РАЗДЕЛ

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

ИДЕОЛОГИЯ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СФЕРЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

IDEOLOGY OF THE FIGHT AGAINST CRIME IN THE FIELD OF COMPUTER SECURITY

УДК 343.2

О.Н. ГОРОДНОВА,
кандидат юридических наук,
кандидат философских наук, доцент
(Чебоксарский кооперативный
институт (филиал)
Российского университета кооперации,
Россия, Чебоксары)
gorodno.olga@yandex.ru

OLGA N. GORODNOVA,
Candidate of Law,
Candidate of Philosophy Sciences,
Associate Professor
(Cheboksary Cooperative
Institute (branch)
Russian University of Cooperation,
Cheboksary, Russia)

Аннотация: уголовно-правовая наука рассматривает уголовно-правовую идеологию в качестве одного из аспектов уголовной политики тогда, когда уголовная политика вторична по отношению к идеологии борьбы с преступностью и должна следовать ей. Задача построения эффективного уголовного законодательства и обеспечения безопасности общества диктует необходимость построения идеологических основ совершенствования уголовного законодательства, в том числе противодействия преступлениям в сфере компьютерной информации.

В статье через призму принципов уголовного права как идеологических основ рассмотрена идеология как концепт противодействия преступлениям в сфере информационных технологий. Автором актуализирована тема глобальной информатизации общественных процессов и явлений и обозначена проблема информационной безопасности на основе данных статистики роста преступности в сети Интернет с использованием компьютерной техники. Сделан вывод о том, что уголовно-правовая идеология противодействия угрозам киберпреступности должна быть нацелена на ее предотвращение путем нормотворчества и эффективного применения.

В статье акцентировано внимание на компьютерных преступлениях, предусмотренных ст.ст. 272–274.1 Уголовного кодекса Российской Федерации. Работа нацеливает на необходимость введения нового квалифицирующего признака «с целью скрыть другое преступление или облегчить его совершение» в диспозиции ст.ст. 272, 273 Уголовного кодекса Российской Федерации; обращает внимание на внесение изменений в ст. 273 Уголовного кодекса Российской Федерации и необходимость криминализации незаконного приобретения вредоносных компьютерных программ, что гармонизирует принципы законности и равенства граждан перед законом. Предлагается в статьях главы 28 Уголовного кодекса Российской Федерации признать крупным ущерб, сумма которого превышает 250 тыс. руб., что будет соответствовать принципам равенства и гуманизма. Кроме того, «посягательство на критическую информационную инфраструктуру» в качестве квалифицирующего или особо квалифицирующего признака предложено поместить в ст. 272, 273, 274 Уголовного кодекса Российской Федерации.

Ключевые слова: идеология, преступность, принципы, компьютерные преступления, совершенствование законодательства.

Для цитирования: Городнова О.Н. Идеология борьбы с преступностью в сфере компьютерной безопасности // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2022. – № 4. – С. 44–49.

Abstract: criminal law science considers criminal law ideology as one of the aspects of criminal policy when criminal policy is secondary to the ideology of combating crime and must follow it. The task of building effective

criminal legislation and ensuring the security of society dictates the need to build ideological foundations for improving criminal legislation, including countering crimes in the field of computer information.

In the article, through the prism of the principles of criminal law as ideological foundations, ideology is considered as a concept of actions to counter crimes in the field of information technology. The author actualizes the topic of global informatization of social processes and phenomena and identifies the problem of information security based on statistics on the growth of crime on the Internet using computer technology. The conclusion is made that the criminal legal ideology of countering the threats of cyber crime should be aimed at preventing it through rulemaking and effective application. improving criminal legislation, including countering crimes in the field of computer information.

