Научная статья
УДК 34:343.3/.7:004:654.1
EDN: https://elibrary.ru/fiseet
DOI: https://doi.org/10.21202/jdtl.2023.28

Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности

Евгений Александрович Русскевич

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Ключевые слова

Законодательство,
Интернет,
информационная безопасность,
киберпреступление,
киберустойчивость,
оператор связи,
право,
сеть связи,
уголовная ответственность,
цифровые технологии

Аннотация

Цель: получение нового знания об ответственности за нарушение правил управления техническими средствами противодействия угрозам информационной безопасности, разработка теоретических рекомендаций и предложений по совершенствованию законодательства и правоприменения.

Методы: методологическую основу исследования составляет совокупность методов научного познания, в том числе абстрактно-логический, догматический, сравнения и др.

Результаты: на основе изучения документов, изданий сделаны следующие выводы: 1) предпринятые на национальном уровне меры по регулированию отношений, связанных с внедрением технических средств противодействия угрозам, в целом соответствуют положениям Доктрины информационной безопасности Российской Федерации; 2) одним из основных направлений развития зарубежного законодательства о телекоммуникациях является построение системы государственно-частного взаимодействия, при котором операторы связи стали бы воспринимать проблему информационной безопасности не как их внутреннюю задачу, а как элемент общей безопасности государства. В этом отношении предельно четко прослеживается констатация необходимости эффективного контроля за деятельностью операторов связи, прежде всего в сфере вводимых технических стандартов обеспечения киберустойчивости; 3) регулирование отношений в сфере управления техническими средствами противодействия угрозам в России характеризуется многочисленностью, многоуровневостью и, соответственно, вполне

предсказуемой сложностью; 4) реализованная в ст. 274.2 Уголовного кодекса Российской Федерации модель ответственности представителей операторов связи за нарушения в области эксплуатации технических средств противодействия угрозам не представляется оптимальной. Довольно уязвимым является подход к описанию административно преюдициальных признаков состава. Несмотря на значимость отношений, возможность уголовно-правовой реакции на конкретный инцидент возникает не в связи с наступлением тех или иных общественно опасных последствий и даже не при традиционной повторности, а лишь при третьем задокументированном нарушении. Более предпочтительной представляется модель криминализации нарушения управления техническими средствами противодействия угрозам в зависимости от причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

Научная новизна: во многом определяется фактической неразработанностью вопросов, связанных с законодательным определением и реализацией уголовной ответственности за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования.

Практическая значимость: основные положения и выводы исследования могут быть использованы для совершенствования механизма уголовно-правовой охраны информационной безопасности, дальнейшего развития отечественной доктрины уголовного права об ответственности за преступления в сфере компьютерной информации.

Для цитирования

Русскевич, Е. А. (2023). Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности. *Journal of Digital Technologies and Law*, *1*(3), 650–672. https://doi.org/10.21202/jdtl.2023.28

Содержание

Введение
1. Методика исследования нарушения правил централизованного управления техническими средствами противодействия угрозам информационной безопасности
2. Информационная безопасность и технические средства противодействия угрозам
3. Регулирование в сфере централизованного управления техническими средствами противодействия угрозам информационной безопасности
4. Уголовная ответственность за нарушение централизованного управления техническими средствами противодействия угрозам информационной безопасности
Выводы
Список литературы

Введение

Цифровой мир является как настоящим, так и перспективным будущим человека. Его повседневная деятельность с неизбежностью предполагает взаимодействие с устройствами и технологиями, которые стремительно меняют представление о реальности. Через аккаунты, свои цифровые alter ego, человек коммуницирует, осуществляет трудовую деятельность, получает услуги, приобретает товары. В результате современный человек оказывается в положении параллельного бытия – физического и виртуального. Устраниться от этого, замедлить цифровизацию в известном смысле можно, но неизбежность и необратимость этого процесса заставляет задаться вопросом: а зачем это делать? Отвечая на него, отдельные исследователи указывают на негативные последствия внедрения телекоммуникационных технологий с точки зрения состояния и динамики преступности, изменения ее характеристик. Здесь, как правило, демонстрируется виртуализация механизма криминального оборота запрещенных предметов, существенно осложняющая деятельность правоохранительных органов. Кроме того, довольно обстоятельно раскрывается, что развитие отдельных направлений исследований (например, в сфере искусственного интеллекта и робототехники) обладает вполне конкретной угрозой для человечества в целом.

Пожалуй, все приведенное выше в известном смысле справедливо. Однако верно и то, что дискурс этот в целом не выходит за рамки традиционного для человека замешательства перед чем-то новым, неизведанным, природа которого и возможное влияние представляются не до конца ясными. Любая технология имеет перспективу своей эксплуатации в преступных целях. Это, однако же, не может отменить прогресса как такового, т. е. стремления человека к устройству своей жизни наиболее разумным образом. По этой причине надо говорить не о защите человека от технологий, а о построении модели защиты технологий, или, если точнее, модели правового обеспечения информационно-телекоммуникационного развития, которая позволила бы упреждать и адекватно реагировать на совершение конкретных преступных посягательств. В этом смысле вполне закономерно в центре внимания оказываются вопросы качественного обеспечения устойчивости цифровых сетей по отношению к негативному воздействию или их киберустойчивости.

