с жестоким обращением с несовершеннолетним. Отсутствие жестокости при совершении деяния не позволяет рассматривать данное деяние как преступление, а позволяет расценивать его как правонарушение.

Жестокое обращение — причинение нравственных и психических страданий, унижающих честь и достоинство несовершеннолетнего, лишение его свободы, полноценного питания, отдыха, принуждение к выполнению непосильных работ, телесные наказания, в том числе побои, оскорбление, иные действия, причиняющие психические и физические страдания несовершеннолетнему, покушение на половую неприкосновенность ребенка и т. д., те действия или бездействие, которые находят свое отражение при рассмотрении способа совершения преступления как криминалистической категории.

Различие состоит в том, что криминалистика рассматривает способ совершения преступления более широко: как систему действий, содержащую способ приготовления, способ непосредственного совершения и способ сокрытия преступления.

Заключение. Наблюдая за поведением несовершеннолетнего (конечно, больше это относится к маленьким детям от рождения и до семи лет, а также детям и более старшим, но с отклонениями в развитии), и анализируя следы, оставшиеся на теле ребенка, можно выдвинуть версию о том, что в отношении его было совершено преступление, заключающееся в ненадлежащем исполнении обязанностей по воспитанию несовершеннолетнего, связанном с жестоким обращением с ним, выполненное различными способами, которые можно установить, анализируя механизм следообразования [5, с.31].

Выявление в ходе расследования преступления следов насилия, механизма их образования, фиксация их надлежащим образом — это необходимые условия формирования доказательственной базы и, как следствие, успешного расследования уголовного дела и вынесения обвинительного приговора в суде.

Список используемых источников

1. Генеральная прокуратура Республики Беларусь [Электронный ресурс] / Информ. служба. — Минск, 2020. — Режим доступа: http://prokuratura.gov.by/ . — Дата доступа: 29.01.2020.

2. *Шкурихина, Н. И.* Расследование преступлений, связанных с неисполнением или ненадлежащим исполнением обязанностей по воспитанию несовершеннолетнего : автореф. дис. … канд. юрид. наук : 12.00.09 / Н. И. Шкурихина. — Барнаул, 2007. — 24 с.

3. *Гордейчик, А. А.* Уголовно-правовые и криминологические проблемы борьбы с преступлениями против семьи и несовершеннолетних : автореф. дис. … канд. юрид. наук : 12.00.08 / А. А. Гордейчик. — Харабовск, 2008. — 26 с.

4. *Кореневский, Ю. В*. Криминалистика для судебного следствия / Ю. В. Кореневский. — М. : ЦентрЮрИнфоР, 2001. — 198 с.

5. *Кочин, А. А*. Детерминация криминального насилия в семье : учеб. пособие / А. А. Кочин, В. С. Харламов. — М. : ВНИИ МВД России, 2004. — 52 с.

УДК: 343.3/.7

И. В. Шуленкова, И. Н. Овдийчук

Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

РАЗРАБОТКА, ИСПОЛЬЗОВАНИЕ ИЛИ РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ КАК ОПАСНОЕ ПРЕСТУПЛЕНИЕ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение. Кажется, только недавно белорусские законодатели криминализировали деяния в сфере компьютерной информации. Однако, развитие технических средств и программного обеспечения всегда будет опережать правовое регулирование информационных отношений, в связи с чем появление «пробелов» в республиканском законодательстве, в том числе и в Уголовном кодексе, неизбежно. В связи с этим особенно важным сегодня становится деловое взаимодействие технических специалистов и юристов с целью развития теории уголовного права и своевременной реакции законодателя на технический прогресс, привлечение инженеров-программистов к разработке мер профилактики преступлений против информационной безопасности и методик их расследования.

Основная часть. Эволюция науки и техники движется в направлении новых информационных технологий. Огромное количество компьютерных технологий задействовано в коммерческом обороте, что в конечном итоге приводит к реальной необходимости защитить их от незаконных действий преступников. В результате сочетания этих факторов возникли новые понятия: компьютерная преступность (киберпреступность), интернет-преступность и информационная зависимость.

Количество фактов разработки, использования или распространения вредоносных программ в последние годы в Республике Беларусь увеличивается: с 2015 года их количество увеличилось на 215,6 % (123 факта в 2017 году, 136 фактов было установлено в 2018 году). Это связано с высоким уровнем латентности данной категории преступлений, а также с ежегодным появлением новых типов вирусов и методов «заражения» компьютеров, что требует значительных усилий для раскрытия таких преступлений [1].