The article focuses on computer crimes provided for in Articles 272-274.1 of the Criminal Code of the Russian Federation. The work focuses on the need to introduce a new qualifying feature: «In order to conceal another crime or facilitate its commission» in the disposition of Articles 272, 273 of the Criminal Code of the Russian Federation; draws attention to the amendments to Article 273 of the Criminal Code of the Russian Federation and the need to criminalize the illegal acquisition of malicious computer programs, which harmonizes the principles of legality and equality of citizens before the law. The article proposes to recognize damages in the articles of Chapter 28 of the Criminal Code of the Russian Federation, the amount of which exceeds 250 thousand rubles, which will comply with the principles of equality and humanism. In addition, it is proposed to place «encroachment on critical information infrastructure» as a qualifying or particularly qualifying feature in Article 272,272,274 of the Criminal Code of the Russian Federation.

Keywords: ideology, crime, principles, computer crimes, improvement of legislation.

For citation: Gorodnova O.N. Ideology of the fight against crime in the field of computer security // Vestnik of Putilin Belgorod Law Institute of Ministry of the Interior of Russia. – 2022. – № 4. – P. 44–49.

Философ А. Дестют де Траси писал, что «идеология как наука об идеях сможет исследовать природу человеческого мышления и ответить на вопросы, что есть правда, а что ложь, обеспечить адекватное восприятие действительности и выявить реальные нужды людей, разрешив таким образом все проблемы общества» [1, с. 39–47]. Современная уголовно-правовая наука не уделяет пристального внимания институту идеологии борьбы с преступностью. В отечественном праве уголовно-правовая идеология представлена в качестве одного из аспектов уголовной политики [2, с. 125–132]. Вместе с тем задача построения эффективного уголовного законодательства и обеспечения безопасности общества диктует необходимость построения идеологических основ совершенствования уголовного законодательства, в том числе противодействия преступлениям в сфере компьютерной информации. Только в этом случае изменения, вносимые в законодательство, не будут носить бессистемный характер. Уголовная политика должна быть вторичной по отношению к идеологии борьбы с преступностью и следовать ей. Средствами уголовно-правовой идеологии должно создаваться справедливое уголовное законодательство и практика его применения [3, с. 201–204]. В то же время получает все большее распространение в условиях современного интернет-пространства криминально-идеологическое воздействие на сознание граждан. Это и идеология криминального бизнеса в сети Интернет, и идеология терроризма, и иные виды, что нацеливает на выработку мер по противодействию криминальным явлениям. Какую идеологию необходимо противопоставить идеологии преступности, если на государственном уровне такой идеологии нет? На наш взгляд, идеология может быть основана на основополагающих правовых идеях. Отдельные авторы рассматривают правовые принципы в качестве носителей (элементов) «идеологии российского права и государства в области борьбы с преступностью и защиты личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод» [4, с. 3.]. На наш взгляд, идеологию обеспечения компьютерной безопасности следует рассматривать как концепт действий, нацеленных на совершенствование уголовного права, направленных на реализацию интересов, потребностей общества. Современное уголовное право базируется на законодательно определенных и доктринальных принципах, которые являются фундаментом формирования уголовно-правовой идеологии, базисом, на который ориентирован правотворческий и правоприменительный процесс. Именно в этом контексте через призму принципов уголовного права как идеологических основ рассмотрим идеологию противодействия преступлениям в сфере информационных технологий. Данная тема долгое время не утратит актуальность, поскольку осознавать окружающую действительность в современном обществе с развитием технического прогресса стали чаще не офлайн, а онлайн. Глобальные информационные технологии открыли

огромные возможности для коммуникации, которая не всегда является безопасной. Отсутствие границ в киберпространстве делает его неконтролируемым с правовой точки зрения.

