Должностные лица, занимающиеся взаимопомощью, обязаны досконально разбираться в законодательстве и таможенной деятельности, иначе возникновение большого количества ошибок приведет к неэффективному сотрудничеству. Автор предлагает таможенным службам и администрациям разработать руководство по взаимопомощи, которое могло бы состоять из основных знаний и советов для подготовки запросов о помощи и сотрудничестве.

Таким образом, международное сотрудничество и взаимопомощь являются неотъемлемой частью сегодняшней деятельности таможенных служб, что позволяет не только проводить всестороннее расследование нарушений таможенного законодательства и надлежащего применения, но также является одним из предварительных условий надежного управления рисками и физического контроля. В целях эффективной работы таможни ЕС и государства-члены заключили множество соглашений в области таможенного сотрудничества и взаимопомощи. Это форма сотрудничества, которая ежедневно успешно применяется. Считается полезным подготовить практическое руководство по всем аспектам международного таможенного сотрудничества и взаимопомощи для таможенных служащих и других лиц, заинтересованных в возможностях таможенного сотрудничества.

УДК 343

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Караваев Д. А.
Учреждение образования «Белорусский институт правоведения»
e-mail: deniskarav@gmail.com

Summary. *Every step of a modern person is shrouded in a shell of information technology. Most people don't start their day with breakfast, but by checking their email or social media. All of the above is a fertile environment for the commission of crimes in the field of digital information. This is what will be discussed in this article. This article will examine the types of crimes, as well as responsibility for them.*

Уголовный кодекс предусматривает ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

Статья 212. Хищение путем использования компьютерной техники.

Ответственность за деяния, предусмотренные ст.212, наступает с 14-летнего возраста.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. В последнее время все чаще фиксируются факты хищений с использованием реквизитов карт при осуществлении Интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

Статья 349. Несанкционированный доступ к компьютерной информации.

К примеру, несанкционированный доступ к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

Статья 350. Модификация компьютерной информации.

В качестве примера можно привести произведенные изменения компьютерной информации: переписка в электронной почте, в мессенджере с правами другого пользователя; изменение текстовой, графической и иной информации; внесение изменений в защищенные базы данных и т.д.

Статья 351. Компьютерный саботаж.

Здесь можно упомянуть умышленное уничтожение компьютерной информации: удаление, приведение в непригодное состояние, шифрование.

Статья 352. Неправомерное завладение компьютерной информацией.

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации, повлекшие причинение существенного вреда. К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами фотографий с компьютера.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов, например, поддельных смарт-карт для просмотра закодированных каналов спутникового телевидения.

Статья 354. Разработка, использование либо распространение вредоносных программ.

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например, блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.

Указанная статья применяется к лицам, имеющим доступ к компьютерным сетям и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем.

Ответственность за деяния, предусмотренные ст.ст.349-355 наступает с 16-летнего возраста.

Также с использованием сети Интернет может совершаться ряд иных уголовно наказуемых противоправных деяний:

- Мошенничество (ст.209 УК);
- Причинение имущественного ущерба без признаков хищения (ст.216 УК);
- изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343 УК, ст.343-1 УК);
- Клевета (ст.188 УК);
- Оскорбление (ст.189 УК);
- Разжигание расовой, национальной или религиозной вражды, или розни (ст.130 УК) и иные.

В Республике Беларусь наблюдается отчетливая тенденция роста количества фактов совершения противоправных деяний в сети Интернет, которые выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем мошенничества либо использования компьютерной техники. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.