Вестник Сибирского юридического
института МВД России

УДК 343.2/.7

Руслан Рейзаевич КАРДАНОВ,
начальник кафедры организации
правоохранительной деятельности
Северо-Кавказского института повышения
квалификации (филиала) Краснодарского
университета МВД России (г. Нальчик),
кандидат юридических наук
ruslan-nalchik@yandex.ru

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

CRIMINAL LAW PROTECTION OF INFORMATION SECURITY

В статье рассматривается одно из основных направлений деятельности многих современных государств – обеспечение информационной безопасности, одним из основных инструментов которого выступает институт уголовной ответственности за преступления в сфере информационной безопасности, констатируется отсутствие в действующем российском законодательстве комплексного подхода к проблемам информационной безопасности при фрагментарном закреплении отдельных составов преступлений.

По мнению автора, ориентация российского законодательства в рамках уголовно-правовой охраны на компьютерную информацию существенно осложняет квалификацию деяний, распространенных в настоящее время, совершающихся достаточно часто в отношении именно электронной информации. В данном контексте выделяется ряд проблем, начиная от недостаточной теоретико-правовой разработки заявленной проблематики и заканчивая существующими пробелами в уголовно-правовом законодательстве. В качестве перспективного направления решения указанных проблем автором предлагается создание отдельной главы в УК РФ «Преступления против информационной безопасности», в рамках которой следует не просто объединить существующие уголовно-правовые нормы, но и систематизировать понятийно-категориальный аппарат с учетом реального состояния информационных правоотношений.

The article discusses one of the main activities of many modern states – ensuring information security, one of the main tools of which is the institution of criminal liability for crimes in the field of information security. It is stated that the current Russian legislation lacks an integrated approach to information security problems with fragmentary fixing of individual elements of crimes.

According to the author's opinion, the orientation of Russian legislation within the framework of criminal law protection to computer information significantly complicates the qualification of acts that are currently common, committed quite often in relation to electronic information. In this context, a number of problems are highlighted, ranging from insufficient theoretical and legal development of the stated issues and up to existing gaps in criminal law. As a promising direction for solving these problems, the author proposes the creation of a separate chapter in the Criminal Code of the Russian Federation «Crimes against information security», whereby it is necessary not only to combine the existing criminal law norms, but also to systematize the conceptual and categorical apparatus, taking into account the real state of information legal relations.

Ключевые слова: информационная безопасность, уголовно-правовая охрана, электронные документы, борьба с преступностью, уголовное законодательство.

Keywords: *information security, criminal law protection, electronic documents, fight against crime, criminal legislation.*

В условиях динамично развивающегося информационного общества в российском государстве информация и разнообразные юридически значимые действия с ней становятся неотъемлемой частью жизни каждого человека. Вышеназванная тенденция представляется весьма закономерной, что проявляется в том числе и в масштабности внедрения многообразных информационных технологий в различные сферы жизнедеятельности общества. Однако в сложившихся условиях не просто приобретает актуальность совершенствование действующих законодательных требований, а имеют принципиальное значение своевременное и полное толкование и определение специфики информационных технологий, которые наиболее часто применяются в различные периоды.

Динамичность развития информационных технологий представляется весьма оправданной, поскольку подобные достижения науки и техники позволяют добиться существенных результатов различных общественных отношений в гораздо более короткие сроки. В настоящее время, в том числе в условиях пандемии новой коронавирусной инфекции, от эффективности информационного взаимодействия во многом зависит функционирование жизнеобеспечения современного общества. В данном контексте представляется целесообразным сконцентрировать внимание на вопросах, связанных с уголовно-правовой охраной информационной безопасности, так как масштабное распространение информационных правоотношений и их динамичное развитие не только постоянно формируют новые вызовы и угрозы в отношении частных интересов, но и затрагивают национальную безопасность в целом.

