УДК 343

К. А. Белаш
Учреждение образования «Барановичский государственный университет», Барановичи

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение. Существование современного мира немыслимо без информационных технологий. На сегодня информация является важнейшей ценностью как для общества в целом, так и отдельной личности в частности. Информация присуща всем сферам жизнедеятельности человека. Информационные технологии представляют собой огромные возможности для упрощения и улучшения жизни современного общества. Цифровой мир развивается стремительно. Одновременно с цифровой трансформацией экономики увеличивается число посягательств со стороны криминального мира на данную сферу. Этот вызов нельзя игнорировать.

На ключевое значение информационных технологий указано и в Концепции информационной безопасности Республики Беларусь: «Информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах». Информационная сфера представляет собой самостоятельную сферу национальной безопасности, в которой необходимо обеспечить защиту информационных ресурсов, систем их формирования, распространения и использования, информационной инфраструктуры, реализацию прав на информацию государства, юридических лиц, граждан [1].

По официальным данным МВД Республики Беларусь, состояние криминогенной обстановки по направлению деятельности подразделений в сфере высоких технологий в январе—декабре 2019 года в сравнении с аналогичным периодом прошлого года свидетельствует о значительном увеличении (в 2,2 раза; с 4 741 до 10 539) количества зарегистрированных киберпреступлений. В первую очередь рост данных деяний обусловлен увеличением количества фактов несанкционированного доступа к компьютерной информации, более ⅔ преступлений (76,4 %, или 8 047; 2018 год — 75,6 %, или 3 585), выявленных в сфере высоких технологий, относятся к хищениям путем использования компьютерной техники [2].

Основная часть. Информационная безопасность является понятием многогранным и комплексным. Она имеет два основных аспекта: содержательный (духовная сфера) и технический (материальная сфера). К первому из них можно отнести содержание и направленность всей циркулирующей информации. Технический аспект — совокупность информационно-телекоммуникационных средств, технологий, систем, предназначенных для создания, хранения, распространения, передачи и обработки информации [3, с. 207].

В частности, Концепцией информационной безопасности Республики Беларусь информационная безопасность определена как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [4].

Концепция информационной безопасности Республики Беларусь дает определение преступлениям в информационной сфере, как предусмотренным Уголовным кодексом Республики Беларусь (далее — УК) преступлениям против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети [4].

В настоящее время термин «киберпреступность» зачастую отождествляют с термином «компьютерная» преступность. К примеру, единственная глава в УК, предусматривающая ответственность за преступления, объектом которых является информация, называется «Преступления против информационной безопасности», а в статьях упоминается компьютерная информация. На самом деле, данные термины очень близки друг к другу, но все же не синонимичны.

Разделение преступности на «компьютерную» и в «киберпространстве» имеет теоретическую и практическую значимость. Для более четкого разграничения данных понятий следует определить их сущность. Относя различные составы главы 31 УК к «компьютерным» преступлениям и «киберпреступлениям», следует делать оговорку об их соотношении, учитывая их специфические признаки, которые определяют исключительные моменты, помогающие разграничить данные понятия. Исходя из этого, формируется понятие термина «киберпреступность» — особый вид преступности, который представляет массовое социально правовое явление, охватывающее совокупность общественно опасных деяний, предусмотренных УК, конвенцией «О киберпреступности» и различными международно-правовыми актами [5, с. 173].

Общественные отношения по поводу обмена информацией были поставлены законодателем под уголовно-правовую охрану путем криминализации деяний, описанных в диспозициях статей главы 31 УК «Преступления против информационной безопасности». К категории таких преступлений действующий УК относит:

«Несанкционированный доступ к компьютерной информации» (ст. 349), «Неправомерное завладение компьютерной информацией» (ст. 352), «Модификация компьютерной информации» (ст. 350) и др. [6].

