Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы используются во всех сферах жизнедеятельности человека и государства — от решения проблем национальной безопасности, здравоохранения и управления транспортом до торговли, финансов, и даже просто межличностного общения. Человек всегда был уязвим, но недавно мы узнали, что беззащитны вдвойне — не только в реальной жизни, но и в мире, о котором три десятка лет назад не знали ничего — виртуальном мире, киберпространстве, в мире, моделируемом с помощью компьютеров. Человек поставил себе на службу телекоммуникации и глобальные компьютерные сети, не предвидев, какие возможности для злоупотребления создают эти технологии. Сегодня жертвами преступников, орудующих в виртуальном пространстве, могут стать не только отдельные люди, но и целые государства. При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете.

Эти проблемы волнуют и Европу, и Северную Америку, и Россию. Если в 1996 г. в России было выявлено 15 компьютерных преступлений, то в 1997-м — уже 101, причем размер понесенного ущерба достиг 20 млрд руб. А за пять лет количество подобных преступлений выросло в 33 раза — в 2002 г. в России зарегистрировано 3 371 преступление в области компьютерной информации. Об этом в ходе всероссийской конференции «Информационная безопасность России» сообщил начальник Главного управления специальных технических мероприятий МВД РФ Борис Мирошников. По его словам, из числа зарегистрированных правонарушений в области компьютерной информации, свыше 90% составляют преступления, связанные с незаконным доступом к информационным ресурсам, так называемые «компьютерные взломы». Большая часть киберпреступле-ний остается скрытой и не регистрируется правоохранительными органами. Процентное соотношение раскрытых и нераскрытых правонарушений пока установить не удается.

К сожалению, в российской специальной литературе практически не освещена проблема киберпреступности как следствия глобализации информационных

процессов. Этот пробел еще предстоит восполнить. России также не оказалось среди государств, подписавших в ноябре 2001 г. Конвенцию Совета Европы о киберпреступности. И если эта конвенция является продуктом четырехлетнего труда, т.е. мировое сообщество уже полдесятилетия озабочено данной проблемой, то наша страна пока, увы, не готова ни к подписанию данной конвенции, ни к международному сотрудничеству в этой области. Однако, справедливо будет упомянуть, что и международное сообщество тоже пока находится не только в поиске методов борьбы с этой проблемой, но и в процессе выработки единой политики по данному вопросу, в том числе понятийного аппарата. Преступность в виртуальном пространстве — новое для нас явление, но часть преступлений, совершаемых в сфере высоких технологий, — это привычные нам с незапамятных времен кражи, мошенничества, вымогательство. Поэтому для исследования проблемы киберпреступности необходимо дать корректные определения таким явлениям, как виртуальное пространство, киберпреступность, компьютерные преступления, кибертерроризм, чтобы отграничить их друг от друга и от смежных понятий.

Киберпреступность — это преступность в так называемом виртуальном пространстве. Виртуальное пространство можно определить как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.

Это определение соответствует рекомендациям экспертов ООН. По их мнению, термин «киберпреступность» подразумевает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. Преступление, совершенное в киберпространстве, — это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.

Спорным вопросом является ограничение понятия киберпреступлений рамками «всемирной паутины». Согласимся с мнением А. Щетилова: понятие киберпреступности включает в себя не только деяния, совершенные в глобальной сети Интернет. Оно распространяется на все виды преступлений, совершенных в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, информационная техника могут выступать (являться) предметом (целью) преступных посягательств, средой, в которой совершаются правонарушения, и средством или орудием преступления.

Как соотносятся понятия «киберпреступность» и «компьютерные преступления»? Конвенция Совета Европы говорит о четырех типах компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

• незаконный доступ — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);

• незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

• вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

• вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

На наш взгляд, именно эти четыре вида преступлений являются собственно «компьютерными», остальные — это либо связанные с компьютером (computer-related), либо совершаемые с помощью компьютера (computer-facilitated) преступления. К ним относятся:

• преступления, в которых компьютер является орудием (электронные хищения, мошенничества и т.п.);

• деяния, при совершении которых компьютер является интеллектуальным средством (например, размещение на сайтах детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду и т.д.).

Последние два вида киберпреступлений являются объектом дискуссий. Некоторые зарубежные исследователи, к примеру, полагают, что данные преступления — не более чем противоправные деяния, совершенные с помощью современных средств, они охватываются составами в национальных уголовных кодексах и не являются новыми категориями преступлений. Другие полагают, что киберпреступления — качественно новая категория преступлений, требующая принятия новых норм, освоения новых методов расследования, подразумевающая международное сотрудничество в борьбе с этим явлением. Думаем, правы и те, и другие. Действительно, компьютерные мошенничества, кражи, вымогательства, размещение в Интернете порносайтов и другие подобные преступления не являются новыми видами противоправных деяний, их составы включены в национальное уголовное законодательство. Например, кража является преступлением против собственности, и совершение ее с помощью компьютера не образует нового состава, но средства, с помощью которых совершено это преступление, действительно требуют разработки новых норм закона и освоения новых методов расследования. Это обусловлено тем, что киберпреступления (в том числе кражи, мошенничество, вымогательство в киберпространстве) зачастую выходят за рамки обычных составов, не признают государственных границ (транснациональны), кроме того, их «виртуальный» характер позволяет быстро уничтожить следы, что значительно затрудняет поиск преступника.

Заключение

К сожалению, многие средства массовой информации употребляют термин «кибертерроризм» весьма некорректно, создавая путаницу в понятиях, ставя знак равенства между понятием «хакер» и «кибертеррорист». Вряд ли это можно считать правильным. Терроризм — это преступление, но не каждое преступление есть терроризм, точно так же, как кибертеррориста, как правило, можно назвать хакером, но не всякий хакер совершает теракты в киберпространстве или с помощью компьютера. Именно корректное определение того или иного явления позволяет увидеть его суть и, если это явление имеет негативные последствия, то выявить формы и методы борьбы с ним. Таким образом, первым шагом в борьбе с киберпреступностью и ее опаснейшей разновидностью — кибертерроризмом — на наш взгляд, должно стать создание корректного понятийного аппарата.