Разработка, использование или распространение вредоносных программ регламентировано в соответствии со ст. 354 Уголовного кодекса Республики Беларусь (далее — УК) [2]. По мнению А. Л. Савенка, объектом этого преступления являются отношения в области компьютерной информации [3, с. 105]. М. М. Малыковцев считает, что непосредственным объектом преступления является совокупность отношений, возникающих в связи с обеспечением безопасности и порядка использования информационных систем и информационно-телекоммуникационных сетей конкретных физических и юридических лиц. Кроме, того, он полагает, что при оценке тяжести совершенного правонарушения должен учитываться дополнительный непосредственный объект преступления, который охватывает право собственности, авторское право, неприкосновенность частной жизни, другие объекты, охраняемые уголовным законом [4, с. 16].

Предметом в составе выступают вредоносные компьютерные программы, а также компьютерные носители с такими программами. Вредоносность программы в связи с этим определяется в зависимости от того, было ли сделано уведомление о характере действия программы и учитывает ли программа согласие пользователя на реализацию своих целей. Объективная сторона преступления выражается в нескольких альтернативных действиях:

1) разработка вредоносного программного обеспечения (т. е. написание их алгоритма в виде последовательности логических команд и его последующее преобразование в машиночитаемый язык независимо от того, вставлено ли оно в память компьютера или нет);

2) внесение изменений в существующие программы, (т. е. исключение фрагментов алгоритма, замена другими, введение в программу дополнительных команд и др.;

3) преднамеренное использование специальных вирусных программ (любые действия по вводу программ в обращение);

4) распространение носителей с использованием специальных вирусных программ (передача компьютерных носителей с такими программами третьим лицам за плату или бесплатно, в постоянное владение или на временную основу. Состав преступления по конструкции объективной стороны — формальный.

Любое из перечисленных в ст. 354 УК действий является совершенным преступлением независимо от наступления вредных последствий — уничтожения, блокирования или изменения информации. Мы полагаем, что законодатель приравнял вредоносные программы к объектам и веществам, которые были изъяты из обращения, таким как оружие, наркотические средства и другие, признавая действия, связанные с вредоносными программами, преступными. Разработка вредоносных программ подразумевает написание их текста (алгоритма) в виде последовательности логических команд и его дальнейшее преобразование в машиночитаемый язык независимо от того, была ли такая программа введена в память компьютера или нет. Внесение изменений в существующие программы — это их изменение, то есть изменение текста программы путем исключения ее фрагментов, замены их другими, дополнения текста программы. Изменение считается уголовно наказуемым, только если правонарушитель исправил компьютерную программу или распространил исправленную программу на любом носителе. Исправление бумажной программы не является преступлением.

Следует подчеркнуть, что распространение программ без передачи их носителя возможно только в компьютерной сети — в локальной, региональной или международной. Следовательно, предоставление другим лицам доступа к вирусным программам через компьютерную сеть влечет за собой уголовную ответственность по ст. 354 УК.

Использование заведомо вредоносных программ будет наказуемо как при их использовании для заражения других компьютеров, так и при защите их программного обеспечения, баз данных и другой информации от несанкционированного копирования. Ответственность по ст. 354 УК несут не только разработчики вредоносных программ, но и другие лица, использующие или распространяющие эти программы. По части 2 ст.354 УК предусматривается повышенная ответственность за те же действия, которые повлекли за собой тяжкие последствия. К ним относят следующие — аварии, катастрофы, несчастные случаи с людьми, негативные изменения в окружающей среде, причинение материального ущерба в особо крупных размерах и др.

Для того, чтобы привлечь к ответственности по ч. 2 ст. 354 УК необходимо установить, наличие прямого или косвенного умысла к причинению тяжких последствий, так как в норме отсутствует указание на неосторожную форму вины. С субъективной стороны это преступление характеризуется только прямым умыслом. Кроме того, особенностью субъективной стороны является наличие обязательной цели — несанкционированное уничтожение, блокировка, изменение или копирование информации, хранящейся в компьютерной системе. Мотивы преступления не влияют на квалификацию [5, с. 20—21].

