УДК [343.3/.7:004]:31

В. В. МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

СТАТИСТИЧНЕ ДОСЛІДЖЕННЯ ПОКАЗНИКІВ КІБЕРЗЛОЧИННОСТІ: МЕТОДОЛОГІЧНИЙ АСПЕКТ

Розглянуто методологічні особливості аналізу кількісних (статистичних) характеристик кіберзлочинності в Україні з урахуванням особливостей цього виду злочинності як об'єкта статистичного аналізу, чим і визначається актуальність теми. Проведено аналіз сучасних методологічних аспектів статистичного аналізу стану і динаміки злочинності та відзначено особливості, які повинні бути враховані при вирішенні таких завдань з урахуванням специфіки кіберзлочинності. Обґрунтовано і запропоновано використання адаптивних і узагальнених моделей, що дозволить проводити аналіз стану кіберзлочинності з урахуванням факторів, що впливають на її формування.

Ключові слова: *кіберзлочинність, статистичний аналіз, адаптивна модель, узагальнена модель кіберзлочинності, фактор.*

У зв'язку з поширенням застосування у всіх сферах людської діяльності сучасних інформаційних технологій відбувається значне зростання кількості кіберзлочинів, проблема розкриття яких сьогодні є однією з найактуальніших у сфері правоохоронної діяльності.

Ефективна боротьба з кіберзлочинністю неможлива без розробки цілісної концепції основ кримінологічного та статистичного вивчення злочинності, що включає в себе загальні методологічні, окремі методичні основи дослідження кіберзлочинності, подальшого прогнозування її стану і динаміки.

Першочерговим завданням таких досліджень має стати встановлення соціально-економічних, кримінально-правових та інших причин та умов існування кіберзлочинності й розробка на їх основі найефективніших запобіжних заходів. Усе це актуалізує завдання пошуку, розробки та ефективного використання нових кримінологічних комп'ютерних систем і технологій, заснованих на сучасних математичних, статистичних, соціально-економічних та інших методах.

Вирішення таких завдань можливе тільки за умови належної організації аналітичної роботи в підрозділах органів внутрішніх справ, яка насамперед пов'язана з аналізом і оцінкою оперативної обстановки, що склалася на території обслуговування відповідного органу внутрішніх справ.

Важливу роль у цьому процесі відіграє інформаційно-аналітичне забезпечення аналізу стану та динаміки розвитку злочинності [1], яке дозволяє контролювати внутрішні зв'язки між різними видами злочинності і показниками динаміки її розвитку. Таке дослідження особливо важливе для розуміння механізму формування злочинності і вироблення заходів щодо її попередження.

Ключове місце в аналізі злочинності займає аналіз її стану, структури і тенденцій розвитку. Саме якісно-кількісна характеристика злочинності є відправною точкою кримінологічного дослідження. Не знаючи масштабу даного виду злочинів, складно що-небудь говорити про причини, наслідки та необхідні заходи боротьби і профілактики.

Слід підкреслити, що якісну (кримінологічну) характеристику кіберзлочинності докладно розглядали у своїх дослідженнях В. О. Голубєв [2], Б. Уорлі (B. Worly) [3], Д. Л. Шайндер (D. L. Shinder), Д. Чирило (J. Chirillo), Д. Шрейн та ін.

Методики кількісного (статистичного) аналізу злочинності відомі і розроблені давно [4], однак стосовно дослідження показників, що характеризують кіберзлочинність, не завжди є ефективними і вимагають переробки й уточнення. Так, наприклад, проведені в цей час дослідження показників, що характеризують динаміку розвитку злочинів у даній сфері, зводяться до обчислення найпростіших показників динаміки, зокрема таких, як абсолютний приріст і темп росту, чого, на наш погляд, недостатньо для виявлення довгострокових тенденцій розвитку.

Таким чином, метою даної роботи є розгляд особливостей методології аналізу кількісних (статистичних) характеристик кіберзлочинності в Україні. Виявлення цих особливостей дозволить підвищити ефективність діяльності працівників правоохоронних органів щодо попередження кіберзлочинності.

На нашу думку, повне кількісне вивчення кіберзлочинності в даний час вкрай утруднено через відсутність достовірної статистичної інформації про всі її фактичні показники, що обумовлено високою латентністю окремих видів злочинності.

