ОСОБЕННОСТИ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В.Г. Стаценко

Ключевые слова: информационно-коммуникационные технологии, информационная безопасность, преступления против компьютерной безопасности.

Анализ зарубежного уголовного законодательства показывает, что многие страны в том или ином виде криминализировали, в последние годы, деяния, нарушающие информационную безопасность, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства. И, хотя признаки составов этих преступлений в УК разных государств описаны по-разному, смысл заключается в запрете несанкционированного доступа к компьютерной информации или компьютерному оборудованию. Указанный запрет, независимо от степени описания объективных и субъективных признаков, призван охранять безопасность использования компьютерной информации.

Необходимость указанной криминализации деяний в сфере защиты информационно-коммуникационных технологий, также как постоянного совершенствования законодательства, связаны, прежде всего, с о значительным ухудшением криминогенной ситуации во многих странах, в том числе и в Республике Беларусь, определяемой увеличением числа преступлений, объединяемых общим понятием «киберпреступность».

Официальная криминальная статистика последних лет свидетельствует о том, что преступления против компьютерной безопасности увеличиваются темпами, значительно опережающими динамику других видов преступного поведения. Так, если в 2018 году в Республике Беларусь было зарегистрировано 4741 преступление с использованием компьютерной техники, то в 2020 году - 25.561, т.е. увеличение составило более чем 5 раз. Удельный вес киберпреступлений в общем числе регистрируемых преступлений составляет более четверти всех преступлений 2020 года. 92% от всех рассматриваемых преступлений - хищения с использованием компьютерной техники [1].

В 2021 году динамика преступлений против компьютерной безопасности сохраняется. Как полагают специалисты, если не принять меры по совершенствованию законодательства и правоприменительной практики в сфере ИКТ, число киберпреступлений к 2025 году может увеличиться до100 тысяч в год [2].

Анализ действующего законодательства Республики Беларусь показывает, что понятие «преступления против информационной безопасности» включает в себя следующие группы преступлений:

- преступления против информационной безопасности, так или иначе связанные с использованием компьютерной техники: изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343УК), в том числе с изображением несовершеннолетнего (3431УК); разжигание расовой, национальной, религиозной либо иной социальной вражды или розни (ст.130 УК); вымогательство (ст. 208 УК); доведение до самоубийства через распространение каких-либо сведений (ст.145 УК); разглашение врачебной тайны (ст. 178 УК); клевета (ст.188 УК); оскорбление представителя власти (ст.369 УК); незаконные действия в отношении информации о частной жизни и персональных данных (ст.203.1 и 203.2); нарушение авторского права, смежных прав и права промышленной собственности (ст. 201 УК); распространение ложной информации о товарах и услугах (ст.250 УК); заведомо ложное сообщение об опасности (ст.340 УК); нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 203 УК), коммерческий шпионаж (ст. 254 УК); мошенничество (ст.209 УК); шпионаж (ст. 358 УК); умышленное либо по неосторожности разглашение государственной тайны (ст.373-374 УК); умышленное разглашение служебной тайны (ст.375 УК) и др.

– преступления против компьютерной безопасности (несанкционированный доступ к компьютерной информации, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

– хищения путем использования средств компьютерной техники (ст. 212УК).

Законом Республики Беларусь, принятым 26 мая 2021 г. № 112-З [3] в статьи УК в сфере уголовно-правовой охраны как информационной безопасности в целом, так и компьютерной безопасности, были внесены значительные изменения.

Отметим наиболее существенные новации, внесенные в УК [4].

Диспозиция ч.1 статьи 208 «Вымогательство» расширена путем внесения дополнения, относящегося к охране компьютерной информации:»1.Требование передачи имущества или права на имущество либо совершения каких-либо действий имущественного характера под угрозой применения насилия к потерпевшему или его близким, уничтожения или повреждения их имущества, уничтожения, завладения, блокирования, модификации компьютерной информации, распространения клеветнических или оглашения иных сведений, которые они желают сохранить в тайне (вымогательство)…».