Федеральным законом от 14 июля 2022 г. № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» глава 28 Уголовного кодекса Российской Федерации[1] (далее – УК РФ) была дополнена новой нормой, устанавливающей ответственность за нарушение специальных правил управления техническими средствами, обеспечивающими нормальное функционирование на территории государства сети Интернет и сетей связи общего пользования (ст. 274.2 УК РФ). Изучение паспорта законопроекта не позволяет ознакомиться с обоснованием реализованной законодательной инициативы – в первоначальной редакции выделение ст. 274.2 УК РФ не планировалось. Соответствующие дополнения появились только ко второму

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. (1996, 17 июня). *Собрание законодательства Российской Федерации*, 25, ст. 2954.

чтению законопроекта[2]. Вместе с тем крайне важно не только разобраться в причинах, побудивших к решению о криминализации отдельных нарушений, связанных с управлением техническими средствами противодействия угрозам (далее – ТСПУ), но и проанализировать юридико-технические особенности ст. 274.2 УК РФ, выявить ее достоинства и возможные недостатки.

1. Методика исследования нарушения правил централизованного управления техническими средствами противодействия угрозам информационной безопасности

Методологический инструментарий исследования представлен комплексным сочетанием философских, общенаучных и частнонаучных средств познания. Из общенаучных методов научного познания были использованы такие, как анализ, синтез, дедукция, индукция, классификация, структурно-функциональный метод и др. Особое значение в методологии проведенного исследования было отведено системному методу, который выступал исходной посылкой при решении всех поставленных исследовательских задач.

Эмпирические методы (анализ документов, печатных и электронных изданий) были задействованы при накоплении и изучении материалов исследования. В процессе подготовки статьи было направлено письмо в федеральное государственное унитарное предприятие «Главный радиочастотный центр»[3] (далее – ФГУП «ГРЧЦ») в целях получения разъяснений о ТСПУ (получен официальный ответ на обращение от 25 декабря 2022 г.).

В ряду частнонаучных методов познания были использованы сравнительно-правовой, формально-юридический (догматический) и др. Формально-юридический метод применялся при непосредственном изучении нормативных правовых актов Российской Федерации в сфере регулирования и охраны информационных отношений, отечественного и зарубежного уголовного законодательства. Использование догматического метода позволило решить целый ряд исследовательских задач, связанных, например, с выявлением юридико-технической определенности признаков ст. 274.2 УК РФ.

2. Информационная безопасность и технические средства противодействия угрозам

Для понимания процессов, приведших к появлению в отечественном уголовном законодательстве специальной нормы об ответственности за нарушение централизованного управления ТСПУ (ст. 274.2 УК РФ), следует прежде всего обратиться к категории информационной безопасности и документам стратегического планирования в этой сфере.

---

2 Законопроект № 130406-8 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (в целях совершенствования уголовно-правовой охраны национальных интересов Российской Федерации, прав и свобод граждан от новых форм преступной деятельности и угроз государственной безопасности). https://sozd.duma.gov.ru/bill/130406-8

3 ФГУП «ГРЧЦ» представляет собой отраслевой экспертный центр, обеспечивающий выполнение задач и функций, возложенных на радиочастотную службу, а также сопровождение контрольно-надзорных и регуляторных функций Роскомнадзора по основным направлениям его деятельности в области связи и в сфере средств массовой информации и массовых коммуникаций. https://grfc.ru

В отечественной литературе информационная безопасность разработана обстоятельно[4]. М. А. Ефремова справедливо подчеркивает, что информационная безопасность являет собой динамическую систему общественных отношений. Открытость этой системы обусловлена тем, что информационная безопасность не может иметь постоянный, неизменный характер (Ефремова, 2018).

Категория информационной безопасности (в более узком смысле – киберустойчивости) хорошо исследована и в зарубежной литературе (Colding et al., 2020; Espinoza-Zelaya & Moon, 2022; Hausken, 2020; Li et al., 2020; Prasad & Moon, 2022; Tonhauser & Ristvej, 2019; Tsao et al., 2022).

Как известно, информационная безопасность имеет нормативное определение в Доктрине информационной безопасности Российской Федерации[5]. В соответствии с данным документом «информационная безопасность представляет собой состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[6].

Задача обеспечения информационной безопасности, в том числе посредством действенного контроля за деятельностью операторов связи, в некотором смысле является понятной ровно настолько, чтобы можно было предположить отсутствие необходимости это отдельно обосновывать. Все отечественные операторы связи составляют единую сеть связи государства и обеспечивают целостность, доступность, в отдельных случаях конфиденциальность данных, устойчивость и безопасность информационно-коммуникационной инфраструктуры в целом. Как справедливо пишет по этому поводу А. К. Жарова, сеть Интернет, сети связи общего пользования, локальные сети, функционирующие на территории Российской Федерации, хотя и не являются государственными информационными системами, но обеспечивают доступ к информации, содержащейся в государственных информационных системах. Соответственно, безопасность функционирования таких технологий и каналов доступа должна быть обеспечена правовыми инструментами (Жарова, 2022).

