УДК 343.79

ХИЩЕНИЕ ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Е. В. Севрюк

студентка, Белорусский государственный университет, г. Минск, Беларусь, evgenia.sevruk21@gmail.com

Научный руководитель: **М. Г. Головенчик**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, goloventchikmg@bsu.by

В статье автором рассмотрено хищение путем модификации компьютерной информации как угрозы экономической безопасности. Сформулировано предложение по совершенствованию законодательства в целях охраны соответствующих общественных отношений.

Ключевые слова: киберпреступность; экономическая безопасность; хищение путем модификации компьютерной информации; внутренние угрозы.

THEFT BY MODIFICATION OF COMPUTER INFORMATION AS A THREAT TO ECONOMIC SECURITY

E. V. Sevruk

student, Belarusian State University, Minsk, Belarus, evgenia.sevruk21@gmail.com

Supervisor: **M. G. Goloventchik**

senior lecturer, Belarusian State University, Minsk, Belarus, goloventchikmg@bsu.by

In the article, the author considers theft by modification of computer information as a threat to economic security. A proposal has been formulated to improve legislation in order to protect relevant public relations.

Keywords: cybercrime; economic security; theft by modification of computer information; insider threats.

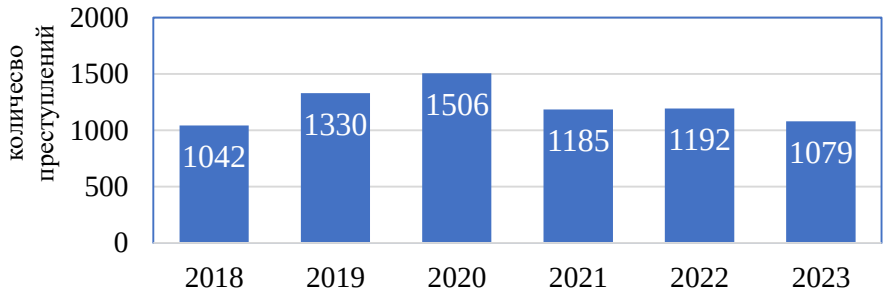
В век научно-технического прогресса информационные технологии являются не только неотъемлемой составляющей прогрессивного экономического развития, но также фактором существования киберпреступности. В свою очередь актуальность обеспечения экономической безопасности и противодействия киберугрозам усиливаются с каждым годом.

Как отмечает начальник управления по раскрытию киберпреступлений главного управления по противодействию киберпреступности Министерства внутренних дел А. Рингевич, по состоянию на август 2023 г. зафиксировано более 10 тыс. киберпреступлений, что вдвое больше по сравнению с аналогичным периодом 2022 г. Из них 90 % – мошенничество и хищение денежных средств: как накоплений граждан, так и кредитных ресурсов [1]. Лишь в первом квартале 2023 г. в Минске выявлено 1548 киберпреступлений, тогда как за аналогичный период 2022 г. – 1082, что свидетельствует о постоянном росте совершения такой группы преступлений [2].

Следует отметить, что согласно Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, преступлениями в информационной сфере признаются предусмотренные Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети. В Уголовном кодексе Республики Беларусь (далее – УК) данным преступлениям посвящена гл. 31 УК «Преступления против компьютерной безопасности». Но многие исследователи ст. 212 УК «Хищение путем модификации компьютерной информации», входящую в гл. 24 УК «Преступления против собственности», относят к киберпреступлениям. Сейчас большинство преступлений (83,4%), совершенных в сфере высоких технологий, связаны со ст. 212 УК [3].

Также Н. А. Швед отмечает, что, криминализировав несанкционированный доступ к компьютерной информации путем закрепления его в статье, открывающей гл. 31 УК, законодатель определил фундамент компьютерных преступлений, сформулированных с ориентацией на признаки данного состава преступления [4]. Мы отметим, что несанкционированный доступ также является признаком хищения путем модификации компьютерной информации, в связи с чем отдельные авторы относят ст. 212 УК к киберпреступлениям. Общественно опасные деяния, предусмотренные ст. 212 УК, безусловно, посягают на отношения собственности. В свою очередь собственность играет важную роль в экономике, служит основой для экономической деятельности.

Согласно ежегодным статистическим данным о деятельности судов общей юрисдикции по осуществлению правосудия, наблюдается устойчивая тенденция совершения свыше тысячи преступлений по ст. 212 УК.



Статистические сведения о количестве осужденных за хищение имущества путем модификации компьютерной информации (ст. 212 УК).
Источник: [5]

На практике наблюдается бóльшее количество преступлений, однако, в силу своей технически продвинутой природы, хищения путем модификации компьютерной информации становятся все более изощренными и трудно выявляемыми, то есть являются высоколатентными.

Согласно п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» (далее – постановление № 15), хищением имущества путем модификации компьютерной информации (ст. 212 УК) признается умышленное противоправное безвозмездное завладение чужим имуществом с корыстной целью посредством противоправного изменения компьютерной информации либо внесения в компьютерную систему заведомо ложной компьютерной информации.

Данное преступление предполагает манипулирование процессами ввода и вывода информации, когда компьютер, в соответствии со встроенной в него программой, идентифицирует нарушителя как законного владельца денежных средств.

