УДК 004.021 + 343.143 Вестник УрФО № 4(30) / 2018, с. 38–42

Максимова Е. А., Баранов В. В., Зязин В. П.

DOI: 10.14529/secur180406

МОДЕЛЬ ОЦЕНКИ РИСКОВ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Количество компьютерных преступлений постоянно возрастает. В это же время показатели расследования их остаются на низком уровне и отражают низкую степень профессионализма сотрудников правоохранительных органов. В ходе расследования данного вида преступлений не исключена ситуация «эксперт-возможный злоумышленник». Следовательно, необходима соответствующая оценка рисков.

Предлагается для обсуждения разработанная модель «эксперт-возможный злоумышленник». Элементы модели: набор возможных мотивов, соответствующий набор личностных характеристик, соотношение между возможными угрозами и мотивами потенциального злоумышленника–эксперта. Стоимость возможного ущерба от совершенного компьютерного преступления в количественной оценке рисков обоснована с точки зрения законодательства. В том случае, когда оценочная величина риска больше допустимой, то предлагается принять решение о возможности участия эксперта в работе. Если вариант привлечения иного специалиста не возможен, то в ходе следственных мероприятий предлагается использовать программу видеозахвата.

Предложенная модель оценки рисков позволит автоматизировать процесс работы с компьютерными преступлениями на этапе расследования и повысить уровень их раскрываемости.

Ключевые слова: *риск, компьютерное преступление, расследование, мотив, угроза, архитектура, модель.*

Maksimova E. A., Baranov V. V., Ziazin V. P.

THE MODEL OF RISK ASSESSMENT IN THE INVESTIGATION OF COMPUTER CRIMES

The number of computer crimes is constantly growing. At the same time, their investigation indicators remain low and reflect the low degree of professionalism of law enforcement officers. During the investigation of this type of crime, the situation is not excluded: "an expert-possible attacker". Therefore, an appropriate risk assessment is necessary.

The developed model "expert-possible attacker" is proposed for discussion. Elements of the model: a set of possible motives, a corresponding set of personal characteristics, the relationship between possible threats and motivations of a potential attacker-expert. The cost of possible damage from a committed computer crime in the quantitative assessment of risks is justified from the point of view of legislation.

In the event that the estimated value of the risk is more than acceptable, it is proposed to

decide on the possibility of the expert's participation in the work. If the option of engaging another specialist is not possible, then during the investigation activities it is proposed to use the video capture program.

The proposed model of risk assessment will allow to automate the process of working with computer crimes during the investigation phase and to raise their level of disclosure.

Keywords: *risk, computer crime, investigation, motive, threat, architecture, model.*

В последнее время количество компьютерных преступлений (КП) постоянно увеличивается. Так, согласно данных Главного информационно-аналитического центра Министерства внутренних дел РФ, количество их за последние 10 лет увеличилось в 22,3 раза и ежегодно продолжает увеличиваться, в среднем, в 3,5 раза. Кроме того, ежегодный размер материального ущерба от КП - 613,7 млн. рублей; средний ущерб потерпевшего от 1 КП - 1,7 млн. рублей. В это же время расследуется около 49% преступлений; обвинительные приговоры выносятся в 25,5% случаев от общего числа возбужденных уголовных дел; средний показатель количества уголовных дел, по которым производство приостановлено, составляет 43,5% и ярко отражает низкую степень профессионализма сотрудников правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению указанных преступных посягательств.

Сегодня при работе с КП применяются стандартные алгоритмы действий, не учитывающие специфик данного вида деяний [2-5]. Это является одной из причин роста киберпреступности и низким показателем их раскрытия. Таким образом, необходим новый подход к работе, эффективность которого, в том числе определяется оценкой рисков.

Сравнительный анализ методов и этапов работы с КП показал существенное отличие в работе с данного вида деянием. На этапе расследования КП привлекаются эксперты. Высококвалифицированных специалистов, способных провести экспертизу в данном направлении не достаточно. Таким образом, не исключена ситуация «эксперт-возможный злоумышленник». Следовательно, необходима оценка рисков, связанных с данной ситуацией.

В разработанной модели «эксперт-возможный злоумышленник» (рисунок 1) выделен набор возможных мотивов [1]:

М1 – Причинение имущественного ущерба путем мошенничества или иным преступным путем.

М2 – Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.

М3 – Получение конкурентных преимуществ.

М4 – Причинение имущественного ущер-

Рис. 1. Схема работы с экспертами при расследовании компьютерных преступлений

ба путем обмана или злоупотребления доверием

М5 – Непреднамеренные, неосторожные или неквалифицированные действия

М6 – Любопытство или желание самореализации (подтверждение статуса).

М7 – Месть за ранее совершенные действия.

М8 – Идеологические или политические мотивы.

Каждый из представленных мотивов соответствует набору личностных характеристик (таблица 1).