Национальная безопасность больше не определяется исключительно военной составляющей и границами государства. Киберугрозы носят спорадический и многомерный характер, создают риски причинения колоссального ущерба. При этом эти угрозы нельзя предупредить только традиционными средствами, такими как применение военной силы или правоохранительного механизма, – требуется эффективное двустороннее сотрудничество между правительствами и частным сектором (Li & Liu, 2021).

---

4 См., например: Калмыков, Д. А. (2005). *Информационная безопасность: понятие, место в системе уголовного законодательства Российской Федерации, проблемы правовой охраны*: дис. … канд. юрид. наук. Ярославль. https://elibrary.ru/nnomvb; Кубышкин, А. В. (2002). *Международно-правовые проблемы обеспечения информационной безопасности государства*: дис. … канд. юрид.наук. Москва; Лопатин, В. Н. (2000). *Информационная безопасность России*: дис. … д-ра юрид. наук. Санкт-Петербург.

5 Указ Президента РФ № 646 от 05.12.2016. (2016, 12 декабря). *Собрание законодательства Российской Федерации*, 50, ст. 7074.

6 *Там же*.

Несмотря на это, в России выстраивание архитектуры регулирования государственно-частного взаимодействия в этой области долгое время не реализовывалось. Соответственно, не ставился вопрос и об ответственности операторов связи за несоблюдение необходимых стандартов информационной безопасности. Нельзя сказать, что такие решения не вызревали в общественном сознании и не обсуждались как перспективные в профессиональном сообществе. Дискуссия велась довольно активно, но, как это часто бывает, для непосредственной реализации потребовались изменение социальных условий и формирование актуального запроса в векторе обеспечения государственной безопасности.

Нетрудно понять, почему соответствующие изменения российского уголовного законодательства о введении ответственности за нарушение использования ТСПУ появились именно на этом этапе. За последнее время кибератаки на информационную инфраструктуру возросли многократно (Ельчанинова, 2020; Трунцевский, 2019; Красинский, Машко, 2023; Бокшицкий, Мельцева, 2017), в том числе в условиях пандемии коронавируса (Lallie et al., 2021; Hoheisel et al., 2023; Хисамова, Бегишев, 2022). При этом они имеют сложный характер, свидетельствующий о тщательной подготовке таких действий, наличии у злоумышленников высоких компетенций и дорогостоящего оборудования (Horsman, 2021; Kouloufakos, 2023; Boughton, 2019). Роскомнадзор сослался на это в своих комментариях относительно рассматриваемых законодательных новелл. В частности, было отдельно отмечено, что «в условиях гибридной войны, включающей элементы информационного противостояния, а также регулярные кибератаки, защита информационного пространства России является критически важной для государства и общества. В связи с этим необходимо безусловное выполнение операторами связи требований к установке, эксплуатации и модернизации ТСПУ и требований к пропуску всего трафика через них. Все технические средства противодействия угрозам находятся под управлением Центра мониторинга и управления сетью связи общего пользования (далее – ЦМУ ССОП), обеспечивающего отражение информационных атак»[7].

Другим обстоятельством является то, что в условиях нарастающей международной напряженности и информационного противоборства особую значимость приобрело соблюдение вводимых ограничений по доступу к отдельным сетевым ресурсам. Иными словами, потребовалось не только поставить поток информации под технологический контроль (фильтрацию), выстроить барьеры, препятствующие доступу пользователей к конкретному трафику и мобильным приложениям, но и действенным образом обеспечить ответственность представителей операторов связи за уклонение от исполнения этих стандартов. В этом ключе были даны и пояснения Роскомнадзора: «Нередки случаи, когда операторы пропускают трафик в обход ТСПУ, по тем или иным причинам допускают отключение такого оборудования. Это может представлять угрозу устойчивому функционированию Интернета в России, привести к сбою в работе информационных ресурсов государственных органов. При отключении ТСПУ или пропуске трафика в обход российские пользователи получают доступ к информации, представляющей опасность: детской порнографии, пронаркотическому контенту, пропаганде самоубийства, фейкам, экстремистской информации»[8].

---

[7] *В РКН заявили, что отказ операторов от использования ТСПУ представляет угрозу для граждан*. (2022, 15 июля). https://tass.ru/obschestvo/15228891

[8] *Там же*.

Принятие решения о построении системы мониторинга с использованием ТСПУ в целом соответствует положениям Доктрины информационной безопасности Российской Федерации, которая основными направлениями ее обеспечения определяет: противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации; пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами и др.