Сегодня современный человек не мыслит свою жизнь без телефона, ноутбука, смарт-часов, которые собирают о нем персональные данные и подстраивают рекламу с учетом запросов пользователя. В этой связи актуальна проблема информационной безопасности и крупных коммерческих холдингов, криптоинвесторов, и обычных рядовых потребителей товаров, работ и услуг, данные которых становятся доступными не только рекламщикам, но и злоумышленникам. Не только бытовые хищения, но и сбыт наркотических средств, шпионаж, терроризм и экстремизм получают распространение в интернет-пространстве. Именно поэтому важно поддерживать высокий уровень правосознания пользователей интернет-социума за счет стойкого неприятия преступности и справедливости, неотвратимости уголовно-правовой репрессии, которая неотделима от четкого следования законности. Уголовно-правовая идеология противодействия угрозам киберпреступности нацелена на ее предотвращение путем нормотворчества и эффективного применения. Результативность противодействия преступлениям в сфере компьютерной информации следует оценивать с точки зрения кодификации конкретных составов преступлений и правильности или, наоборот, ошибочности их квалификации в разрезе вызовов и рисков со стороны новых решений «компьютерных гениев». Это сделать непросто, так как преступники оказываются изощреннее в своей узкой специализации и создают новые вирусы, атакуют финансовую, банковскую систему, похищают персональные данные с целью материального обогащения.

В условиях пандемического кризиса экономики, сокращения численности работающего населения, а главное, массовой компьютеризации экономических, политических, социально-культурных, образовательных процессов и явлений возрастает угроза причинения вреда общественным отношениям путем распространения компьютерных вирусов.

Ежегодно правоохранительные органы фиксируют рост преступности в сети Интернет с использованием компьютерной техники. По данным статистики МВД России, за первое полугодие 2021 г. рост IT-преступности по сравнению с аналогичным периодом 2020 г. составил 20,3%[1]. Всего за 2021 г. совершено 518 тыс. киберпреступлений, что на 1,4% больше показателей за предшествующий период и почти в 1,8 раза больше значений 2019 г.[2] По прогнозам экспертов, ущерб от преступных кибератак с применением искусственного интеллекта в России в 2022 г. может достигнуть 165 млрд руб. Это обусловлено не только масштабной компьютеризацией общества, но и низкой компьютерной грамотностью пользователей программных продуктов, а также отсутствием опыта борьбы с электронными деликтами у должностных лиц следственных и судебных органов, что приводит к бесконтрольности распространения вредоносных компьютерных программ, подрывает доверие к власти и уголовному, уголовно-процессуальному закону, снижает правосознание общества.

Оценивая качество идеологии противодействия преступлениям в сфере охраны компьютерной безопасности, следует акцентировать внимание на собственно компьютерных преступлениях, предусмотренных ст. 272 – 274.1 Уголовного кодекса Российской Федерации[3], а также иных, совершаемых с использованием программ для ЭВМ. К ним, например, можно отнести кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств, или мошенничество в сфере компьютерной информации. Для их совершения информационные технологии выступают лишь инструментом.

Нередко компьютерные преступления называют инструментальными, поскольку они способствуют совершению различных преступлений с целью достижения иных преступных результатов, а также нацелены на сокрытие или облегчение совершения иных преступлений. В этом случае деяние квалифицируется по совокупности по ст. 128.1, 137, 138, 165, 183, 283, 283.1 УК РФ и др. *Это нацеливает на необходимость введения нового квалифицирующего признака «с целью скрыть другое преступление или облегчить его совершение» в диспозиции ст. 272, 273 УК РФ*. В этом контексте важно установить границы дифференциации уголовной ответственности, адекватные степени общественной опасности деяния с целью определения справедливого наказания. Проблема назначения справедливого наказания не замыкается вопросами дифференциации ответственности, ее решение способствует индивидуализации наказания *в каждом конкретном случае при рассмотрении дела в суде*.

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – июнь 2021 года [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/25094008/ (дата обращения: 26.07.2022).

[2] Потенциальный ущерб от киберпреступности в 2022 году оценили в 165 млрд [Электронный ресурс]. – URL: https://news.rambler.ru/sociology/48152500/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 26.07.2022).

[3] Далее – УК РФ.

