УДК 004.056.53+343.3/.7+681.5.015.42

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 4, pp. 363-369

ХАРАКТЕРИСТИКА И ЗНАЧЕНИЕ МЕЖДУНАРОДНОЙ СТАТИСТИКИ КИБЕРПРЕСТУПНОСТИ

В.И. Трапезников

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: comandor1949@yandex.ua

Рассматривается статистика киберпреступности на материалах США с точки зрения ее необходимости для оценки состояния, динамики изменения в количественных и других характеристиках для определения проблемных направлений организации противостояния этому виду преступления. Показана невозможность организации, правильной постановки задачи решения вопроса искоренения киберпреступности для всех участников этой сложной работы без серьезного изучения конкретной статистики этого вида преступления.

Ключевые слова: киберпреступность, статистическая классификация преступлений, латентность киберпреступлений, виктимизация киберпреступлений

Введение

Если количество радиослушателей во всем мире достигло 50 млн. человек только через 38 лет после изобретения радио, а для телевидения этот срок составил 13 лет, то количество пользователей всемирной сети Internet превысило полсотни миллионов всего через 4 года после ее появления. Эффект формирования глобального информационного пространства, придавший мощнейший импульс человеческому прогрессу, одновременно (как, впрочем, и всегда) имел и негативную сторону.

Во второй половине истекшего века развитие общественных и экономических отношений привело к огромному увеличению перерабатываемой информации, вследствие чего возникла необходимость в поиске новых и более эффективных средств хранения, учета, поиска и переработки этой информации, поскольку прежние формы пользования информацией уже не удовлетворяли потребности общества.

Внедрение в управленческие процессы и другие сферы жизни общества электронно-вычислительной техники позволило успешно решить эту задачу, способствовало стремительному развитию научной мысли и успешному решению многих технических и социальных проблем. Но это достижение человечества стало использоваться не только в полезных для общества целях.

Фактически развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу ЭВМ, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасному антисоциальному явлению, получившему распространенное название – киберпреступность.

«Киберпреступность не имеет государственных границ, – следовательно, и усилия по противодействию ей – дело не одного государства. Нужное плодотворное международное сотрудничество многих стран мира, как на государственном уровне, так и на уровне сотрудничества между правительственными организациями и представителями бизнеса в сфере распространения IT-технологий», – цитирует пресс-

центр СБУ слова руководителя отдела кибернетической защиты Директората новых вызовов безопасности Международного секретариата НАТО Сулеймана Анила.

Определения киберпреступности

Большая часть отчетов, рекомендаций и публикаций по вопросам киберпреступности начинаются с определения термина «киберпреступность». Одно общепринятое определение описывает киберпреступность как любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры или сети. Одним из примеров международного подхода является Статья 1.1 Проекта Международной Конвенции по улучшению защиты от киберпреступности и терроризма (CISAC), которая отмечает, что киберпреступностью называются действия в отношении кибернетических систем [1].

В некоторых определениях предприняты попытки учесть цели, намерения при определении киберпреступности как «действий посредством компьютеров, которые либо являются незаконными, либо считаются противоправными некоторыми сторонами и которые могут быть совершены при помощи глобальных электронных сетей» [2]. Эти более точные описания исключают те случаи, когда физическое оборудование используется для совершения обычных преступлений, но они рискуют исключить преступления, которые считаются киберпреступлениями в международных соглашениях, например в «Конвенции о киберпреступности». Например, человек, который создает USB85-устройства, содержащие злонамеренные программы, которые разрушают информацию в компьютере, если устройство к нему присоединено, совершает преступление, которое определяется Статьей 4 Конвенции о киберпреступности Совета Европы. Однако действие по удалению данных с использованием физического устройства для копирования злонамеренного кода не совершается по глобальным электронным сетям и не может быть квалифицировано как киберпреступление в соответствии с вышеприведенным узким определением. Это действие было бы квалифицировано как киберпреступление только в соответствии с определением, основанным на более широком описании, включающем такие действия как незаконное искажение информации. Это показывает, что определение термина «киберпреступность» встречает заметные трудности [1].