Немаловажно отметить, что предпринятые на национальном уровне меры по регулированию отношений, связанных с внедрением ТСПУ, в целом соответствуют тенденциям ряда зарубежных стран (Bitzer et al., 2023; Cascavilla et al., 2021; Mohamed, 2013; Nguyen & Golman, 2021; Broadhead, 2018; Qamar et al., 2023). В настоящей работе нет задачи дать развернутую характеристику тем процессам, которые происходят во всем мире. Вместе с тем сформировать некое общее представление о них все же необходимо хотя бы потому, чтобы лучше понимать ситуацию с обеспечением функционирования ТСПУ в России.

В определенном смысле российская модель регулирования и охраны отношений, связанных с внедрением и эксплуатацией ТСПУ, повторяет опыт Китайской Народной Республики (далее – КНР). Как совершенно справедливо отмечается в литературе, миллиардное количество пользователей сети Интернет в КНР предоставило государству большие экономические преимущества, но вместе с тем создает реальные угрозы для его экономической и политической безопасности (Дремлюга и др., 2017). Китай одним из первых столкнулся с рисками и оценил те «достоинства», которые возникают при сохранении курса на невмешательство в деятельность операторов телекоммуникационной связи на национальном уровне (Ye & Zhao, 2023). В настоящее время многие популярные зарубежные интернет-ресурсы в КНР заблокированы по причине того, что они осуществляют распространение информации, противоречащей идеологии Китая, морально-нравственным устоям общества, имеют признаки террористической либо экстремистской пропаганды. Более того, Закон КНР о безопасности сети Интернет 2016 г.[9] обязывает провайдеров требовать от пользователей регистрироваться под своими реальными именами, осуществлять фильтрацию контента и реализацию запретов на блокирование ресурсов, использовать только сертифицированное оборудование, исполнять требование о локализации данных пользователей, предоставлять техническую поддержку и содействие органам общественной и государственной безопасности и др. Нарушение соответствующих правил, обеспечивающих безопасность сетевого пространства КНР, может повлечь принудительное прекращение деятельности оператора связи, а равно привлечение ее сотрудников к ответственности, в том числе уголовной.

В отечественной литературе небезосновательно признается, что репрессивное китайское законодательство в интернет-сфере, кроме очевидного для западной

[9] *В Китае вступает в силу резонансный Закон о кибербезопасности*. https://ria.ru/20170601/1495523455.html

общественности нарушения прав и свобод, все же серьезным образом способствует «фильтрации» попадающего в китайский сегмент противоправного контента, защищая государственность и своих граждан от терроризма, экстремизма, сект, порнографии, насилия, подрывной деятельности иностранных разведок и т. п. (Лузянин, Трощинский, 2018).

В рамках Содружества Независимых Государств (далее – СНГ) подход, связанный с определением ответственности за нарушение правил использования ТСПУ, не получил своего распространения. В Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий[10] соответствующие рекомендации также отсутствуют. Пожалуй, наиболее близкими по содержанию являются положения ст. 2781 «Нарушение правил информатизации» Уголовного кодекса Республики Узбекистан[11].

20 декабря 2018 г. вступила в силу Директива (ЕС) 2018/1972 Европейского парламента и Совета от 11.12.2018 о Европейском кодексе электронных коммуникаций[12]. В соответствии с Директивой государства-члены должны обеспечить, чтобы поставщики общедоступных сетей электронной связи или общедоступных услуг электронной связи принимали надлежащие и пропорциональные технические и организационные меры для надлежащего управления рисками, связанными с безопасностью сетей и услуг. Принимая во внимание уровень техники, эти меры должны обеспечивать уровень безопасности, соответствующий существующему риску. Агентство Европейского союза по сетевой и информационной безопасности (ENISA) должно способствовать координации действий государств-членов во избежание расхождений в национальных требованиях, которые могут создавать риски безопасности и барьеры для внутреннего рынка. Государства-члены также должны обеспечить, чтобы поставщики общедоступных сетей электронной связи или общедоступных услуг электронной связи уведомляли без неоправданной задержки компетентный орган об инциденте безопасности, который оказал значительное влияние на работу сетей или услуг.

Государства-члены должны обеспечить, чтобы компетентные органы имели право издавать обязательные инструкции, в том числе касающиеся мер, необходимых для устранения инцидента безопасности или предотвращения его возникновения, поставщикам сетей электронной связи общего пользования или общедоступных услуг электронной связи. Государства-члены должны обеспечить, чтобы компетентные органы имели право требовать от поставщиков сетей электронной связи общего пользования или общедоступных услуг электронной связи: предоставлять информацию, необходимую для оценки безопасности своих сетей и услуг, включая документированные политики безопасности; подвергаться аудиту безопасности, проводимому квалифицированным независимым органом или компетентным органом, и предоставлять его результаты компетентному органу; стоимость аудита оплачивается поставщиком[13].