Так, обсяг фінансових втрат, викликаних діями кіберзлочинців, і кількість скоєних ними правопорушень не піддаються реальній оцінці, оскільки не можна з упевненістю вважати коректними цифри, отримані шляхом обробки результатів проведених вибіркових опитувань. До речі, цей недолік може стосуватися не тільки даних про збитки, але й кількості зафіксованих правопорушень. Незрозумілим залишається і те, який відсоток потерпілих заявляють про вчинені проти них кіберзлочини. Хоча правоохоронні органи, які ведуть боротьбу з кіберзлочинністю, закликають її жертв повідомляти про факти вчинення злочинів, існує думка, що деякі з них, особливо у фінансовому секторі (тобто банки), все ж не розкривають таку інформацію через можливість заподіяння шкоди їхній репутації поширенням негативних відомостей подібного роду. Крім того, користувачі, які піддаються таким атакам, не завжди вірять у здатність правоохоронних органів знайти винних.

Разом з тим не викликає сумнівів той факт, що кількісні характеристики кіберзлочинності можуть дати уявлення про її основні тенденції в тому чи іншому регіоні за певний проміжок часу.

У зв'язку з цим актуальним видається аналіз основних показників, а також причин та умов кіберзлочинності в різних сферах суспільства та економіки, що дозволяє пояснити

існування і подальший розвиток злочинності даного напрямку.

Зазначимо, що аналіз показників, які характеризують кіберзлочинність, може здійснюватися як ізольовано (аналіз окремих показників), так і в рамках узагальненої моделі (встановлення зв'язків між окремими показниками і проведення аналізу з урахуванням виділених зв'язків).

Для проведення аналізу окремих показників кіберзлочинності, на наш погляд, необхідно враховувати специфіку формування кіберзлочинності з урахуванням зовнішніх факторів (рівень розвитку інформаційних технологій, число зареєстрованих Internet-користувачів тощо). У зв'язку з цим методи аналізу, засновані на використанні традиційного апарату математичної статистики, є неефективними, і на перший план виходять адаптивні методи обробки даних, які використовуються для роботи в умовах дефіциту і неточності інформації.

Адаптивні методи виявляються корисними в тих випадках, коли є можливість заздалегідь накопичити, а потім обробити інформацію і тим самим усунути початкову невизначеність. З одного боку, вони можуть бути використані для накопичення та обробки інформації, а з іншого боку, – дозволяють отримати ті ж самі результати, минаючи попереднє накопичення інформації. До того ж дані методи дозволяють проводити аналіз з урахуванням пізніших тенденцій.

Разом з тим необхідно відзначити деякі особливості використання цих методів при аналізі показників кіберзлочинності:

– аналіз стану і сформованих тенденцій розвитку злочинності здійснюється на основі статистичних даних, які характеризують велику кількість скоєних і вже розслідуваних злочинів кожного типу. З кіберзлочинами справа йде не так, як з іншими видами: їх здійснюється відносно небагато, а виявляється і розслідується – ще менше. Тому, на наш погляд, існуючу інформацію слід сприймати не як істину, а лише як перше наближення до майбутніх характеристик, які з'являться після накопичення значного досвіду;

– поява нових видів кіберзлочинів призводить до того, що вихідні ряди показників є короткими. Ця проблема істотно обмежує сферу застосування існуючих статистичних методів.

У зв'язку з вищевикладеним більш оптимальним видається аналіз показників у рамках узагальнених моделей. Такі моделі дозволяють проводити аналіз окремих видів кіберзлочинності з урахуванням впливу зовнішніх соціально-економічних факторів, здійснювати виявлення взаємозв'язків між показниками і факторами, що особливо важливо в дослідженні кіберзлочинності як явища.

З побудовою таких моделей необхідно враховувати той факт, що в останні роки з'являється велика кількість нових видів небезпечних діянь, які на даний час не криміналізовані, оскільки їх суспільна небезпека не так очевидна, розтягнута в часі або завдає відносно невеликого матеріального збитку конкретній людині.

Крім цього через високу латентність кіберзлочинності для побудови узагальненої моделі кіберзлочинності та встановлення справжніх масштабів її поширення, на наш погляд, потрібне використання нових методів і джерел одержання інформації (наприклад, контент-аналіз сайтів, що містять злочинні відомості; аналіз структури сайтів за допомогою пошукових систем, аналіз числа відвідувань тих чи інших сайтів, лінгвістичний аналіз псевдонімів хакерів тощо).