В названии главы 31 УК четко определен родовой объект рассматриваемых преступлений — информационная безопасность — совокупность общественных отношений, складывающихся в процессе защиты информационных ресурсов и охраны прав субъектов информатизации, а также обеспечения безопасности пользователей и пользования компьютерными системами и сетями. Предметом анализируемых преступлений является компьютерная информация, т. е. содержащиеся на машинных носителях, в компьютерной системе или сети сведения о лицах, предметах, фактах, событиях и явлениях, и компьютер как информационная структура — носитель этой информации. В предусмотренных главой 31 УК преступлениях компьютерная информация как предмет преступления является обязательным признаком состава. Записи компьютерных программ, первичные базы данных и другая подобная информация, исполненная рукой человека, отпечатанная на печатной машинке или набранная типографским способом, т. е. информация, зафиксированная на ином материальном носителе (к примеру, на бумаге), не является предметом преступлений, предусмотренных ст. 349—355 УК [7].

Закон Республики Беларусь «Об информации, информатизации и защите информации» впервые на уровне законодательства определил понятие «защита информации» как комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации [8].

Характеризуя объективную сторону рассматриваемых составов, заметим, что большинство из них конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно опасного деяния, но и наступление общественно опасных последствий, а также установление причинной связи между этими двумя признаками. Для всех преступлений данного вида необходимо наличие вины в форме умысла, три состава предусматривают две ее формы: умысел по отношению к деянию и неосторожность в отношении наступивших общественно опасных последствий. Субъектом рассматриваемых преступлений может стать, в принципе, любой человек. Ответственность за преступления против компьютерной безопасности наступает с 16 лет. Диспозиции статей главы 31 УК описательные, зачастую — бланкетные или отсылочные. Санкции большинства — альтернативные.

Характеризуя преступления в целом, необходимо отметить, что 31 глава УК включает разные категории преступлений, не представляющие большой общественной опасности, менее тяжкие и тяжкие. Разнообразен перечень наказаний, применяемых за совершение преступлений против информационной безопасности. Уголовный кодекс предлагает семь видов наказаний, среди которых общественные работы, штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, исправительные работы, арест, ограничение свободы, лишение свободы [6].

В ст. 349 УК закреплена ответственность за такое преступление, как «Несанкционированный доступ к компьютерной информации». Непосредственным объектом анализируемого преступления является порядок доступа к компьютерной информации, дающий субъекту право на ознакомление с ней. Порядок предоставления доступа к информации регламентируется ее правовым режимом [9, с. 762]. Так как состав исследуемого преступления материальный, то обязательным признаком его объективной стороны является наступление одного из перечисленных в диспозиции вредных последствий, которые по смыслу можно объединить понятием «существенный вред». Поэтому само по себе ознакомление с информацией в результате несанкционированного доступа к ней, не образующее состава другого преступления и не повлекшее этих последствий, преступлением не является [7].

В ст. 350 УК закреплены признаки состава преступления «Модификация компьютерной информации». Под ней понимают изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности, т. е. изменение первоначального содержания файлов, что усложняет либо исключает ее законное использование. Состав данного преступления материальный. В отличие от несанкционированного доступа к компьютерной информации, который может быть совершен также и по неосторожности, это преступление совершается только умышленно.

Определение понятия «компьютерный саботаж» закреплено в ст. 351 УК. Это умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя. Состав компьютерного саботажа — материальный. Отметим, что в указанной статье не перечислены действия, которые могут быть квалифицированы как компьютерный саботаж, следовательно, это могут быть любые действия, которые могут стать причиной уничтожения, блокирования, приведения в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя.

Комментируя ст. 351 УК, В. В. Лосев определил, что под разрушением компьютерной системы необходимо понимать уничтожение всех аппаратных средств этой системы либо отдельных из них, без которых компьютерная система не работает. Термин «разрушение машинного носителя», по его мнению означает полное уничтожение либо такое его повреждение, которое исключает получение информации [7].