---

[10] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий. (2022, 15 августа). *Собрание законодательства Российской Федерации*, 33, ст. 5883

[11] https://lex.uz/docs/111457#111470

[12] *Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02018L1972-20181217

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972#d1e4938-36-1

Директива обусловила изменение законодательств стран Европейского союза о телекоммуникационных технологиях и защите данных. Так, например, в Германии 22 апреля 2021 г. был принят Telecommunications Modernization Act (TKMG). Кроме того, был принят Telecommunications Telemedia Data Protection Act (TTDSG) – Закон о защите данных в телекоммуникациях Германии, который сопровождается новым техническим руководством по осуществлению установленных законом мер по мониторингу телекоммуникаций. Новые требования безопасности к телекоммуникационной отрасли вводят категорию «критических компонентов телекоммуникаций». Эти компоненты могут использоваться только в том случае, если они были протестированы и сертифицированы официально признанным органом по сертификации и если производитель компонентов представил оператору сети «декларацию о надежности». В соответствии с новым регулирующим режимом операторы с повышенным потенциалом риска должны использовать соответствующие системы обнаружения вторжений (IDS) и/или обнаружения атак (ADS). Кроме того, соответствующие операторы должны проходить внешний аудит безопасности каждые два года[14].

В Великобритании 17 ноября 2021 г. был принят Закон о телекоммуникационной безопасности (Telecommunications (Security) Act 2021)[15]. Этим законом были внесены изменения в Закон о связи 2003 г.[16] В ряду наиболее значимых положений следует назвать прямое определение в ст. 105A обязанностей операторов связи выявлять угрозы киберустойчивости и предпринимать меры, направленные на их преодоление и предупреждение. Кроме того, в ст. 105B предусмотрена обязанность операторов связи исполнять предписания государственного регулятора. В ст. 105E закреплено, что орган государственного контроля обладает полномочиями по подготовке и принятию правил обеспечения киберустойчивости. Соответствующие правила, закрепляющие технические стандарты безопасности и конкретные практики, являются обязательными для исполнения провайдерами. Функциями по непосредственному контролю и надзору за исполнением правил наделено Управление связи OFCOM.

За нарушения правил и стандартов телекоммуникационной безопасности, уклонение от исполнения предписаний OFCOM предусмотрены значительные штрафы, в том числе оборотные. Закон о связи Великобритании только в ст. 404 оговаривает вопрос о возможном привлечении к уголовной ответственности руководителя компании, «если деяние совершено юридическим лицом и доказано, что оно было совершено с согласия или при попустительстве, или было связано с каким-либо пренебрежением со стороны директора, менеджера, секретаря или другого лица, выполняющего управленческие функции».

14 июня 2022 г. в Канаде было инициировано обсуждение законопроекта (Bill C-26), направленного на внесение изменений в Закон о телекоммуникациях[17]. Его целью является укрепление безопасности государства, а также обеспечение киберустойчивости телекоммуникационной инфраструктуры посредством представления соответствующим государственным структурам новых полномочий

14 https://www.gesetze-im-internet.de/ttdsg/

15 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted

16 https://www.legislation.gov.uk/ukpga/2003/21/contents

17 https://www.parl.ca/legisinfo/en/bill/44-1/C-26

относительно контроля за деятельностью операторов связи. Изучение законопроекта позволяет сделать вывод, что перечень таких полномочий крайне широк и предполагает не только надзор за соблюдением принятых стандартов безопасности, но и возможность налагать запреты на использование отдельного оборудования, предоставлять услуги связи отдельным пользователям и др. Надо сказать, что законопроект вызвал активное обсуждение. Так, было опубликовано открытое письмо министру общественной безопасности, в котором отмечалось, что законопроект C-26 уполномочивает правительство тайно приказывать операторам связи «делать что-либо или воздерживаться от чего-либо». Это открывает дверь для наложения обязательств по надзору на частные компании и на другие риски, такие как ослабление стандартов шифрования – то, что общественность уже давно отвергает как несовместимое с нашими правами на неприкосновенность частной жизни»[18]. Профессиональное сообщество заявило о существенном и неоправданном ограничении свободы экономической деятельности, а также о том, что предлагаемые стандарты попросту разорят малых участников рынка телекоммуникационных услуг. До настоящего времени законопроект не принят.

Таким образом, если попытаться в самом общем виде определить направление развития зарубежного законодательства о телекоммуникациях, то можно сделать вывод, что оно заключается в попытке выстроить систему государственно-частного взаимодействия, при котором операторы связи стали бы воспринимать проблему информационной безопасности не как их внутреннюю задачу, а как элемент общей безопасности государства. В этом отношении предельно четко прослеживается констатация необходимости эффективного контроля за деятельностью операторов связи, прежде всего в сфере вводимых технических стандартов обеспечения киберустойчивости.

3. Регулирование в сфере централизованного управления техническими средствами противодействия угрозам информационной безопасности

Обязанность оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети Интернет, обеспечивать установку в своей сети ТСПУ предусмотрена п. 5.1 ст. 46 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[19]. Соответствующее положение впервые появилось в отечественном законодательстве с принятием Федерального закона от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”»[20].