Статья 208 УК снабжена примечанием, определяющим понятие модификации компьютерной информации: «Под модификацией компьютерной информации в настоящей статье, статьях 212, 216, 350 и 354 настоящего Кодекса понимаются противоправное изменение компьютерной информации либо внесение в компьютерную систему заведомо ложной компьютерной информации».

Ч. 1 статьи 212 «Хищение имущества путем модификации компьютерной информации» (прежнее наименование статьи: «Хищение путем использования компьютерной техники») приводится в новой редакции: «1. Хищение имущества путем модификации компьютерной информации» (было: «Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации»)».

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. Ответственность за деяния, предусмотренные ст.212, наступает с 14-летнего возраста

До недавнего времени уголовный закон не содержал специальных составов об ответственности за действия с персональными данными. Статья 179 Уголовного кодекса Республики Беларусь предусматривала лишь ответственность за незаконные собирание либо распространение сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия, повлекшие причинение вреда правам, свободам и законным интересам потерпевшего. Кроме того, ряд статей УК предусматривал ответственность за умышленное разглашение отдельных видов охраняемой законом тайны (ст. 177, 178, 203, 205). Законом от 26 мая 2021 г. № 112-З УК дополнен двумя новыми статьями: 203-1 «Незаконные действия в отношении информации о частной жизни и персональных данных» и 203-2 «Несоблюдение мер обеспечения защиты персональных данных». Статьи 203-1 и 203-2 размещены в главе о преступлениях против конституционных прав и свобод человека и гражданина (статья 179 ранее размещалась в главе о преступлениях против уклада семейных отношений и интересов несовершеннолетних).

Глава 31 Раздела 12 Уголовного Кодекса Республики Беларусь, именовавшая (как и раздел в целом) «Преступления против информационной безопасности» и включавшая в себя 7 статей, была переименована в «Преступления против компьютерной безопасности». Под этим наименованием она включает сегодня 5 видов преступлений, содержащихся в соответствующих статьях, также потерпевших значительные изменения:

ст. 349 УК «Несанкционированный доступ к компьютерной информации как преступление против компьютерной безопасности»;

ст. 350 «Уничтожение, блокирование или модификация компьютерной информации»;

ст. 352 «Неправомерное завладение компьютерной информацией»;

ст. 354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»;

ст. 355 «Нарушение правил эксплуатации компьютерной системы или сети».

Статья 351 УК прежней редакции была исключена из УК, понятие «компьютерный саботаж» – исключено.

Статья 353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети» – исключена из УК. Деяния, предусмотренные ст. 353 – включены в ст. 354 действующего УК.

Принятие Закона от 26 мая 2021 г. № 112-З, дополнившего УК нормами уголовной ответственности за незаконные действия против информационной и компьютерной безопасности, стало важным этапом развития белорусского уголовного законодательства.

В то же время, необходимо отметить, что до сих пор отсутствуют межгосударственные соглашения, которые бы содержали признаваемые участниками этих соглашений единообразные правовые нормы и терминологию. Разнобой правового закрепления составов преступлений с использованием компьютерных технологий в законодательстве различных государств, очевидно требует осуществления унификации правового регулирования в сфере безопасности информационно-коммуникационных технологий на международном уровне.

Список использованных источников:

1. Сведения о совершенных правонарушениях на территории Республики Беларусь за январь–декабрь 2018–2020 г. / Информационный центр МВД Республики Беларусь. – Минск, 2019–2021.

2. СК: число киберпреступлений может вырасти до 100 тыс. в 2025 году [Электронный ресурс]. – Режим доступа: https://officelife.media /news /22947-kolichestvo-kiberprestupleniy-vyroslo-v-belarusi-v-proshlom-godu-v-2-5-raza/part2/. – Дата доступа: 30.10.2021

3. Об изменении кодексов по вопросам уголовной ответственности: Закон Республики Беларусь 26 мая 2021 г. № 112-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2021

4.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.// ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.