Так как в УК за совершенное компьютерное преступление предусмотрен либо штраф, либо срок отбывания наказания, то можно рассмотреть в качестве оценочного эквивалента - стоимость возможного ущерба от совершенного компьютерного преступления.

При этом, для оценки срок-эквивалента, так как отсутствует точная денежная оценка, то можно ввести показатель Е – одна условная денежная единица, соответствующая одному году лишения свободы и оценить стоимость возможного ущерба по каждому виду компьютерного преступления.

Таблица 1

Соответствие возможных мотивов показателям характеристик личности

Показатели характеристики личности	Мотивы
Уровень тревожности (U1)	М3, М5
Уровень упорства (U2)	М3, М6, М7
Уровень агрессию(U3)	М1, М6, М7,М4,М5
Уровень обидчивость(U4)	М1, М6, М7,М5
Уровень жадности (U5)	М1, М6, М8
Уровень алчности (U6)	М2, М8, М3
Уровень самооценки (U7)	М3, М2, М6, М7

В свою очередь, можно составить соотношение между возможными угрозами и мотивами потенциального злоумышленника –эксперта. К примеру, для угроз: «уничтожение данных», «изменение системы», «модификация данных» представлено следующее соответствие (рисунок 2), где количественные показатели: «0; 0,3; 0,6; 0,9» - мотивационная оценка в шкале «0,1».

Тогда, оценка стоимости возможного ущерба от совершенного компьютерного преступления рассчитывается по формуле:

$$C = S + Y \cdot E$$

где S- штраф за совершенное компьютерное преступление,

Y- срок отбывания наказания за совершенное компьютерное преступление,

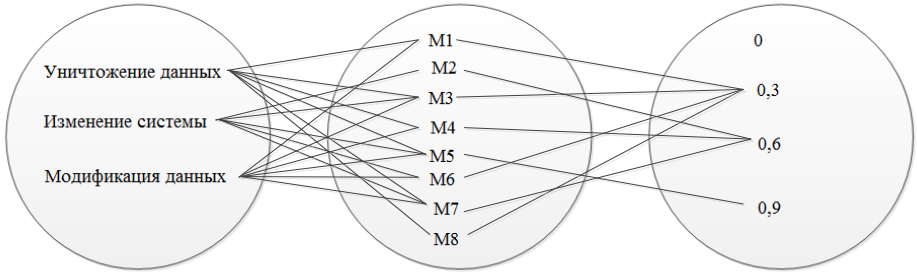

Рис. 2. Соотношение «угрозы при расследовании КП – мотивы эксперта-потенциального злоумышленника»

Обобщенная оценка риска определяется по формуле:

$$|\mathrm{Risk}| = \frac{1}{n} \cdot \sum_{i=1}^{n} Risk_i;$$

где i – номер пройденного модуля,

n - количество пройденных модулей,

$Risk_i$ - риск наличия i-го мотива

$$Risk_i = p_i \cdot \mathrm{C},$$

С – стоимость возможного ущерба от совершенного компьютерного преступления.

Е – одна условная денежная единица, соответствующая одному году лишения свободы.

В том случае, когда оценочная величина риска больше допустимой, то должно быть принято решение о возможности участия эксперта в работе. Если вариант привлечения иного специалиста не возможен, то в ходе следственных мероприятий предлагается использовать программу видеозахвата.

На рисунке 3 представлена архитектура модели оценки рисков при расследовании компьютерных преступлений.

Для каждого из модулей представлен модуль расчета результата.