Важно отметить, что сама законодательная инициатива явилась ответом на Стратегию национальной кибербезопасности США, принятую в сентябре 2018 г. Как отмечается в пояснительной записке к законопроекту: «В подписанном Президентом США документе декларируется принцип “сохранения мира силой”. Россия же впрямую и бездоказательно обвиняется в совершении хакерских атак, откровенно

18 https://ccla.org/privacy/joint-letter-of-concern-regarding-bill-c-26/

19 (2003, 14 июля). *Собрание законодательства Российской Федерации*, 28, ст. 2895.

20 http://publication.pravo.gov.ru/Document/View/0001201905010025

говорится о наказании: “Россия, Иран, Северная Корея провели ряд безответственных кибератак, которые нанесли ущерб американским и международным компаниям, нашим союзникам и партнерам и не понесли соответствующего наказания, что могло бы сдерживать кибератаки в будущем”. В этих условиях необходимы защитные меры для обеспечения долгосрочной и устойчивой работы сети Интернет в России, повышения надежности работы российских интернет-ресурсов. Определяются необходимые правила маршрутизации трафика, организуется контроль их соблюдения. Создается возможность для минимизации передачи за рубеж данных, которыми обмениваются между собой российские пользователи. Определяются трансграничные линии связи и точки обмена трафиком. Предусматривается возможность установки на сетях связи технических средств, определяющих источник передаваемого трафика. Технические средства должны будут обладать возможностью ограничить доступ к ресурсам с запрещенной информацией не только по сетевым адресам, но и путем запрета пропуска проходящего трафика»[21].

Закон от 1 мая 2019 г. № 90-ФЗ, также известный как Закон «О суверенном Рунете», вызвал принципиальные споры и даже протесты среди отдельных представителей отрасли и гражданского общества. Отмечалось, что его реализация создает неоправданные риски для конституционных прав и свобод граждан, потребует миллиардных затрат, угрожает конкуренции на рынке услуг связи и будет способствовать коррупционному поведению[22]. Ситуация, во многом аналогичная той, которая сложилась в связи с обсуждением законопроекта (Bill C-26) в Канаде, о чем уже было сказано ранее. Сейчас уже можно вполне уверенно заявить о том, что другого возможного решения для России по большому счету не оставалось. Конечно, создание единого контура защиты информационной инфраструктуры государства требует значительного финансирования. Нельзя не согласиться и с тезисом о принципиальном расширении контроля со стороны государства за активностью граждан в виртуальном пространстве. Вместе с тем здесь важен тот баланс, который и определяет состояние информационной безопасности как динамической системы, меняющейся под влиянием внешних условий.

Основным документом, определяющим в настоящее время регулирование в сфере управления техническими средствами обеспечения киберустойчивости цифровых сетей, является Постановление Правительства Российской Федерации от 12 февраля 2020 г. № 126 «Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования»[23].

Изучение данного нормативного акта позволяет сделать вывод, что механизм взаимодействия между радиочастотной службой и оператором связи имеет

---

21 Пояснительная записка «К проекту Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации». *СПС «КонсультантПлюс»*.

22 См.: Бизнес раскритиковал детали перехода к «суверенному рунету». (2019, 26 июня). *Коммерсант*. https://www.kommersant.ru/doc/4012730?ysclid=ldkccj43i272099969; Глава РСПП заявил о коррупциогенных рисках закона о «суверенном Рунете». (2019, 30 июля). *РБК*. https://www.rbc.ru/technology_and_media/30/07/2019/5d3f08389a7947ada3baf05b

23 (2020, 24 февраля). *Собрание законодательства Российской Федерации*, 8, ст. 1001.

многоэтапный характер. Правила предусматривают, что не позднее 90 календарных дней до планируемой даты установки ТСПУ оператору связи направляется запрос о предоставлении информации, включающей в себя: схемы построения сети связи оператора связи; технические характеристики средств связи оператора связи; места планируемой установки ТСПУ; количество каналов передачи данных с указанием физических свойств таких каналов, их технологии и пропускной способности; сведения о среднестатистической и максимальной загрузке каналов; сведения о структуре узла связи в месте планируемой установки ТСПУ; сведения о планах модернизации, реконструкции узла связи, ликвидации фрагмента сети связи; техническую информацию и технологические параметры средств связи операторов связи, необходимые для разработки проектной документации по установке и подключению ТСПУ.

Оператор связи обязан подготовить ответ на соответствующий запрос в течение 15 рабочих дней с момента его получения. При этом постановлением предусмотрена возможность направления оператору связи уточняющего запроса в течение семи рабочих дней после получения ответа. В таком случае оператор связи должен подготовить ответ в течение трех рабочих дней со дня получения запроса.