Термин «киберпреступность» используется для описания широкого спектра правонарушений, включая традиционные компьютерные преступления, а также сетевые преступления. Поскольку эти преступления во многом отличаются друг от друга, не существует единого критерия, который может включать в себя все действия, упомянутые в проекте Стэнфордской конвенции и Конвенции о киберпреступности, исключая при этом традиционные преступления, которые совершаются с использованием только оборудования. Тот факт, что не существует единого определения «киберпреступности», не должен быть очень важным до тех пор, пока этот термин не используется в качестве юридического термина [1].

Типология киберпреступности

Термин «киберпреступность» включает в себя большое разнообразие преступлений. Признанные преступления охватывают широкий спектр правонарушений, что усложняет разработку системы типологии или классификации для киберпреступности. Одна интересная система приводится в Конвенции о киберпреступности Совета Европы. Конвенция о киберпреступности различает *четыре типа правонарушений*:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
- преступления, связанные с компьютерами;
- преступления, связанные с контентом;
- преступления, связанные с правами собственности.

Эта типология не является полностью последовательной, поскольку она не основана на едином базовом критерии, который бы определял различия между категориями. Три категории сфокусированы на объекте юридической защиты: «Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем»; преступлениях, связанных с контентом; и преступлениях, связанных с правами собственности. Четвертая категория «преступления, связанные с компьютерами» сфокусирована не на объекте юридической защиты, а на методе. Эта непоследовательность приводит к некоторому пересечению между категориями [1]. Кроме того, некоторые термины, которые используются для описания преступных действий (например, «кибертерроризм» или «фишинг»), охватывают действия, которые попадают в несколько категорий. Тем не менее, категории, приведенные в Конвенции о киберпреступности, являются полезной основой для обсуждения явления киберпреступности. [1]

Характеристика статистики киберпреступлений

Борьба с киберпреступностью требует всестороннего подхода. Учитывая, что одни технические меры не могут предотвратить преступлений, важно чтобы органы правопорядка имели право эффективно расследовать и наказывать киберпреступления. Очень трудно количественно оценить влияние киберпреступности на общество. Финансовые потери, обусловленные киберпреступностью, а также число правонарушений оценить очень трудно. Согласно некоторым источникам, потери из-за киберпреступности для предприятий и организаций в Соединенных Штатах Америки достигают 67 миллиардов долларов США (2011г.); однако неясно, оправдана ли экстраполяция примерных результатов исследований. Эта методологическая критика применима не только к потерям, но также и к известным правонарушениям [1].

Трудно измерить число киберпреступлений, поскольку их жертвы могут не всегда сообщать о правонарушениях. Тем не менее, исследования могут помочь в понимании влияния киберпреступности. Более важно, что точное число киберпреступлений в каждый отдельно взятый год – это тенденция, которую можно определить путем сравнения результатов за последние несколько лет.

Одним из примеров является обзор компьютерных преступлений и безопасности 2007 г., выполненный ЦРУ в Соединенных Штатах Америки, в котором помимо иных тенденций анализируется число совершенных преступлений, связанных с компьютерами. Оно основано на ответах, полученных от 494 практикующих экспертов в области компьютерной безопасности из корпораций США, правительственных органов и финансовых организаций США. В исследовании задокументировано множество правонарушений, о которых сообщили респонденты с 2000 по 2007 год. В нем показано, что с 2001 года уменьшился процент респондентов, которые испытывали или видели вирусные атаки или несанкционированный доступ к информации, или проникновение в систему. В исследовании не объяснено, почему такое уменьшение происходит. Однако это снижение числа распознанных правонарушений указанных категорий подтверждается также исследованиями других организаций (в противовес тому, что иногда предполагают средства массовой информации). Аналогичное развитие наблюдается и при анализе статистики преступности, например, статистика преступности Германии показывает, что после пика в 2004 г. количество преступлений, связанных с компьютерами, уменьшилось вплоть до уровня 2002 года [1].

