер}$ предлагаются такие: $A1$ (H, H), $B1$ (H, L), $C1$ (L, H), $D1$ (L, L).

3. Далее проведем *уровневую оценку величины наказания за совершенные киберпреступления по действующим нормативно-правовым актам*.

Оценку длительности срока лишения свободы осуществим на основе параметра величины срока наказания $H_{ср}$, показатели которого будут иметь следующие возможные значения:

- высокий уровень наказания (H): срок лишения/ограничения свободы ≥ 3 лет;
- низкий уровень наказания (L): срок лишения/ограничения свободы менее 3 лет.

Финансовая оценка наказания осуществляется на основе параметра величины срока наказания $H_{фин}$, показатели которого будут иметь следующие возможные значения:

- высокий уровень (H): сумма штрафа ≥ 100 тыс. долларов США;
- низкий уровень (L): сумма штрафа менее 100 тыс. долларов США.

Таким образом, представление уровневой оценки величины наказания за совершенные киберпреступления по действующим нормативно-правовым актам $У_{НПА}$ с учетом описанных параметров оценки будет иметь вид:

$$У_{НПА} = \{H_{ср}, H_{фин}\}. \quad (2)$$

В качестве *базовых уровней оценки величины наказания* за совершенные киберпреступления по действующим нормативно-правовым актам $У_{НПА}$ предлагаются уровни: $A2$ (H, H), $B2$ (H, L), $C2$ (L, H), $D2$ (L, L).

4. Затем необходимо провести *экспертные оценки средней стоимости организации атаки /услуги на рынке киберпреступности* $С_{орг}$, а также *потенциально возможного среднего дохода от организации атаки / услуги* $С_{дох}$.

5. На следующем этапе необходимо рассчитать *уровень доходности атаки* $У_{дох}$ *с учетом коэффициента риска* $К_{риска}$ по формуле

$$У_{дох} = К_{риска} \cdot \left(\frac{С_{дох}}{С_{орг}} \right). \quad (3)$$

Коэффициент риска $К_{риска}$ будем рассчитывать по формуле

$$К_{риска} = К_{кибер} \cdot К_{НПА}. \quad (4)$$

Соответствующие значения $К_{кибер}$ и $К_{НПА}$ на основе экспертной оценки будем определять из соответствующих параметров оценки $У_{кибер}$ и $У_{НПА}$, указанных в таблицах 1 и 2 соответственно.

Таблица 1

Значения коэффициента $К_{кибер}$

Показатель	Базовый уровень $У_{кибер}$			
	A1	B1	C1	D1
Значение $К_{кибер}$	0,9	0,6	0,3	0,1

Таблица 2

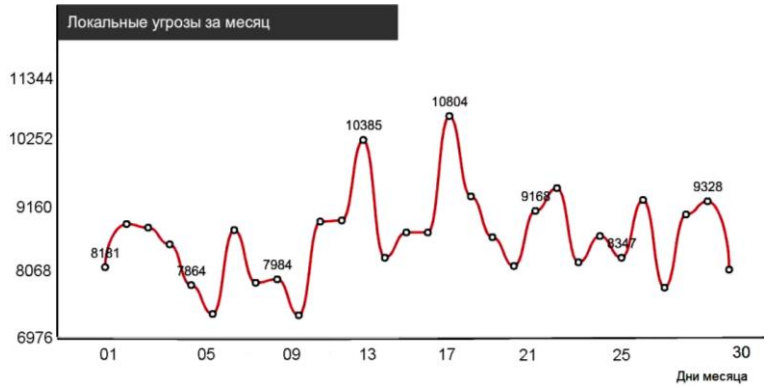
Значения коэффициента $К_{НПА}$

Показатель	Базовый уровень $У_{НПА}$			
	A2	B2	C2	D2
Значение $К_{НПА}$	0,9	0,7	0,5	0,3

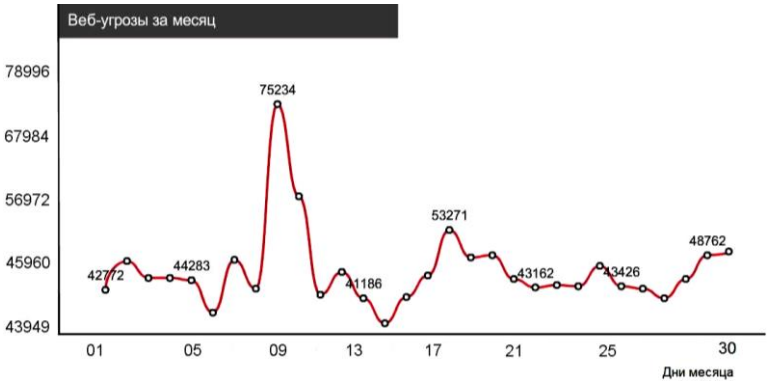
При этом государственным регуляторам и организациям по борьбе с киберпреступлениями в первую очередь необходимо обратить внимание на преступления с $У_{дох} \geq 0{,}4$, так как в данных случаях высокий уровень дохода при низком уровне ответственности будет способствовать увеличению такого рода атак.

6. Далее определим *потенциально возможное количество атак / услуг* $Ч_{общ}$, на основе экспертных оценок и/или результатов практического сканирования уязвимостей.