В рамках дальнейшего анализа нами будет рассмотрен пример из следственной практики. Так, в сентябре прошлого года 38-летний гражданин обратился к своему 33-летнему знакомому с просьбой настроить доступ к криптокошельку. Знакомый помог, но в тайне сфотографировал секретную фразу для входа в систему управления виртуальными активами. Спустя некоторое время, находясь на территории Польши, он воспользовался данной информацией. В течение нескольких месяцев обвиняемый вывел «монеты» в сумме, эквивалентной 881262 бел. руб. О краже потерпевший узнал, когда проверил свой цифровой кошелек. Мужчина обратился в правоохранительные органы. По возвращению на Родину он был задержан сотрудниками милиции [6].

Отметим, что правовая природа криптовалют не однозначна, а в уголовном законодательстве она не определена. Однако, для упрощения процесса квалификации преступлений, связанных с хищением криптовалют, используется ст. 212 УК.

Данное преступление предполагает манипулирование процессами ввода и вывода информации, когда компьютер, в соответствии со встроенной в него программой, идентифицирует нарушителя как законного владельца денежных средств, что и отличает хищение путем модификации компьютерной информации от иных форм хищения, предусмотренных в гл. 24 УК «Преступления против собственности».

До внесения изменений и дополнений в УК Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» (далее – Закон № 112-З), ст. 212 УК именовалась «Хищение путем использования компьютерной техники». Процесс становления рынка высоких технологий и факт проникновения в данную сферу преступных элементов потребовал от законодателя изменить норму в целях реагирования на происходящие процессы.

Также Закон № 112-З внес изменения в ч. 4 примечаний к гл. 24 УК «преступления против собственности», закрепив, что лицо подлежит привлечению к уголовной, а не административной ответственности, если совершит хищение путем использования компьютерной информации у физического лица на сумму свыше двух базовых величин, а у юридического лица на сумму свыше десяти базовых величин.

В соответствии с изменениями ч. 2 ст. 27 УК «Возраст, с которого наступает уголовная ответственность», введенными Законом № 112-З, лицо, совершившее хищение имущества путем модификации компьютерной информации в возрасте от четырнадцати до шестнадцати лет подлежит уголовной ответственности.

Вместе с этим, законодатель постепенно смягчал санкции для квалифицированных составов ст. 212 УК, предусмотрев в качестве альтернативы лишению свободы более мягкие наказания, также были снижены верхние и (или) нижние пределы наказаний.

Закон № 112-З исключил такой квалифицирующий признак, как хищение, сопряженное с несанкционированным доступом к компьютерной информации. Хищения с использованием чужих данных всегда сопровождались вменением данного признака. Так, с учетом изменений такие действия будут квалифицироваться по ч. 1 ст. 212 УК, что смягчает уголовную ответственность.

Законом Республики Беларусь от 9 января 2019 г. № 171-З «О внесении изменений и дополнений в некоторые кодексы Республики Беларусь» за совершение деяний, предусмотренных ч. 4 ст. 212 УК (организованной

группой либо в особо крупном размере) были снижены пределы наказания в виде лишения свободы на срок от 5 до 12 лет (ранее был предусмотрен срок от 6 до 15 лет).

Подводя итог вышеизложенному, процесс проникновения криминальных элементов в сферу высоких технологий потребовал от законодателя принять соответствующие меры реагирования. С учетом влияния киберпреступлений на экономическую безопасность необходима дальнейшая работа с действующим уголовным законодательством. Постановление № 15 на данный момент разъясняет лишь, что понимается под терминами «хищение имущества путем модификации компьютерной информации», «компьютерная информация», однако положений направленных на разъяснение особенностей хищения путем модификации компьютерной информации, отграничение от смежных преступлений не содержится. Предлагаем в этой связи внести соответствующие дополнения в постановление № 15.

Библиографические ссылки

1. В Беларуси в 2023 году зафиксировано более 10 тыс. Киберпреступлений [Электронный ресурс] // БЕЛТА. URL: https://www.belta.by/society/view/v-belarusi-v-2023-godu-zafiksirovano-bolee-10-tys-kiberprestuplenij-585322-2023/?utm_source=belta&utm_medium=news&utm_campaign=accent (дата обращения: 04.04.2024).
2. Куда уходят деньги? В первом квартале 2023 года в столице выявлены 1548 киберпреступлений [Электронный ресурс] // Минские новости. URL: https://minsknews.by/kuda-uhodyat-dengi-v-pervom-kvartale-2023-goda-v-stolicze-vyyavleny-1-548-kiberprestuplenij/ (дата обращения: 04.04.2024).
3. Киберпреступность в Беларуси: с каждым годом интернет-мошенники и взломщики становятся все моложе Киберпреступлений [Электронный ресурс] // parvo.by. URL: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2016/october/21191/ (дата обращения: 04.04.2024).
4. *Швед Н. А.* Уголовное законодательство зарубежных стран об ответственности за несанкционированный доступ к компьютерной информации // СПС «КонсультантПлюс Беларусь».
5. Статистика [Электронный ресурс] // Интернет-портал судов общей юрисдикции Республики Беларусь. URL: https://www.court.gov.by/ru/justice_rb/statistics/ (дата обращения: 04.04.2024).
6. Столичные следователи установили обстоятельства хищения криптовалюты [Электронный ресурс] // Интернет-портал Следственного комитета Республики. URL: https://sk.gov.by/ru/news-usk-gminsk-ru/view/stolichnye-sledovateli-ustanovili-obstojatelstva-xischenija-kriptovaljuty-13309/ (дата обращения: 04.04.2024).