Статистические данные по киберпреступности не позволяют предоставить надежную информацию о масштабе или размерах правонарушений. Эта неуверенность относительно размеров правонарушений, о которых сообщают их жертвы, а также факт невозможности найти объяснение снижению уровня киберпреступности, делают эти статистические данные открытыми для различных интерпретаций [1].

В настоящее время нет достаточного числа доказательств, для того чтобы предсказывать будущие тенденции и ход развития.

Глобальная картина статистики киберпреступности

В 2011 году по меньшей мере 2.3 миллиарда человек или более одной трети от общей численности населения планеты имели доступ к Интернету. Более 60 процентов всех пользователей Интернета находятся в развивающихся странах, причем 45 процентов всех пользователей Интернета составляют лица в возрасте до 25 лет. По оценкам, к 2017 году доступ к мобильному широкополосному Интернету получат до 70 процентов от общей численности населения мира. К 2020 году количество сетевых устройств («Интернет вещей») будет в шесть раз превосходить численность населения, что полностью изменит нынешнее представление об Интернете. В сверхподключенном к сети мире будущего будет трудно представить себе какое-либо «компьютерное преступление», а, возможно, и вообще любое преступление, которое не сопровождалось бы электронными доказательствами, связанными с подключением к интернет-протоколу (IP) [3].

Во многих странах резкий всплеск в количестве подсоединений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах, сокращением расходов в частном секторе и снижением финансовой ликвидности. На общемировом уровне правоохранительные органы в своих ответах на вопросник отмечают рост уровня киберпреступности в связи с тем, что и частные лица, и организованные преступные группы используют новые возможности для совершения преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды. По оценкам, свыше 80 процентов киберпреступлений совершаются в той или иной форме организованной деятельности, со сложившимися черными рынками киберпреступности в области цикла создания вредоносных программ, компьютерных вирусов, управления бот-сетями, сбора персональных и финансовых данных, продажи данных и получения денег за финансовую информацию. Для совершения киберпреступлений более не требуется обладание сложными навыками или знание сложных методов. Особенно в контексте развивающихся стран появилась субкультура молодых людей, занимающихся финансовым мошенничеством при помощи компьютеров, многие из которых начинают заниматься киберпреступностью в конце подросткового возраста [3].

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием содержащейся в компьютере информации, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем. Однако государственные органы и предприятия частного сектора по-разному воспринимают относительный риск и угрозу. В настоящее время статистические данные о преступности, регистрируемые полицией, не являют собой прочной основы для сравнений между странами, хотя такие статистические данные часто важны для разработки политики на национальном уровне. Две трети стран считают свои системы полицейской статистики недостаточными для того, чтобы регистрировать киберпреступность. Показатели киберпреступности, регистрируемые полицией, зависят не столько от непосредственного уровня преступности, сколько от уровня развития страны и специализированных возможностей полиции [3].

Деятельность правоохранительных органов и проведение расследований

Свыше 90 процентов стран-респондентов сообщают, что правоохранительным органам становится известно о деяниях в области киберпреступности из сообщений частных лиц или организаций, ставших жертвами такой деятельности. По оценкам стран-респондентов, полиция получает сообщения о виктимизации в результате киберпреступности в одном проценте случаев или более. В одном глобальном обследовании частного сектора указано, что 80 процентов частных лиц, ставших жертвами киберпреступности, в полицию о преступлении не сообщают. Тот факт, что люди редко обращаются в полицию, объясняется тем, что они не знают о виктимизации и о механизмах сообщения информации, ощущают стыд или неловкость в связи с тем, что они стали жертвами преступников, а корпорации опасаются возможного репутационного риска.

Государственные органы стран всех регионов мира сообщают об инициативах, направленных на повышение уровня представления информации о совершении преступлений, в том числе о системах, позволяющих сообщать о преступлениях по Интернету и горячим телефонным линиям, кампаниях по повышению информированности общественности, контактах с частным сектором и активизации информационно-пропагандистской деятельности полиции и обмене информацией. Однако меры борьбы с киберпреступностью, принимаемые в порядке реагирования на совершенные преступления, должны сопровождаться среднесрочными и долгосрочными тактическими расследованиями в отношении рынков преступности и разработчиков преступных схем.