Н. Ф. Ахраменка, комментируя ст. 352 УК, считает, что под неправомерным завладением компьютерной информацией следует понимать несанкционированное копирование либо иное неправомерное

завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда. Статья 354 УК предусматривает ответственность за разработку, использование либо распространение вредоносных программ. Предмет преступления — вредоносные компьютерные программы и носители с такими программами [9, с. 769].

Отдельного внимания заслуживает такое преступление, как «Хищение путем использования компьютерной техники», предусмотренное в ст. 212 УК и отраженное в главе 24 УК. Основной состав предусматривает два способа хищения: хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, и хищение путем введения в компьютерную систему ложной информации. Самым распространённым примером, встречающимся в отношении преступлений, предусмотренных ст. 212 УК, является ввод преступником персонифицированного идентификационного номера (ПИН-кода) чужой пластиковой банковской карточки, так как в данном случае хищение происходит посредством компьютерной техники у потерпевшего, который не давал разрешения на производство операций с его банковской карточкой.

Заключение. Республика Беларусь на современном этапе проходит сложный период становления ИТ-технологий. Повсеместное внедрение высоких технологий в нашу повседневную жизнь привело к тому, что информационная безопасность стала не просто важным направлением деятельности заинтересованных субъектов, а необходимым условием обеспечения всех сфер национальной безопасности, политических, экономических, социальных и иных интересов общества и государства. Охрана урегулированных законом правоотношений по поводу обмена и использования информации на различных носителях сегодня обеспечивается положениями уголовного законодательства. Преступления против информационной безопасности являются обособленной в уголовном законодательстве подгруппой более крупного явления — компьютерных преступлений.

В целом УК содержит достаточное многообразие конкретных составов преступлений, что соответствует развитию современного информационного общества. Однако, на наш взгляд, введение новых ИТ-технологий подразумевает и разработку новых мер по их защите для обеспечения их безопасности. Безусловно, нормы о каждом из видов ответственности должны постоянно совершенствоваться и соответствовать современному информационному обществу.

Список цитируемых источников

1. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 9 нояб. 2010 г., № 575 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2020.
2. Министерство внутренних дел Республики Беларусь [Электронный ресурс]. — Режим доступа: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere vysokih-tehnologij-upravlenie-k/statistika-urpsvt . — Дата доступа: 22.05.2020.
3. Национальная безопасность Республики Беларусь / С. В. Зась [и др.] ; под ред. М. В. Мясниковича, Л. С. Мальцева // Беларус. навука. — 2011. — 557 с.
4. Концепция информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2020.
5. Уголовная юстиция: законодательство, теория и практика : сб. науч. ст. / Брест. гос. ун-т ; редкол.: Е. А. Коротич (отв. ред.) [и др.]. — Брест : БрГУ, 2018. — 291 с.
6. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. ; одобр. Советом Респ. 24 июня 1999 г. : изм. и доп. по сост. на 1 февр. 2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2020.
7. Преступления против информационной безопасности : учеб. пособие / В. В. Лосев [и др.] ; под общ. ред. В. В. Коклюхина. — Брест, 2000. — 45 с.
8. *Макаревич, А. В.* Отдельные аспекты правовых мер защиты информации [Электронный ресурс] // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информации Республики Беларусь. — Минск, 2020.
9. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н. Ф. Ахраменка [и др.] ; под общ. ред. А. В. Баркова, В. М. Хомича. — Минск : ГИУСТ БГУ, 2007. — 1007 с.

УДК 339.138

В. А. Василицкая

Учреждение образования «Барановичский государственный университет», Барановичи

СОЦИАЛЬНЫЕ СЕТИ В СИСТЕМЕ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ

Введение. В настоящее время Social Media Marketing (SMM) набирает стремительную популярность, социальные сети активно внедряются в нашу бытовую жизнь, забирая все свободное время. Мы привыкли выбирать, покупать, изучать в Интернете все, что нам интересно. Благодаря этим неизбежным привычкам, продающим компаниям приходится идти в ногу со временем и быть на одной волне с клиентом. Чтобы заслужить лояльность и внимание потребителя, нужно быть современным и соответствовать запросам современности.