Преступная деятельность в условиях повсеместной информатизации и цифровизации развивается стремительными темпами, что проявляется в существенном изменении способов совершения противоправных деяний и в трансформации объективной стороны преступлений. Информационные технологии не только расширяют возможности современных преступников, они формируют совершенно новые правоотношения, в которых информация все чаще становится предметом преступного деяния. В данном контексте принципиальное значение имеет наличие необходимых уголовно-правовых подходов к информационным правоотношениям, которые бы позволяли в полной мере оценивать противоправные деяния, совершаемые в указанной сфере.

Современная правовая литература содержит множество исследований, посвященных проблемам обеспечения информационной безопасности, однако уголовно-правовая направленность данных работ в большинстве своем связана с анализом отдельных преступных деяний. Например, пристальное внимание правоведы уделяют проблемам охраны персональных данных в контексте обеспечения информационной безопасности [1, с. 74]. Данная тематика, безусловно, имеет важнейшее значение в рамках заявленной проблематики, однако в рамках представленного исследования видится целесообразным комплексно проанализировать существующее состояние уголовно-правовой охраны информационной безопасности в Российской Федерации.

Российская правовая система в настоящее время лишь фрагментарно воспринимает идею информации не как чего-то материального, а как иного объекта, который вне зависимости от его физической фиксации имеет существенное значение в рамках конкретных правоотношений. Подобный подход частично реализовывается в информационном законодательстве, однако нормативно-правовые акты в иных отраслях права до сих пор в большинстве своем ориентированы на материальное обличие информации.

В первую очередь отметим, что в рамках заявленной проблематики принципиальное значение имеет акцентирование внимания на отдельных характеристиках информации, отличающих ее от материальных объектов:

1) при тайном хищении сведения не всегда исчезают, а могут сохраниться в системе;

2) в определенных случаях возникают сложности с оценкой стоимости нанесенного ущерба при утечке информации;

3) все чаще отсутствует привязанность информации к носителю, из-за чего возникают сложности при отстаивании прав;

4) информация является основой для деятельности с целью извлечения прибыли, соответственно, нуждается в полноценной охране.

Важно отметить, что категория «информационная безопасность» в российском уголовном законодательстве не используется, что, с одной стороны, объективно обусловлено динамикой развития информационных правоотношений и существенным изменением отраслевых подходов за последнее десятилетие, с другой – подобный пробел сужает применимость института уголовной ответственности в указанной сфере. Так, действующее уголовное законодательство содержит ряд составов в главе 28 УК РФ, посвященной преступлениям в сфере компьютерной информации. Современная следственная и судебная практика демонстрирует существенную сложность квалификации многих совершаемых деяний в рамках указанных уголовно-правовых норм непосредственно по причине их ориентации на материальное восприятие информации.

Правильное с методологической точки зрения решение проблем информационной безопасности должно начинаться с выявления субъектов общественных отношений, а также интересов данных субъектов, которые связаны с применением той или иной информации. Главной особенностью современного этапа развития российского государства является существенное расширение субъектного состава подобных отношений: в них активно вовлечены личность и общество с государством в целом, так как информация в настоящее время используется не только и не столько для достижения частных интересов, а посредством противоправного масштабного распространения способна влиять на восприятие обществом отдельных значимых процессов, что в целом негативно отражается на национальной безопасности [3, с. 22]. Вопросы неправомерного распространения информации как раз нашли отражение в действующем уголовно-правовом законодательстве, однако комплексного подхода к проблемам информационной безопасности в нем по-прежнему не разработано.

Таким образом, Особенная часть УК РФ не содержит базовых норм, охраняющих отношения в области информационной безопасности, в одной главе. Наоборот, они находятся в разных главах и разделах УК РФ, хотя имеют тесную взаимосвязь. Ориентация российского законодательства в рамках уголовно-правовой охраны на компьютерную информацию существенно осложняет квалификацию деяний, распространенных в настоящее время, так как последние совершаются достаточно часто в отношении именно электронной информации.