Как уже указывалось, предметом преступления являются вредоносные компьютерные программы и носители с такими программами. Как правило, вредность или полезность программы в отношении рассматриваемого преступления следует определять не в зависимости от ее основного назначения или способности блокировать, изменять или копировать информацию, а при наличии следующих двух условий:

1) включает ли действие таких программ предварительное уведомление владельца информации о компьютере или другого добросовестного пользователя о характере программы;

2) предполагает ли программа получение их согласия (то есть санкций) на реализацию программы ее цели. В случае, если программа не соответствует хотя бы одному из этих двух условий, она считается вредоносной.

Вредоносные программы — это те, которые, к примеру, содержат фрагменты кода с алгоритмами «почтовой бомбы», «троянского коня», «асинхронной атаки», «штриховки», «червя» и т. д., или программы с вирусами. Вредность компьютерных вирусов связана с их способностью к самовоспроизведению, перекрестными сетями из одной системы в другую, проникновением в компьютеры, то есть распространением, аналогичным вирусному заболеванию, и вмешательством в работу компьютера без ведома и согласия добросовестного пользователя. Чаще всего сбои в работе компьютера сопровождаются полным или частичным уничтожением информации.

Помимо вредоносных программ, предметом рассматриваемого преступления являются компьютерные носители с такими программами. По нашему мнению, при описании особенностей рассматриваемого акта белорусские законодатели не совсем успешно использовали законодательную технику с использованием множественного числа. Буквальное толкование диспозиции приводит к выводу, что для применения данной статьи необходимо выполнить вышеуказанные действия в отношении не одной, а обязательно нескольких программ. Однако для уголовного преследования по ст. 354 УК, достаточно выполнить хотя бы одно из этих действий и в отношении одной вредоносной программы.

Заключение. Для обеспечения согласованности правового регулирования в ч.1 ст. 354 УК предлагается заменить слова «или копия» словами «копия или иное владение»; после слова «медиа» добавить слова «или передать с помощью компьютерной связи».

Считаем необходимым внести изменения в ч. 1 ст. 354 УК и изложить ее в следующей редакции: «Разработка компьютерной программы или внесение изменений в существующую программу с целью несанкционированного уничтожения, блокировки, изменения или копирования информации, хранящейся в компьютерной системе, сети или компьютерном носителе, либо разработка специальной вирусной программы, либо ее преднамеренное использование, либо распространение носителя с такой программой — наказывается…»

Кроме того, полагаем, что существует необходимость улучшения процесса дифференциации наказания с помощью квалифицирующих признаков в рамках ст.354 УК. С этой целью предлагаем дополнить ст. 354 УК частью 3 следующего содержания: «те же действия, совершенные с участием двух и более лиц, наказываются…».

Список цитируемых источников

1. Преступность в Республике Беларусь [Электронный ресурс] // Нац. стат. ком. Респ. Беларусь. — Режим доступа: http://www.belstat.gov.by . — Дата доступа: 12.01.2020.
2. 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. : в ред. Закона Респ. Беларусь от 09.01.2019 г., № 171-З // Нац. правовой Интернет-портал Респ. Беларусь. — 27.10.2019 — 2/2609.
3. *Савенок, А. Л.* Уголовное право Республики Беларусь. Особенная часть : учеб.-метод. пособие / А. Л. Савенок, В. С. Яловик. — Минск : Тэхналогія, 2001. — 141 с.
4. *Малыковцев, М. М.* Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : автореф. дис. … канд. юрид. наук : 12.00.08 / М. М. Малыковцев. — М., 2006. — 186 с.
5. *Лосев, В. В.* Уголовно-правовой анализпреступлений против информационной безопасности / В. В. Лосев // Судовы весн. — 2003. — № 4. — С. 18—22.

УДК 347.45/.47

Н. В. Языков

Учреждение образования «Белорусский государственный экономический университет, Минск, Республика Беларусь

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ДОГОВОРА НА РАЗРАБОТКУ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Введение. В связи с динамичным развитием рынка цифровых услуг и постепенной цифровизацией экономики, а также повсеместным внедрением и использованием различными компаниями программных продуктов (программ, корпоративных сайтов и т. д.) появляется необходимость в правовом оформлении сделок по выполнению работ на их разработку. Одним из таких продуктов является программное обеспечение, которое зачастую разрабатывается индивидуально под заказ и является одним из главных элементов в системе программных продуктов компании.

Согласно Д. А. Тимофееву процесс разработки программного обеспечения (далее — ПО) представляет собой комплексный набор последовательных действий и состоит из определенных этапов (плани-