Виктимизация – это сложный процесс, который может включать в себя несколько этапов. Первый из них – первичная виктимизация, включает в себя взаимодействие между преступником и жертвой в процессе совершения преступления, а также последствия этого взаимодействия или самого преступления. Второй этап – реакция жертвы на преступление, в том числе возможные изменения в самовосприятии, а также формальные меры, которыми жертва может отреагировать на преступление. Третий этап – последующие взаимодействия жертвы с другими людьми, в том числе с представителями правоохранительных органов, к которым она может обратиться. Если это взаимодействие тоже оказывает негативный эффект на жертву, его называют повторной виктимизацией [4].

Правоохранительные органы развитых стран работают в этой области, в том числе используя действующие под прикрытием подразделения по выявлению правонарушителей на сайтах социальных сетей, в чатах и при обмене мгновенными сообщениями и пользовании материалами совместного пользования. Трудности при расследовании киберпреступлений связаны с использованием преступниками новаторских преступных методов, сложностями в получении доступа к электронным доказательствам и с внутренними ограничениями в отношении ресурсов, потенциала и материально-технических возможностей. Подозреваемые часто используют технологии анонимизации и запутывания следов, и новые технологии быстро получают распространение в преступном мире благодаря онлайновым преступным рынкам.

Выводы. Зачем нужна статистическая классификация преступлений?

Классификация преступлений для статистических целей, в первую очередь, необходима для организованного сбора данных о преступлениях в рамках информационно-аналитической работы. Классификация преступлений позволяет эффективно и упорядоченно структурировать данные по всем видам преступлений, подразделяя их на несколько категорий, что отчасти напоминает концептуально-аналитическую деятельность и работу, связанную с вопросами политики [5].

Стандартная классификация преступлений для статистических целей является важным инструментом для улучшения сопоставимости и повышения качества данных на национальном и международном уровнях [5].

На национальном уровне классификация данных позволяет лучше систематизировать информацию об отдельных правонарушениях, предусмотренных нормативно-правовыми документами, которую обычно трудно использовать в аналитических целях. Классификация также может служить важнейшим средством согласования деятельности по сбору и распространению данных, проводимой различными органами уголовного правосудия (полицией, прокуратурой, судами и тюрьмами) и органами субнационального уровня, которые могут использовать различные нормативно-правовые базы и организационные принципы, а также деятельности по сбору и распространению данных из различных источников (административных документов и статистических обследований). Благодаря общей классификации данных о преступности и уголовном правосудии уровень согласованности национальных данных повышается [5].

На международном уровне использование статистической классификации преступлений необходимо для улучшения сопоставимости данных о преступности по странам, что имеет важность для повышения эффективности анализа тенденций и ситуации в целом на глобальном и региональном уровнях. Несмотря на то, что на пути обеспечения высокой степени сопоставимости данных по странам сохраняются другие проблемы (различия в методах регистрации преступлений, правилах учета, технических и организационных возможностях и т.д.), использование согласованных подходов, общей терминологии и единых критериев является важным шагом в сторону улучшения сопоставимости статистических данных.

Было отмечено, что есть с трудом поддающиеся статистическому учету преступления, в их числе киберпреступность, или компьютерные преступления, которые охватывают различные правонарушения, такие как незаконный доступ к компьютерным данным и системам (хакерство), размещение запрещенного контента (например, детской порнографии или ксенофобских материалов), нарушение авторских прав и другие компьютерные правонарушения (такие как интернет-мошенничество в целях хищения личных данных или кража цифровых персональных данных). Во всех случаях качество данных, полученных из административных документов, страдает из-за низкого уровня их регистрации и выявления по таким причинам, как отсутствие прямых жертв (как в случае с нарушением авторских прав), существование современных систем для сокрытия следов преступления и личности преступников, нежелание жертв сообщать о преступлении из-за опасения возможных негативных последствий (как, например, в случае хакерской атаки против какого-либо финансового учреждения) [5].