Из данных модулей формируется общий

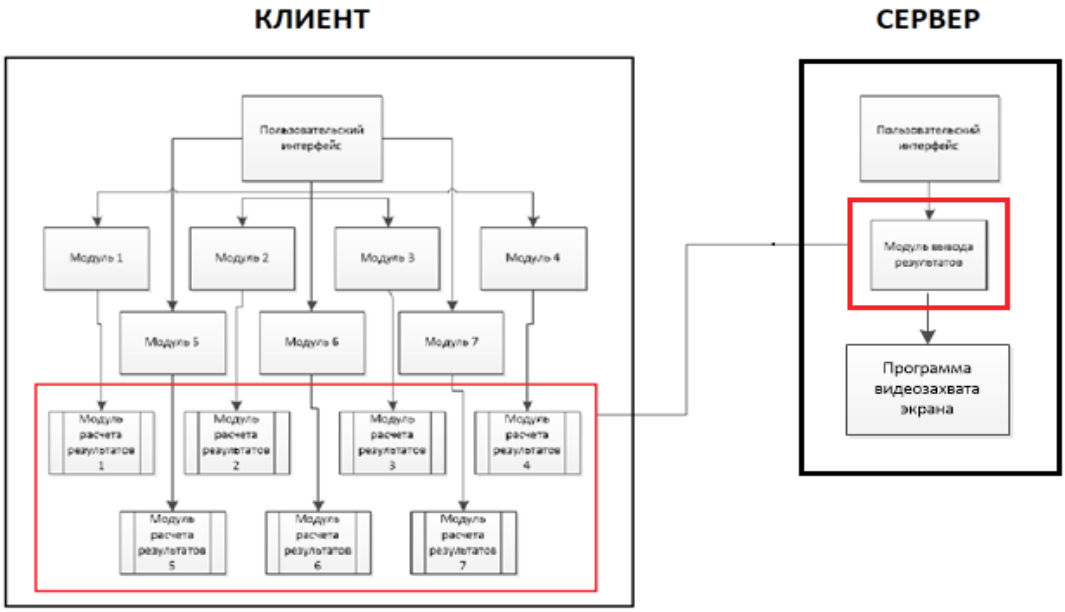

Рис. 3. Архитектура модели оценки рисков при раскрытии компьютерных преступлений

Архитектура модели представлена управляющим модулем, который содержит:

для КЛИЕНТА:

— Модуль 1. Тест на определение уровня тревожности

— Модуль 2. Тест «Упорство» (Методика е.П.Ильина, е.К.Фещенко)

— Модуль 3. Тест агрессивности (опросник л. Г. Почебут)

— Модуль 4. Тест на обидчивость

— Модуль 5. Тест на алчность

— Модуль 6. Тест на жадность

— Модуль 7. Тест на самооценку личности. Методика Будасси.

отчет по пройденным тестам и вывод результата на сервер;

для СЕРВЕРА:

— Модуль вывода результатов, и уровня риска (в соответствии с пройденными тестами)

— Программа видеозахвата экрана.

Предложенная модель позволит автоматизировать процесс работы с компьютерными преступлениями на этапе расследования и повысить уровень их раскрываемости.

Литература

1. Максимова Е.А.

2. Ляхова О. О. Классификация следственных версий // Молодой ученый. — 2018. — №7. — С. 137-138. — URL https://moluch.ru/archive/193/48373/ (дата обращения: 16.09.2018)

3. Коровин Н. К. Криминалистика: учебное пособие/ НГТУ 2014. — 308 С.

4. Никифоров В. Г. Процессуальный и криминалистический аспекты производства судебного следствия: монография/ ЮНИТИ-ДАНА: Закон и право, 2010. — 144 С.

5. Шаталов А.С. Алгоритмизация и программирование расследования преступлений в системе криминалистической методики/ Право. Журнал Высшей школы экономики. 2017. №2. — С. 155-172

References

1. Maksimova E.A.

2. Lyahova O. O. Klassifikaciya sledstvennyh versij // Molodoj uchenyj. — 2018. — №7. — S. 137-138. — URL https://moluch.ru/archive/193/48373/ (data obrashcheniya: 16.09.2018)

3. Korovin N. K. Kriminalistika: uchebnoe posobie/ NGTU 2014. — 308 S.

4. Nikiforov V. G. Processual'nyj i kriminalisticheskij aspekty proizvodstva sudebnogo sledstviya: monografiya/ YUNITI-DANA: Zakon i pravo, 2010. — 144 S.

5. SHatalov A.S. Algoritmizaciya i programmirovanie rassledovaniya prestuplenij v sisteme kriminalisticheskoj metodiki/ Pravo. ZHurnal Vysshej shkoly ehkonomiki. 2017. №2. — S. 155-172

МАКСИМОВА Елена Александровна, кандидат технических наук, доцент, заведующий кафедрой информационной безопасности ФГАОУ ВО «Волгоградский государственный университет». Россия, 400062, г. Волгоград, проспект Университетский, д. 100. E-mail: maksimova@volsu.ru

БАРАНОВ Владимир Витальевич, кандидат военных наук, доцент, заведующий кафедрой информационной безопасности Южно-Российского государственного политехнического университета имени М.И. Платова, 346428, Ростовская обл., г. Новочеркасск, ул. Просвещения, 132. E-mail: baranov.vv.2015@yandex.ru

ЗЯЗИН Валентин Петрович, профессор кафедры информационной безопасности Института кибернетики, ФГБОУ ВО «МИРЭА - Российский технологический университет», 119454 г. Москва, проспект Вернадского, дом 78. E-mail: zval47@yandex.ru

MAKSIMOVA Elena, Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Security, Volgograd State University. Russia, 400062, Volgograd, Universitetsky Avenue, 100. E-mail: maksimova@volsu.ru

BARANOV Vladimir, Candidate of Military Sciences, Associate Professor, Head of the Department of Information Security of the South-Russian State Polytechnic University named after M.I. Platov. 346428, Rostov region, Novocherkassk, str. Enlightenment, 132. E-mail: baranov.vv.2015@yandex.ru

ZIAZIN Valentin, Professor, Department of Information Security, Institute of Cybernetics, FSBEI HE "MIREA - Russian Technological University". 119454, Moscow, Vernadskogo Avenue, 78. E-mail: zval47@yandex.ru