Те обстоятельства, что практически любое преступление может быть совершено при применении программно-технических устройств, информационная инфраструктура способствует сокрытию координат ее владельцев, повышают общественную опасность применения коммуникационных технологий и мотивируют законодателя дополнить ст. 63 УК РФ обстоятельством – совершение преступления с использованием информационно-коммуникационных технологий либо иных технологий хранения, обработки, передачи и защиты компьютерной информации.

Действие принципа справедливости распространяется и на определение деяния в качестве преступного, и на дифференциацию санкций, и на процесс квалификации, ошибки которой могут привести к несправедливому наказанию [5, с. 30–32].

Квалификация преступлений представляет собой сложный мыслительный процесс, который направлен на получение объективной информации о совершении субъектом конкретного преступления или преступлений. Квалификация тогда является справедливой, когда установлены обстоятельства дела, необходимые для определения состава преступления и верно применен уголовный закон [6, с. 605–616]. Например, субъект совершает неправомерный доступ не просто к компьютерной информации, а к информации, составляющей коммерческую или государственную тайну, и уничтожает ее. Его деяния квалифицируются по совокупности ст. 272 и 183 УК РФ или ст. 272 и 283.1 УК РФ соответственно.

Чтобы не возникали трудности при квалификации деяний, необходимо иметь четкие, недвусмысленные диспозиции статей. В этом также находит отражение идеология справедливости уголовного закона и наказания [7, с. 123–129]. Несовершенство содержания уголовно-правовых запретов требует совершенствования норм главы 28 УК РФ. Рассмотрим некоторые юридико-технические проблемные аспекты конструкции составов компьютерных преступлений.

Проблема выявления компьютерных правонарушений обусловлена тем, что деяния могут совершаться в режиме инкогнито дистанционно из любой точки земного шара и причинять вред неограниченному числу пользователей, обладателей компьютерной информации. Злоумышленники подключаются через VPN-сервисы, чтобы было сложно определить IP-адрес их компьютера или другого девайса и установить их персональные данные. Кроме того, не всегда отдельные представители правоохранительных органов обладают цифровой грамотностью для расследования киберделиктов. В условиях приспособленности молодежи к новой виртуальной реальности появляются различные способы совершения преступлений на фоне пропаганды идеологии коммерциализации интернет-пространства. Так, получили распространение киберпреступления в области игровой индустрии. Они носят латентный характер и создают угрозу для развития киберспорта в России, который признан на официальном уровне. Уроженец г. Екатеринбурга А. Кирсанов стал первым приговоренным за читерство – продажу вредоносных программ (читов) для игр, которые дают геймеру преимущество над другими участниками-игроками. Злоумышленника удалось выявить благодаря контрольной закупке. Фигурант создал сайт, на котором с 2015 по 2021 г. продавал вредоносные боты автоприцеливания – программы для игр World of Tanks и World of Warships – стоимостью от 25 руб. до более 2 тыс. руб. В отношении злоумышленника было возбуждено уголовное дело по ч. 2 ст. 273 УК РФ за создание и распространение вредоносных компьютерных программ. Ущерб разработчику игр от действий обвиняемого следствие оценило в 670 млн руб. Верх-Исетский районный суд г. Екатеринбурга приговорил А. Кирсанова к 2,5 годам ограничения свободы[4]. При этом покупатели читов, модифицирующих лицензионный программный продукт, остались безнаказанными, что противоречит идее справедливости как мере регулирования должного в праве. *По-прежнему остается без внимания со стороны законодателя проблема отсутствия уголовной репрессии за приобретение вредоносных компьютерных программ, информации, цифровых кодов, которые могут быть использованы для незаконного копирования, изменения компьютерной информации, несанкционированного доступа к компьютеру, его средствам защиты. Без должного запрета приобретения вредоносной информации сложно будет остановить ее создание и распространение, так как спрос рождает предложение. Это требует внесения изменений в ст. 273 УК РФ и криминализации незаконного приобретения вредоносных компьютерных программ, что гармонизирует принципы законности и равенства граждан перед законом в рассматриваемой нами ситуации*.

