1. Об оперативно-розыскной деятельности [Электронный ресурс] : Закон Респ. Беларусь, 15 июля 2015 г., № 307-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Голяндин, Н.П. Взаимодействие оперативно-поисковых подразделений с другими оперативными подразделениями органов внутренних дел в борьбе с преступностью : автореф. дис. ... канд. юрид. наук : 12.00.12 / Н.П. Голяндин ; Акад. МВД России. – М., 1997. – 19 с.

3. Назаров, С.Д. Взаимодействие аппаратов по борьбе с организованной преступностью с другими субъектами оперативно-розыскной деятельности : автореф. дис. ... канд. юрид. наук : 12.00.12 / С.Д. Назаров ; Волгоград. юрид. ин-т МВД России. – Волгоград, 1997. – 22 с.

4. Баландин, Д.А. Взаимодействие оперативных подразделений исправительных колоний Минюста России и органов внутренних дел в борьбе с экономическими преступлениями : автореф. дис. ... канд. юрид. наук : 12.00.12 / Д.А. Баландин ; Акад. упр. МВД России. – М., 2004. – 27 с.

5. Галахов, С.С. Правовые и организационные основы деятельности подразделений специальных технических мероприятий органов внутренних дел и перспективы их развития / С.С. Галахов, В.Н. Копытин ; ВНИИ МВД России. – М., 2003. – 288 с.

6. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

УДК 343.985

Д.В. Гриб

КРИМИНАЛИЗАЦИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ХИЩЕНИЕ, СОВЕРШАЕМОЕ ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Сегодня информация представляет собой один из важнейших ресурсов, способствующих обеспечению функционирования организаций, а также является основой процесса глобализации общественных отношений. Вместе с тем цифровизация общества и государства оказала негативное влияние на рост преступлений в сфере информационных технологий.

В этой связи своевременной реакцией белорусских законодателей стало введение 9 июля 1999 г. в Уголовный кодекс Республики Беларусь (УК) ст. 212 «Хищение путем использования компьютерной техники», которая установила новую форму хищения – использование компьютерной техники. Кроме того, 26 мая 2021 г. внесены изменения в диспозицию ст. 212 «Хищение имущества путем модификации компьютерной информации».

Вместе с тем в ближайшей перспективе аналитики прогнозируют значительный рост числа таких преступлений. В подтверждение данной позиции следует отразить тот факт, что удельный вес регистрируемых преступлений, предусмотренных ст. 212 УК, в структуре преступлений против собственности имеет тенденцию к неизменному росту и составляет уже не менее $^{2}/_{3}$. В частности, рост числа преступлений, предусмотренных ст. 212 УК, в 2019 г. по отношению к 2012 г. составил более 400 %. Более того, ущерб от таких преступлений превысил в разы объем похищенных средств другими преступными способами. Вместе с тем количество возбуждаемых уголовных дел по ст. 212 УК существенно больше, чем направлено в суд. Указанные факты свидетельствуют о возрастающей общественной опасности таких преступных деяний в информационном обществе.

В этой связи в современной науке особую остроту приобретает тема, касающаяся необходимости криминализации данного способа хищений. В узком смысле криминализация представляет собой признание в уголовном законе деяния общественно опасным и объявление его уголовно наказуемым [1, с. 75]. В качестве общего основания криминализации деяний выступает переоценка степени их общественной опасности в силу воздействия на волю законодателя объективных факторов развития общества и государства, в то время как причинами криминализации деяний является, как правило, отсутствие закрепления в уголовном законе новых, относительно недавно возникших угроз объектам (обособленным сферам общественных отношений), находящимся под уголовно-правовой охраной [2, с. 271]. Нельзя не согласиться с мнением Е.В. Епифановой, которая указала, что общественная опасность выступает в роли признака, который позволяет отграничить преступление от иных правонарушений: административные правонарушения, гражданско-правовые деликты являются вредными для общества или конкретного лица, асоциальными, но не общественно опасными [3, с. 47].

Кроме того, криминализация хищений имущества путем модификации компьютерной информации прежде всего обусловлена тем, что возросла их общественная опасность. В связи с чем следует указать, что информационные технологии широко применяются в преступных посягательствах виновных лиц, которые в подавляющих случаях друг друга не знают, и их взаимодействие осуществляется с помощью виртуальных средств идентификации [4, с. 18].