Враховуючи вищесказане, статистичний аналіз стану і динаміки розвитку кіберзлочинності слід здійснювати за наступною схемою:

– збір і систематизація даних про різні види кіберзлочинності, її структуру і динаміку ;

– встановлення причинно-наслідкових зв'язків між кіберзлочинністю та факторами, що вона відображає;

– аналіз ізольованих показників кіберзлочинності на основі адаптивних методів;

– побудова узагальнених моделей кіберзлочинності з урахуванням найбільш істотних факторів, що впливають на її рівень;

– моделювання статистичних показників кіберзлочинності на основі виявлених характеристик тенденцій її розвитку.

Необхідно зазначити, що запропонований підхід значно ускладнює виявлення детермінуючих факторів і особливостей характеристики сучасної кіберзлочинності, що викликає необхідність перегляду кримінологічної оцінки її основних показників, розробки системи кримінально-правових та кримінологічних заходів профілактики і протидії.

В результаті аналіз за запропонованою схемою дозволить краще контролювати внутрішні зв'язки між різними видами та показниками кіберзлочинності, що особливо важливо для розуміння її механізму та вироблення заходів щодо її попередження.

Список використаних джерел

1. Гнусов Ю. В. Методологічні аспекти створення інформаційно-аналітичного забезпечення ОВС / Ю. В. Гнусов // Інформатизація вищих навчальних закладів МВС України : матеріали наук.-практ. конф. – Х. : Харк. нац. ун-т внутр. справ, 2006. – С. 175–179.
2. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія / В. О. Голубєв. – Запоріжжя : ЗІДМУ, 2003. – 250 с.
3. Уорли Б. Интернет: реальные и мнимые угрозы : пер. с англ. / Б. Уорли. – М. : КУДИЦ-ОБРАЗ, 2004. – 320 с.
4. Яковлев С. В. Математические методы оценки состояния и прогнозирования преступности / С. В. Яковлев, Ю. В. Гнусов. – Харьков : Ун-т внутр. дел, 1998. – 158 с.

Надійшла до редколегії 11.07.2013

МАРКОВ В. В. СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ПОКАЗАТЕЛЕЙ КИБЕРПРЕСТУПНОСТИ: МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ

Рассмотрены методологические особенности анализа количественных (статистических) характеристик киберпреступности в Украине особенностей данного вида преступности как объекта статистического анализа, чем и определяется актуальность темы. Проведён анализ существующих методологических аспектов статистического анализа состояния и динамики преступности и отмечены особенности, которые должны быть учтены при решении таких задач с учетом специфики киберпреступности. Обосновано и предложено использование адаптивных и обобщённых моделей, что позволит проводить анализ состояния киберпреступности с учетом влияющих на её формирование факторов.

Ключевые слова: *киберпреступность, статистический анализ, адаптивная модель, обобщённая модель киберпреступности, фактор.*

MARKOV V. V. STATISTICAL RESEARCH OF CYBERCRIME'S INDICATORS: METHODOLOGICAL ASPECT

This article is devoted to the analysis of methodological characteristics of quantitative (statistical) characteristics of cybercrime in Ukraine. Relevance of the topic is determined by the characteristics of cybercrime as an object of statistical analysis.

The author believes that the phenomenon of cybercrime is formed under the influence of many rapidly changing factors, which significantly limits the use of the traditional apparatus of mathematical statistics.

It is outlined in the article that the analysis of indicators, characterizing cybercrime, can be realized both alone and as a part of a generalized model.

Attention is also focused on the fact that while accomplishing analysis of some indicators, it is necessary to consider the specifics of cybercrime's formation taking into account external factors (level of information technologies' development, the number of registered Internet-users).

As a result of the research the following conclusions were made: first of all, the lack of comprehensive research and high latency led to inefficiency of the existing methods of statistical analysis of this type of crime; secondly, the existing methods of analysis of isolated indicators do not allow taking into account existing tendencies in forming cybercrime as a phenomenon. Considering this there is a reasonability to use adaptive methods of analysis.

The use of generalized models letting us to analyze the state of cybercrime considering the factors influencing on its formation, is grounded and proposed.

The author suggested a scheme optimizing the process of decision-making during preventive measures against cybercrime as a recommendation to the statistical analysis of cybercrime's state and dynamics.

Keywords: *cybercrime, statistical analysis, adaptive model, generalized model of cybercrime factor.*