Соответствующая процедура обмена информацией в целом призвана обеспечить необходимую подготовку к реализации согласованного плана мероприятий по установке и (или) модернизации ТСПУ. С уголовно-правовой точки зрения интерес представляет квалификация действий должностных лиц оператора связи, которые сознательно уклоняются от предоставления соответствующей информации либо заведомо указывают недостоверные данные. Полагаем, что при наличии на то фактических оснований следует рассматривать возможность применения ст. 201 УК РФ и 327 УК РФ соответственно. И если в ситуации использования заведомо подложного документа все относительно ясно, то применительно к злоупотреблению полномочиями необходимо установить не только бездействие лица, но и наступление негативных последствий, например, связанных с масштабным сбоем в работе объектов информационно-коммуникационной инфраструктуры и т. п. При этом важным и очевидно непростым моментом реализации механизма уголовной ответственности будет установление наличия причинно-следственной связи между уклонением от предоставления данных, отсутствием ТСПУ на конкретных каналах связи и наступившими общественно опасными последствиями.

Важнейшее значение для применения положений административного и уголовного законодательства имеет п. 10 Правил, определяющий обязанности оператора связи при эксплуатации технических средств противодействия угрозам: обеспечить ТСПУ электропитанием; обеспечить техническую поддержку функционирования ТСПУ в части их подключения к своей сети связи, организации технологического канала связи для управления указанными средствами, в том числе в соответствии с техническими условиями установки ТСПУ; обеспечивать не позднее 48 часов с момента поступления требования радиочастотной службы доступ к ТСПУ представителям радиочастотной службы; не препятствовать радиочастотной службе осуществлять посредством использования специальных программных средств дистанционное управление ТСПУ; соблюдать требования к обеспечению функционирования ТСПУ, содержащиеся в эксплуатационной документации; обеспечить выполнение комплекса мер, направленных на безопасную эксплуатацию ТСПУ, в том числе предусматривающих исключение возникновения аппаратного, программного и физического воздействия неуполномоченных лиц на функционирование ТСПУ и др.

Изучение приведенных выше положений Правил позволяет сделать вывод, что в отдельных случаях привлечение представителей оператора связи к ответственности будет предполагать необходимость непосредственного указания на нарушение конкретных положений и требований, предусмотренных другими документами (например, инструкцией по взаимодействию уполномоченных лиц оператора связи с радиочастотной службой, эксплуатационной документацией оборудования и др.).

Технические условия установки, а также требования к сетям при использовании ТСПУ определены Приказом Роскомнадзора от 31 июля 2019 г. № 228 «Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам»[24].

В дополнение надо указать, что регулирование в части управления ТСПУ приведенными нормативными актами не исчерпывается и в настоящее время характеризуется многочисленностью, многоуровневостью и соответственно вполне предсказуемой сложностью. В ряду таковых следует отдельно отметить: Постановление Правительства Российской Федерации от 3 ноября 2022 г. № 1978 «Об утверждении требований к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и Правил функционирования и взаимодействия системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования с информационными системами и иными системами, в том числе с системами операторов связи»[25], Приказ Минкомсвязи России от 7 октября 2019 г. № 572 «Об утверждении требований к обеспечению функционирования точек обмена трафиком, включая требования к обеспечению устойчивого функционирования технических и программных средств связи, сооружений связи, а также порядка соблюдения требований, предусмотренных п. 4 ст. 56.2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[26] и др.

4. Уголовная ответственность за нарушение централизованного управления техническими средствами противодействия угрозам информационной безопасности

Следует предположить, что объектом преступления, предусмотренного ст. 274.2 УК РФ, выступают общественные отношения, связанные с эксплуатацией ТСПУ, и обеспечением устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования. Возникновение этих отношений между государством и операторами связи, как было показано выше, состоялось сравнительно недавно и имело соответствующие социально-правовые предпосылки.

---

24 http://publication.pravo.gov.ru/Document/View/0001201909120028

25 (2022, 14 ноября). *Собрание законодательства Российской Федерации*, 46, ст. 7995.

26 https://minjust.consultant.ru/documents/45269

Интересным представляется подход, согласно которому в современных условиях объектом преступлений в сфере компьютерной информации являются общественные отношения в сфере цифровой экономики и информационного общества (Дремлюга, 2022). В определенном смысле, опираясь на стратегические документы в сфере развития цифровой экономики России, с такой трактовкой можно согласиться. Пожалуй, его недостатком является лишь вполне очевидная обширность используемой терминологии, которая при определенных обстоятельствах не позволяет выделить специфику именно конкретной группы общественно опасных посягательств в рамках Особенной части УК РФ.

Предметом являются сами технические средства противодействия угрозам (ТСПУ). Следует отметить, что какой-либо перечень соответствующего оборудования в открытом доступе отсутствует. Согласно разъяснениям радиочастотной службы, сведения о данных устройствах составляют коммерческую тайну.

Часть 1 ст. 274.2 УК РФ предусматривает ответственность за нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости функционирования сети Интернет и сети связи общего пользования либо несоблюдение технических условий их установки или требований при использовании. Диспозиция является бланкетной и отсылает к Постановлению Правительства Российской Федерации от 12 февраля 2020 г. № 126[27].

Объективная сторона данного преступления предполагает как активное, так и пассивное поведение субъекта и может заключаться в воспрепятствовании дистанционному управлению радиочастотной службой техническим средствами противодействия угрозам; нарушении требований, содержащихся в эксплуатационной документации; отключении технических средств противодействия угрозам от электропитания; в блокировании доступа к соответствующему оборудованию представителям радиочастотной службы и др.