Более того, повышенная общественная опасность таких хищений обусловлена транснациональным характером их совершения, как пра-

вило, преступники совершают деяния, находясь на территории другого государства, с которым отсутствует международное соглашение в сфере оказания правовой помощи в их выявлении и раскрытии.

Как видим, с одной стороны, широкое распространение рассматриваемого хищения обусловлено тем, что благодаря сети Интернет преступники обладают возможностью доступа к значительному числу потенциальных потерпевших, а также доступа к информационным ресурсам организаций, а также финансовых учреждений.

В связи с чем законодателями при введении специальной нормы, предусмотренной ст. 212 УК, соблюден принцип системности, справедливости уголовного закона, так как преступления, совершаемые в сфере информационных технологий, являются более общественно опасными по сравнению с традиционными преступлениями в сфере собственности, предусмотренными ст. 205 «Кража», ст. 209 «Мошенничество» УК.

Обобщая вышеизложенное, следует констатировать тот факт, что необходимость установления уголовной ответственности за хищение имущества путем модификации компьютерной информации связана со спецификой способов и средств совершения таких преступных посягательств против собственности. Кроме того, о повышенной общественной опасности рассматриваемой разновидности хищений свидетельствуют следующие факторы: высокая латентность данных преступлений, транснациональный характер их совершения и объективная сложность доказывания. В связи с чем указанные факты свидетельствуют о необходимости дальнейшего конструирования диспозиции, квалифицирующих и особо квалифицирующих признаков рассматриваемой уголовно-правовой нормы с целью эффективного противодействия преступлениям, совершаемым в данной сфере.

1. Гриб, Д.В. Социальная обусловленность норм уголовного законодательства Российской Федерации и Республики Беларусь, предусматривающих ответственность за хищения, совершаемые с использованием информационных технологий / Д.В. Гриб // Евраз. адвокатура. – 2019. – № 2 (39). – С. 74–78.

2. Лопашенко, Н.А. Уголовная политика : монография / Н.А. Лопашенко. – М. : Волтерс Клувер, 2009. – С. 579.

3. Епифанова, Е.В. Общественная опасность как научная категория, законодательная дефиниция: история и современность : монография / Е.В. Епифанова. – М. : Юрлитинформ, 2012. – С. 189.

4. Дмитренко, А.П. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий / А.П. Дмитренко, Е.А. Русскевич // Вестн. Акад. Генер. прокуратуры Рос. Федерации. – 2017. – № 5 (61). – С. 18–22.

УДК 343.985

Н.С. Делов

ПРОБЛЕМЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Интернет активно используется каждым пользователем. Данная среда служит для обеспечения доступа к различным информационным ресурсам и системам. С каждым годом интернет все больше проникает в жизнь обычных людей, и это неудивительно. Ведь с помощью него можно обмениваться сообщениями с людьми, которые находятся на дальнем расстоянии от вас, можно найти необходимую информацию, решать производственные вопросы и приобретать необходимые товары и услуги.

Но есть и обратная сторона. Чем больше интернет проникает в нашу жизнь, тем больше появляется интернет-мошенничества, способов их совершения, и тем больше они становятся разносторонними. Стоит также отметить, что данный вид мошенничества является латентным, т. е. скрытым. Ведь он исключает непосредственный контакт с жертвой, данные о преступнике неизвестны, его место расположения, ник-нейм. Учитывая эти факторы, мошенники создают свой бизнес, основанный на обмане, и получают в дальнейшем огромные доходы с доверчивых граждан [1, с. 55].

В ходе раскрытия и расследования уголовных дел, которые связаны с использованием сети Интернет, возникают различные трудности, а именно:

установление личности преступника;

неизвестность его местонахождения;

использование скрытых айпи-адресов;

использование данных другого человека, непричастного к совершению преступления.

Исходя из этого, анализ правоприменительной практики показывает, что чаще всего совершаются следующие преступления:

хищение информации путем использования вирусов, которые ломают систему и позволяют изъять необходимую для преступника информацию;

неправомерный доступ к охраняемой законом компьютерной информации, в том числе базы данных правоохранительных органов;

использование внушения и злоупотребления доверием со стороны граждан и получение от них необходимой информации о банковских счетах, денежных средствах, и даже личной информации.