Компьютерные вирусы, программы-шпионы могут предназначаться не только для модификации или копирования информации без согласия их владельца, но и для иных целей, не обозначенных в ч. 1 чт. 273 УК РФ, в том числе для сбора данных о пользователях ЭВМ. *В этом контексте целесообразно изменить формулировку части 1 диспозиции рассматриваемой*

[4] Суд в России впервые вынес приговор за читы в компьютерных играх [Электронный ресурс] // Деловая газета «Взгляд». – URL: https://vz.ru/news/2022/7/7/1166547.html. (дата обращения: 31.07.2022).

статьи и установить запрет создания, распространения, приобретения, использования компьютерных программ и компьютерной информации, заведомо созданных для выполнения или способствующих выполнению несанкционированных действий в информационной системе, которые создают угрозу причинения вреда. Под вредоносной компьютерной программой следует понимать код или его часть, специально созданные для выполнения или способствующие выполнению несанкционированных действий в информационной системе, которые могут привести к причинению вреда. Отсутствие легального определения понятия «вредоносная компьютерная программа» является законодательным пробелом, что требует устранения путем закрепления его в примечании к ст. 273 УК РФ.

Кроме того, в теории и на практике не теряет своей значимости проблема определения предмета преступления, предусмотренного ст. 272 УК РФ, что приводит к ошибкам в правоприменении. Многие представители правоохранительных органов, как показывает практика, ошибочно полагают, что в ст. 272 УК РФ идет речь о текстовой информации, которая может считываться с компьютера, размещаться в электронной или бумажной форме на материальных носителях. Под компьютерной информацией для целей главы 28 УК РФ понимаются сообщения, данные в форме электрических сигналов в виде системного и прикладного программного обеспечения, которое отвечает за функционирование компьютера и поиск, обработку и пересылку информации. В статье четко представлены способ хранения/передачи компьютерной информации, но сложность применения закона обнаруживается тогда, когда необходимо ответить на вопрос: что признается охраняемой информацией? Ответ на него содержит специальное законодательство об информации, информационных технологиях и защите информации.

Кроме того, безнаказанность порождает отсутствие в уголовном законе эффективных мер ответственности за сам факт неправомерного доступа к компьютерной информации, если он совершен путем ее копирования и записи на электронный носитель (диск, флешку). При этом во внимание принимается не стоимость похищенной информации, а цена ее носителя, которая, как правило, малозначительна. В случае распространения такой информации применяются нормы уголовного закона, охраняющие банковскую, коммерческую тайну в зависимости от ценности и содержания скопированных и украденных данных.

Часть 4 статьи 272 УК РФ, как и особо квалифицированные составы ст. 273, 274 УК РФ, оперируют термином «тяжкие последствия», но конкретно их не называют, что затрудняет процесс правоприменения. Тяжкие последствия, но без создания угрозы их наступления упомянуты и в особо квалифицированном составе ст. 274.1 УК РФ. Предлагаем отказаться от этих оценочных критериев, заменив их последствиями, имеющими стоимостное выражение «крупный размер», «особо крупный размер», чтобы избежать ошибок со стороны судебных и следственных органов, дать возможность более четко дифференцировать уголовную ответственность и наказание.

Понятие «крупный ущерб» применяется в квалифицированных составах ст. 272, 273, 274 УК РФ. Размер крупного ущерба для статей главы 28 УК РФ составляет более 1 млн руб. Размер ущерба, который признается крупным за причинение вреда авторским и смежным правам (ч. 1, 2 ст. 146 УК РФ), равен 10 тыс. руб. Крупным размером ущерба, согласно примечанию 4 к ст. 158 УК РФ, признается стоимость имущества более 250 тыс. руб. Такая несоразмерность крупного ущерба для преступлений в сфере компьютерной информации (ч. 2 ст. 272, 273, ч. 1 ст. 274 УК РФ) и против собственности (ст. 158, 159, 163, 167 УК РФ), а также за нарушение интеллектуальных прав сужает возможности применения уголовно-правовой репрессии в борьбе с киберпреступностью. Хищение денег априори наказывается более сурово, чем блокирование информации о денежных активах, что приводит к невозможности их обналичивания и использования. Несложно представить, что компьютерная информация может обладать стоимостными признаками, выполнять роль денежных купюр и использоваться в качестве электронных средств платежа. Это вызывает необходимость определения единого подхода к установлению размера крупного ущерба для целей рассматриваемых статей, а также ужесточения санкции статей главы 28 УК РФ. *Предлагаем крупным в статьях главы 28 УК РФ признать ущерб, сумма которого превышает 250 тыс. руб., что будет соответствовать принципам равенства и гуманизма*.