В данном контексте представляется необходимым отметить наиболее существенную проблему действующего уголовного законодательства – отсутствие ясных и однозначных понятий в сфере информационной безопасности, которые бы отражали реальное состояние информационных правоотношений. Примечательно, что информационное законодательство весьма детально разработало к настоящему моменту указанный понятийно-категориальный аппарат, однако его потенциал не используется в иных отраслях права. Следует согласиться с мнением Р.Н. Ключко о том, что вышеназванная проблема существенно затрудняет применение уголовно-правового законодательства и вызывает сложности правовой оценки совершаемых деяний [2, с. 54].

В качестве перспективного направления решения указанных проблем, а также обеспечения уголовно-правовой охраны информационной безопасности в Российской Федерации представляется необходимым выделить создание отдельной главы в УК РФ «Преступления против информационной безопасности», в рамках которой должны быть объединены существующие уголовно-правовые нормы. Указанная глава в обязательном порядке в отдельных статьях, а точнее, в примечаниях к ним, должна конкретизировать наиболее значимые понятия.

В современной науке информационная безопасность рассматривается в нескольких

смыслах: как элемент экономической безопасности, как составляющая национальной безопасности, как важнейшее направление современной государственной политики. Вышеназванные подходы совершенно справедливо подчеркивают значимость обеспечения информационной безопасности одновременно для целого ряда сфер жизнедеятельности российского общества и государства. Изначально информация и безопасность ее оборота рассматривались в рамках коммерческих и иных публичных правоотношений, где соответствующие сведения имели существенный экономический интерес. В настоящее время данный подход по-прежнему актуален, однако современная преступная деятельность в сфере информационной безопасности демонстрирует существенные национальные и государственные угрозы. Так, в настоящее время информационные технологии позволяют представителям преступных сообществ весьма в короткие сроки распространять свои противоправные идеи в глобальных масштабах, что в целом негативно отражается на стабильности государственной деятельности.

Несмотря на то, что все вышеназванные аспекты толкования информационной безопасности тесно связаны друг с другом, для эффективной борьбы с преступным поведением в данной сфере недопустимо исключение каких-либо аспектов ее проявлений, поскольку каждый из них имеет принципиальное значение для развития российского государства и общества. В данном контексте совершенно справедливым представляется развернутое толкование информационной безопасности непосредственно в примечаниях к уголовно-правовым нормам, так как данная детальная регламентация позволит конкретизировать сферу их применения. Безусловно, со временем потребуется совершенствование понятийно-категориального аппарата, однако для современного состояния российского уголовного законодательства острую необходимость имеет их первичное закрепление с целью унификации следственной и судебной практики.

Также представляется целесообразным в рамках предложенной отдельной главы рассматривать и компьютерную информацию в случае ее связи с материальными носителями, но указанная информация должна рассматриваться наравне с иными ее разновидностями. Например, в настоящее время существенную актуальность приобретает регулирование правоотношений, связанных с различными юридически значимыми действиями, совершаемыми с электронными документами. Подобная практика активно внедряется в различных органах государственной власти, а также распространяется и в частных взаимоотношениях современных людей. Удаленное взаимодействие людей, в том числе совершение различных юридически значимых действий с использованием электронной подписи и специальных средств идентификации личности, приобрело особую актуальность в условиях пандемии, и масштабы указанной практики сохраняются и в настоящее время. Однако существующие информационные и технические уязвимости подобных взаимодействий, в том числе отсутствие необходимых уголовно-правовых норм, регламентирующих ответственность за отдельные деяния с электронными документами, способствуют расширению масштабов преступности в данной сфере.

