УДК 81

К ВОПРОСУ О ТЕРМИНОЛОГИИ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ (на материале английского языка)

Крылов Д.О., Малюгина А.В.
Воронежский институт МВД, Россия

TERMINOLOGY IN THE FIELD OF CYBERCRIME (based on the English language material)

Krylov D.O., Malyugina A.V.
Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation

Одним из наиболее растущих видов преступлений в настоящее время является киберпреступность, которая характеризуется совершением преступных деяний с помощью информационных технологий. Общемировая тенденция активизации различной криминальной активности в киберпространстве обусловлена хранением в нем огромного объема данных и легкостью совершения такого рода преступлений. Количество кибератак и суммы ущерба растут ежегодно. В 2015 общемировой ущерб от киберпреступлений оценивают в 158 млрд. долларов. Необходимость развития компетенции сотрудников правоохранительных органов для борьбы с киберпреступностью связана, прежде всего, с формированием высоких навыков в сфере информационных технологий, а также овладением соответствующей специальной английской терминологией, позволяющей узнать историю, особенности возникновения киберпреступности, проанализировать методы, которыми пользуются зарубежные коллеги в борьбе с преступлениями, совершаемыми в виртуальном пространстве.

One of the most growing crimes in the modern time is the cybercrime characterized by the commitment of crimes carried out by means of information technologies. The global trend of expanding criminal activity in cyberspace is conditioned by the storage of huge amount of data in the cyberspace and easiness of committing such crimes. The number of cyber attacks and their damages are growing annually. In 2015 the global damage of cybercrime was estimated at 158 billion. Law enforcement agencies are bound to develop competences enabling them to fight against cybercrime. These competences are connected primarily with the formation of high IT skills as well as the study of the relevant English terminology, allowing to learn the history and features of the emergence of cybercrime, analyze the methods used by foreign counterparts in the fight against crimes in the virtual space.

Ключевые слова и фразы: виртуальное пространство, киберпространство, киберпреступность, высокотехнологичная преступность, хакерство.
Key words: virtual space, cyberspace, cybercrime, advanced cybercrime, hacking.

В современном мире люди все чаще начинают взаимодействовать с виртуальной реальностью, или киберпространством. Термин «киберпространство», возникший на основе сочетания слов: кибернетика (наука об общих закономерностях получения, хранения, передачи и преобразования информации в сложных управляющих системах, будь то машины, живые организмы или общество), [6] и пространство - впервые был использован Уильямом Гибсоном, канадским писателем-фантастом в начале 1982г. в новелле «Сожжение Хром» («Burning Chrome»). Киберпространство описывает виртуальное пространство, в котором циркулируют электронные данные всех компьютеров мира [3].

В настоящее время создаются многочисленные программы и приложения для взаимодействия человека с этим миром. Виртуальная реальность содержит огромный объем

различной информации. По итогам 2015 года глобальная численность пользователей интернета составила более 3,2 миллиардов человек [4]

Человек хранит все больше данных в киберпространстве: от личных сведений до государственных тайн. В этой связи неудивительно, что в последние 30 лет сложилась общемировая тенденция активизации различной криминальной активности в киберпространстве, для которой характерно совершение преступных деяний с помощью компьютера или смартфона. Такой вид преступлений называется киберпреступностью от английского *cybercrime*.

Ежегодно количество кибератак и суммы ущерба растут в геометрической прогрессии. Причины этого печального явления связаны с прибыльностью и легкостью совершения такого рода преступлений. Вооруженное нападение требует значительных затрат времени, финансов и тщательной подготовки, а малейший сбой почти неминуемо ведет к провалу всей операции. А вот кибермошенничество может быть успешным и тогда, когда операция пошла не совсем так, как первоначально задумывалась. В этих условиях возможна постановка другой задачи. Важно и то обстоятельство, что для преступных посягательств используются простые и довольно дешевые инструменты. Для работы с бот-сетью (от англ. *botnet*), имеющей различные боты - программы, скрытно устанавливаемые на устройство жертвы, и позволяющей злоумышленнику выполнять действия с использованием ресурсов заражённого компьютера [2], - не нужно ничего, кроме обычного персонального компьютера с доступом в интернет.

Суммы, которые можно украсть с помощью различных ИТ-средств те же, что и при «традиционной» преступности, а часто и больше. Так на 2015 год, по итогам исследования Symantec, общемировой ущерб от киберпреступлений составил 158 млрд. долларов. Согласно отчету компании, жертвами таких преступлений стали 594 млн. человек. В России в 2015 году, по оценке специалистов, был нанесен ущерб минимум на 1 млрд. долларов [5].

Учитывая возрастающую актуальность борьбы с киберпреступностью для правоохранительных органов и иностранное происхождение термина «киберпреступность», цель настоящей статьи состоит в изучении английских лексических единиц, связанных с преступной деятельностью, совершаемой в виртуальном пространстве, анализе различных видов киберпреступлений посредством изучения семантического значения вербализующих их английских лексем и словосочетаний.