Статья 274.1 УК РФ включает три самостоятельных состава преступлений, содержательно дублирующих объективную сторону составов 272, 273 и 274 УК РФ, за исключением предмета преступления. *Наиболее соответствовало бы правилам законодательной техники поместить в качестве квалифицирующего или особо квалифицирующего признака «посягательство на критическую информационную инфраструктуру» в ст. 272, 273, 274 УК РФ*.

Литература

1. ***Брандес М.Э.*** Идеология и миф: общие черты // Политическая наука. Политическая идеология в современном мире. – 2003. – № 4. – С. 39–47.
2. ***Городнова О.Н.*** Реализация уголовно-правовой идеологии при модернизации законодательства // Вестник Российского университета кооперации. – 2020. – № 2 (40). – С. 125–132.
3. ***Сверчков В.В.*** Идеология в отечественном уголовном праве (законодательстве) // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2011. – № 3 (16). – С. 201–204.
4. ***Челохсаев О.З.*** Современная уголовно-процессуальная политика: дис. ... канд. юрид. наук. – Москва, 2009. – 230 с.
5. ***Сабитов Т.Р.*** Система уголовно-правовых принципов: монография / отв. ред. А.И. Чучаев. – Москва: Проспект, 2012. – 130 с.
6. ***Тасаков С.В.*** Система уголовных наказаний нуждается в совершенствовании // Ученые записки Казанского университета. Серия: Гуманитарные науки. – 2016. – Т. 158. – № 2. – С. 605–616.
7. ***Городнова О.Н., Иванцова Н.В.*** Принцип справедливости – презумпция или фикция уголовного права? // Юридическая техника. – 2010. – № 4. – С. 123–129.

References

1. ***Brandes M.E.*** Ideologiya i mif: obshchie cherty // Politicheskaya nauka. Politicheskaya ideologiya v sovremennom mire. – 2003. – № 4. – S. 39–47.
2. ***Gorodnova O.N.*** Realizatsiya ugolovno-pravovoi ideologii pri modernizatsii zakonodatel'stva // Vestnik Rossiiskogo universiteta kooperatsii. – 2020. – № 2 (40). – S. 125–132.
3. ***Sverchkov V.V.*** Ideologiya v otechestvennom ugolovnom prave (zakonodatel'stve) // Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii. – 2011. – № 3 (16). – S. 201–204.
4. ***Chelokhsaev O.Z.*** Sovremennaya ugolovno-protsessual'naya politika: dis. ... kand. yurid. nauk. – Moskva, 2009. – 230 s.
5. ***Sabitov T.R.*** Sistema ugolovno-pravovykh printsipov: monografiya / otv. red. A.I. Chuchaev. – Moskva: Prospekt, 2012. – 130 s.
6. ***Tasakov S.V.*** Sistema ugolovnykh nakazanii nuzhdaetsya v sovershenstvovanii // Uchenye zapiski Kazanskogo universiteta. Seriya: Gumanitarnye nauki. – 2016. – T. 158. – № 2. – S. 605–616.
7. ***Gorodnova O.N., Ivantsova N.V.*** Printsip spravedlivosti – prezumptsiya ili fiktsiya ugolovnogo prava? // Yuridicheskaya tekhnika. – 2010. – № 4. – S. 123–129.

(статья сдана в редакцию 31.08.2022)