В данном контексте следует отметить, что одной из отличительных черт электронного документа от бумажного является способ его незаконного приобретения, а именно не только физическое воздействие, но и техническое. Существенной спецификой обладает и незаконное распространение подобных документов, поскольку сам документ не изменяет своих характеристик, но может быть доступен неограниченному кругу лиц. Способов незаконного приобретения электронных документов в настоящее время весьма много, начиная от копирования в результате незаконного доступа к месту хранения подобного документа (в том числе с использованием облачных технологий) и заканчивая перехватом подобного документа в процессе его пересылки частным или публичным лицом. С одной стороны, все указанные деяния связаны с незаконным доступом к отдельным информационным ресурсам (личные кабине-

ты, информационные хранилища, электронные почты и др.), что само по себе является противоправным. С другой – масштаб негативных последствий вышеназванного незаконного доступа может быть гораздо больше в случае использования преступниками электронных документов, которые представляют интерес для отдельных физических или юридических лиц, а также органов государственной власти.

Весьма распространенным противоправным деянием в отношении электронных документов также является их уничтожение, т.е. удаление впоследствии незаконного доступа к соответствующей информации или ограничение доступа к документу для его владельцев. В данном контексте по-прежнему большое значение имеет незаконный доступ к соответствующим документам, однако факт их недоступности по каким-либо причинам, организованный с преступным умыслом, также нуждается в квалификации с учетом современной значимости электронных документов.

Как таковой электронный документ в буквальном смысле похитить не всегда возможно, но возможно похитить носитель, содержащий в себе документ, чтобы получить доступ к данному документу. Но если у субъекта возникает умысел на похищение носителя информации, например флеш-карты, то данное преступление будет направлено уже против собственности. При этом действующее уголовное законодательство не учитывает целый ряд деяний, которые могут быть совершены с электронными документами с преступным умыслом и соответствующими негативными последствиями для их владельцев. Следует подчеркнуть, что не все деяния в сфере информационной безопасности могут быть квалифицированы в рамках уголовно-правовых норм о компьютерной информации и мошеннических действиях с использованием информационных технологий.

Информационная безопасность в настоящее время представляет принципиальный интерес не только в контексте частных интересов, но и в части обеспечения государственной безопасности в целом. Преступные деяния в сфере информационной безопасности не только негативно отражаются на отдельных общественных отношениях (например, экономической направленности), но и способны дестабилизировать государственное управление в целом. В данном контексте весьма справедливым представляется детальное исследование существующей преступной практики в данной сфере с целью разработки эффективного уголовно-правового регулирования, которое позволит назначать соразмерные и справедливые наказания лицам, совершившим соответствующие деяния.

Таким образом, несмотря на то, что действующее уголовно-правовое законодательство Российской Федерации регламентирует отдельные аспекты охраны информационной безопасности, в условиях распространения масштабов использования различных видов информации в современном мире представляется необходимым комплексное оформление соответствующих составов в рамках отдельной главы УК РФ. Посредством теоретико-правового осмысления современного состояния информационных правоотношений представляется необходимым систематизировать существующие подходы к понятийно-категориальному аппарату по заявленной проблематике, который необходимо использовать и в уголовно-правовых нормах. Вышеназванное предложение по созданию отдельной главы в УК РФ представляется также оправданным с учетом дальнейшего весьма динамичного совершенствования информационного общества в российском государстве, что в перспективе способно создать необходимость дополнения новыми составами преступлений в сфере информационной безопасности. Своевременное изменение действующего законодательства, в том числе и уголовной направленности, выступает залогом эффективной борьбы с преступным поведением в указанной сфере.

Библиографический список

1. Вабищевич, В.В. Уголовно-правовая охрана персональных данных в контексте обеспечения информационной безопасности / В.В. Вабищевич // Юстиция Беларуси. – 2020. – N 4 (217). – С. 74-77.

2. Ключко, Р.Н. Информационная безопасность и кибербезопасность как объекты уголовно-правовой охраны / Р.Н. Ключко // Интеграция и развитие научно-технического и образовательного сотрудничества – взгляд в будущее : сборник статей II международной научно-технической конференции: в 3 т. – Минск, 2020. – С. 53-56.

3. Корабельников, С.М. Преступления в сфере информационной безопасности / С.М. Корабельников. – М.: Юрайт, 2020. – 111 с.