Первый вопрос, который возникает при рассмотрении такого рода лексем, касается их написания. Оказалось, что в англоязычных источниках по вопросу киберпреступности написание релевантных английских терминов разнится. Так, например, на сайте ФБР среди направлений, которыми занимается агентство (*What we investigate*) указано *cyber crime,* а на

официальном сайте Интерпола читаем: *"Cybercrime is a fast-growing area of crime" (Киберпреступность является быстро развивающимся преступным направлением).* В большинстве толковых анлоязычных словарей, однако, например, в Кратком оксфордском словаре английского языка Concise Oxford English vocab, в кембриджском словаре английского языка Cambridge Dictionary имеет место слитное написание - *cybercrime*.

Английская терминология преступлений, совершаемых в виртуальном пространстве, кроме ключевой лексемы *cybercrime,* также включает следующие лексемы с корнем *cyber*: *cyberwar - кибервойна, cyberattack - кибератака, cyberterrorism - кибертерроризм, cybercriminal – киберпреступник, cybersecurity – кибербезопасность и др.*

В разделе «Киберпреступность» на сайте Интерпол отмечается, что, хотя и не существует единого универсального определения термина «киберпреступность», правоохранительные органы, как правило, различают два основных вида интернет-преступлений:

advanced cybercrime - *высокотехнологичная преступность,* представляющая собой изощренные атаки на аппаратные средства компьютера и программное обеспечение,

cyber-enabled crime - преступность, использующая виртуальное пространство для совершения многих "традиционных" преступлений таких, как преступления против детей, финансовые преступления, кражи, мошенничество, незаконные азартные игры, продажа поддельных лекарств и даже терроризм. В этом случае речь идет о новых возможностях совершения преступлений онлайн, которые становятся все более массовыми и разрушительными [7].

Рассмотрим английские термины, описывающие различные типы киберпреступлений.

Hacking / Хакерство. Это преступление, в котором преступник использует различное программное обеспечение для доступа к личным или конфиденциальным данным человека, не подозревающего, что к его компьютеру имеют удаленный доступ. В Соединенных Штатах хакерство классифицируется как уголовное преступление и карается по закону.

Theft / Кража данных. Это преступление связано с нарушением авторских прав и незаконным использованием файлов для скачивания музыки, фильмов, игр и программного обеспечения. К сожалению, в настоящее время есть сайты, такие как Trekker(Torrent), которые поощряют пиратство программного обеспечения, и многие из этих веб-сайтов в настоящее время являются мишенью ФБР. Сегодня существуют законы, которые наказывают людей за незаконное скачивание.

Cyberstalking / Киберпреследование. Это своего рода онлайн-домогательство, в котором жертва подвергается шквалу интернет-сообщений и сообщений электронной

почты. Как правило, сталкеры знают своих жертв, и вместо того, чтобы прибегать к личному выслеживанию, они используют для слежки интернет.

Identity theft / Хищение личных данных. Данный вид киберпреступления стал одной из главных проблем для людей, использующих интернет для совершения кассовых операций и использования банковских услуг. Преступник, получая доступ к данным о банковском счете человека, кредитных картах, социальном обеспечении, дебетовым картам и другой конфиденциальной информации, перекачивает деньги или покупает вещи в интернете, используя имя жертвы.

Malicious Software / Программные средства, нарушающие нормальную работу системы. Совершая такое преступление, преступник использует особое программное обеспечение для того, чтобы нарушить работу сети.

Child soliciting and Abuse / Домогательство и жестокое обращение с ребенком. Это также тип киберпреступности, в котором преступники общаются с несовершеннолетними через чаты с целью получения детской порнографии. ФБР тратит много времени на мониторинг чатов, посещаемых детьми, с надеждами на сокращение и предотвращение этого вида преступлений.

Проведенное исследование показало, что темпы развития киберпреступности поражают своей стремительностью и широким распространением. Неслучайно созданы специальные ведомства по борьбе с кибер-преступностью. В России это Управление «К» МВД РФ, а в США -Министерство внутренней безопасности США, Национальное подразделение по компьютерной безопасности. Для сотрудников правоохранительных органов России важно не только обладать высокими навыками в сфере информационных технологий для оказания эффективного противодействия киберпреступности, но и, прежде всего, владеть соответствующей специальной английской терминологией, позволяющей узнать историю, особенности возникновения киберпреступности, проанализировать методы, которыми пользуются зарубежные коллеги в борьбе с преступлениями, совершаемыми в виртуальном пространстве.

Литература:

1. Борьба с киберпреступностью [Электронный ресурс] URL: https://71.мвд.рф/Dejatelnost/Borba_s_kiberprestupnostju (дата обращения: 24.12.2016).
2. Ботнет. Как создаются ботнеты. Средства защиты от ботнетов [Электронный ресурс] URL: http://www.windxp.com.ru/articles29.htm (дата обращения: 24.12.2016).
3. Гринберг А.С. Информационный менеджмент [Электронный ресурс] URL: http://www.ngpedia.ru/pg6384876uMBWtVn0001082137/ (дата обращения: 24.12.2016).

4. МСЭ публикует данные по ИКТ за 2015 год [Электронный ресурс] URL: http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf (дата обращения: 24.12.2016).
5. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений [Электронный ресурс] URL: https://e-koncept.ru/2016/96090.htm (дата обращения: 24.12.2016).
6. Энциклопедия кибернетики под ред. В.М. Глушкова, т.1., Киев, 1974.- с. 440.
7. Cybercrime [Электронный ресурс] URL: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (дата обращения: 24.12.2016).