Говорить о статистике киберпреступности в Украине на уровне международных требований к сожалению невозможно, так как ее латентность (*латентная преступность* (от лат latens / latentis - скрытый; англ. latens criminality) - уголовно наказуемые деяния, не ставшие известными государственным правоохранительным органам в течение определенного периода времени на определенной территории и не отраженные в официальной уголовной статистике).

Наказуемые деяния, которые не были зафиксированы вообще, относятся к *абсолютной латентной преступности*. Относительную латентную преступность составляют уголовно наказуемые деяния, которые жертва, преступник или третье лицо воспринимают как преступление, но не заявляют о нем в правоохранительные органы [6] практически достигает 90%, а то и более. Это серьезное упущение в работе всех правоохранительных органов нашего государства, которое не дает возможность увидеть все проблемы киберпреступности.

Специалисты НАТО считают, что Украина является уязвимой не только извне, внутренняя опасность существует также. Специалисты отмечают, что для эффективной борьбы с кибер-угрозами в Украине вначале необходимо принять соответствующие законы [7].

Список литературы

1. Понимание киберпреступности: Руководство для развивающихся стран // Отдел приложений ИКТ и кибербезопасности. Департамент политики и стратегии. Сектор развития электросвязи МСЭ. – Проект. Апрель 2009 г. – 228 с.
2. Hale, C. Cybercrime: Facts & Figures Concerning this Global Dilemma [Электронный ресурс] / C. Hale // CJI. – 2002. – Vol. 18. Режим доступа: http://www.cjimagazine.com/archives/cji4411.html?id=37
3. Осипенко, А. Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография / А.Л. Осипенко. – М.: Норма, 2004. – 432 с.
4. Криминология: учебник / под ред. В.Н. Булгакова и Н.М. Кропачева. – СПб.: Изд-во СПбГУ, 2005. – 520 с.
5. E/CN.3/2013/11. Доклад Национального института статистики и географии Мексики и Управления Организации Объединенных Наций по наркотикам и преступности о программе по повышению качества и доступности статистических данных о преступности на национальном и международном уровнях: Пункт 3(j) предварительной повестки дня: Пункты для обсуждения и принятия решения: статистика преступности [Электронный ресурс]/ Записка Генерального секретаря // Организация Объединенных наций. Экономический и социальный совет. – Сорок четвертая сессия 26 февраля - 1 марта 2013 года. – 40 с. Режим доступа: http://unstats.un.org/unsd/statcom/doc13/2013-11-CrimeStats-R.pdf
6. Українські реферати [електронний ресурс]. Режим доступу: refine.org.ua/pageid-11300-1.html
7. СБУ отрабатывает с НАТО механизмы борьбы с киберпреступностью [Электронный ресурс]. Режим доступа: http://za.zubr.in.ua/2011/10/18/13536/

ХАРАКТЕРИСТИКА ТА ЗНАЧЕННЯ МІЖНАРОДНОЇ СТАТИСТИКИ КІБЕРЗЛОЧИННОСТІ

В.І. Трапезніков

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: comandor1949@yandex.ua

Розглядається статистика кіберзлочинності на матеріалах США з точки зору її необхідності для оцінки стану, динаміки зміни у кількісних та інших характеристиках для визначення проблемних напрямів організації протистояння цьому виду злочину. Показано неможливість організації, правильної постановки задачі вирішення питання викорінення кіберзлочинності для усіх учасників цієї складної роботи без серйозного вивчення конкретної статистики даного виду злочину.

Ключові слова: кіберзлочинність, статистична класифікація злочинів, латентність кіберзлочинів, віктимізація кіберзлочинів

CHARACTERISTIC AND IMPORTANCE OF INTERNATIONAL CYBER CRIME STATISTICS

V.I. Trapeznikov

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: comandor1949@yandex.ua

Cyber crime statistics is discussed based on the sources from the USA from the standpoint of its importance in assessing the crime status and trends (involving quantitative and other indicators) and to determine the most problematic areas in combating these crimes. It is shown that without thorough investigation of the statistics of cyber crimes, it is impossible to organize the participants of combat actions and to state their tasks in a proper way for elimination of these crimes.

Keywords: cyber crimes, statistical classification of crimes, latency of cyber crimes, victimization of cyber crimes.