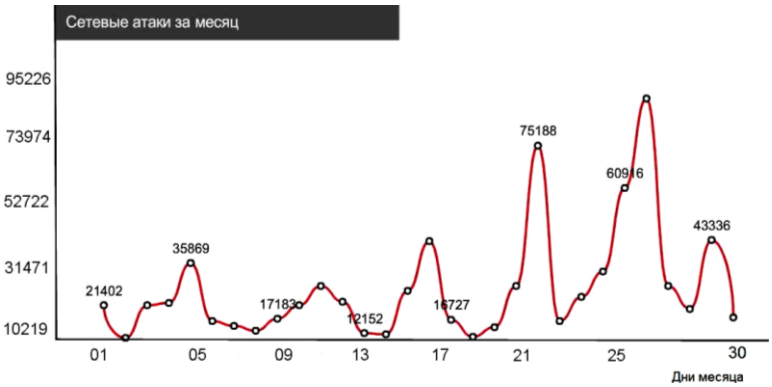
Например, в Республике Беларусь только количество угроз, определенное результатами on-line сканирования в одном из месяцев 2013 года (рис. 2) [6], в день может составить (по среднему числу угроз в месяц) более 50 тысяч.



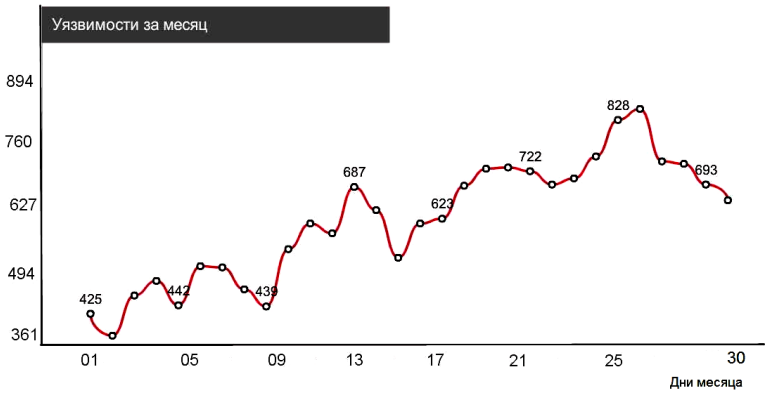
а)



б)



в)



г)

Рис. 2. Результаты on-line сканирования уровня угроз, сетевых атак и уязвимостей в Республике Беларусь за один из месяцев 2013 года: количество локальных угроз, шт. (*а*); количество веб-угроз, шт. (*б*); количество сетевых атак, шт. (*в*); количество уязвимостей, шт. (*г*)

7. На следующем этапе определяем *общий средний доход от реализации атак / услуг* по формуле:

$$Д_{общ} = Ч_{общ} \cdot С_{дох}. \quad (5)$$

Например, по оценкам, суммарная величина доходов рынка киберпреступности в Российской Федерации за 2012 год составила 1,938 млрд. долларов США [2].

Заключение. Предложенный методический подход по оценке уровня киберпреступлений позволяет проводить совокупную экономическую оценку прибыли от реализации атак с учетом величины уровня доходности по критерию близости риска совершения киберпреступлений, основанному на оценках технико-экономического потенциала рынка и уровня наказания в соответствии с нормативно-правовыми актами.

Результаты проведения практической оценки рынка киберпреступлений позволят государственным регуляторам и организациям по борьбе с киберпреступлениями оперативно изменять положения нормативно-правовых актов, методику оперативно-розыскных мероприятий и общей информированности граждан.

ЛИТЕРАТУРА

1. Вехов, В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дис. ... д-ра юрид. наук: 12.00.09 / В.Б. Вехов; ФГОУ ВПО «Волгогр. акад. МВД Рос. Федерации». – Волгоград, 2008. – 59 с.
2. Рынок преступлений в области высоких технологий: состояние и тенденции 2013 года // group-ib.ru [Электронный ресурс]. – 2003–2013. – Режим доступа: http://www.group-ib.ru/list/1008-analytics/?view=article&id=1155.
3. Маликов, В.В. Повышение эффективности информационных и инженерно-технических систем защиты критически важных объектов: дис. ... канд. техн. наук: 05.13.19 / В.В. Маликов; БГУИР. – Минск, 2010. – 174 л.
4. DDoS-атаки первого полугодия 2013 года // securelist.com [Электронный ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/analysis/208050810/DDoS_ataki_pervogo_polugodiya_ 2013_ goda. Спам в июле 2013 // securelist.com [Электронный ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/analysis/208050808/Spam_v_iyule_2013.
5. Статистика 2013 // securelist.com [Электронный ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/statistics#/ru/map/vul/month/Belarus.

Поступила 26.09.2013

METHODICAL APPROACH OF OPERATIVE ASSESSMENT OF THE LEVEL OF CYBER CRIME

V. MALIKOV, E. KRYSHTOPOVA

The comprehensive methodological approach of assessing the level of cyber crime, which takes into account regulatory, technological, economic criteria and parameters is proposed. The article covers the principles of implementing the assessment of the level of cybercrime. The total economic valuation of the profit gained from the realization of attacks, taking into account the value of the profitability level by proximity of the risk of committing cybercrime, based on estimates of technical and economic potential of the market and the level of punishment in accordance with the legal regulations is shown. The classification of the cyber crime market is given.