В ч. 2 ст. 274.2 УК РФ объективная сторона заключается в нарушении требований к пропуску трафика через технические средства противодействия угрозам. Соответствующие требования определены Приказом Минцифры России от 26 января 2022 г. № 44 «Об утверждении Требований к порядку пропуска трафика в сетях передачи данных»[28].

В соответствии с Постановлением Правительства Российской Федерации от 12 февраля 2020 г. № 127 «Об утверждении Правил централизованного управления сетью связи общего пользования»[29] оператор связи имеет право не направлять трафик через технические средства противодействия угрозам в следующих случаях: а) нарушение функционирования технического средства противодействия угрозам, при котором прекращается пропуск трафика через данное техническое средство, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам; б) нарушение функционирования технического средства противодействия угрозам, при котором параметры пропуска трафика не соответствуют параметрам, указанным в проектной документации на установку и функционирование

---

27 Постановление Правительства РФ № 126 от 12.02.2020. *Собрание законодательства Российской Федерации*, 8, ст. 1001.

28 http://publication.pravo.gov.ru/Document/View/0001202203010002

29 (2020, 24 февраля). *Собрание законодательства Российской Федерации*, 8, ст. 1002.

технических средств противодействия угрозам, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам; в) выявление информации или информационных ресурсов, доступ к которым не подлежит ограничению в соответствии с законодательством Российской Федерации, но доступ к которым ограничивается. Направление трафика помимо технических средств противодействия угрозам в иных случаях, не предусмотренных Постановлением № 127, может быть квалифицировано как нарушение требований к пропуску трафика по смыслу ч. 2 ст. 274.2 УК РФ.

Оба состава преступления сконструированы с использованием административной преюдиции и предполагают, что соответствующее нарушение правил должно быть допущено в период, когда лицо считается подвергнутым административному наказанию за правонарушения, предусмотренные квалифицированными видами ст. 13.42 Кодекса Российской Федерации об административных правонарушениях[30] (далее – КоАП РФ) и 13.421 КоАП РФ. Отягчающим признаком в обоих случаях выступает повторность административного правонарушения. Таким образом, по смыслу ст. 274.2 УК РФ признаки уголовно наказуемого деяния будут иметь место лишь при третьем нарушении правил централизованного управления ТСПУ.

С точки зрения законодательного описания деяние, предусмотренное ст. 274.2 УК РФ, относится к весьма многочисленной группе преступлений, связанных с нарушением специальных правил, двойственная природа которых, по меткому определению Н. И. Пикурова, характеризуется сочетанием проступка и преступления (как бы формат «юридической матрешки») (Пикуров, 2009).

Предложенная законодательная модель ответственности представителей операторов связи за нарушения в области эксплуатации ТСПУ не представляется оптимальной. Во-первых, довольно уязвимым является подход к описанию административно-преюдициальных признаков состава. Несмотря на значимость отношений, обеспечиваемых системой централизованного управления ТСПУ, возможность уголовно-правовой реакции на конкретный инцидент появляется не в связи с наступлением тех или иных общественно опасных последствий и даже не при традиционной повторности, а лишь при третьем задокументированном нарушении.

В продолжение данной мысли следует предположить, что напрасно законодатель отказался от модели криминализации нарушения управления ТСПУ в зависимости от причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства. Это в некотором смысле уже сейчас ставит вопрос о квалификации действий представителя оператора связи, который, используя свои управленческие полномочия, вмешался в функционирование ТСПУ, что в результате привело к наступлению значимых общественно опасных последствий (например, в результате кибератаки были утеряны персональные данные нескольких тысяч пользователей, выведена из строя информационная инфраструктура крупных хозяйствующих субъектов, похищены денежные средства в особо крупных размерах и т. п.). Полагаем, что при наличии признаков специального субъекта, предусмотренного ст. 201 УК РФ, предпочтение должно быть отдано в пользу применения именно данной нормы. На это, в частности, указывает и соотношение санкций ст. 274.2 УК РФ и 201 УК РФ.

---

30 (2002, 7 января). *Собрание законодательства Российской Федерации*, 1 (ч. I), ст. 1.

Субъект обоих преступлений специальный – должностное лицо, понятие которого сформулировано в примечании к ст. 274.2 УК РФ, – лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации, а равно индивидуальный предприниматель, подвергнутые административному наказанию за соответствующие деяния, предусмотренные Кодексом об административных правонарушениях Российской Федерации.

В исследуемой норме законодатель допускает не вполне удачное использование терминологии. Должностными лицами названы субъекты, обладающие управленческими функциями в коммерческой или иной организации (см. примечание к ст. 201 УК РФ). Таким образом, как бы утверждается два вида должностных лиц – в коммерческих и иных организациях, а также в государственных органах, органах местного самоуправления и т. д. (см. примечание к ст. 285 УК РФ).

Субъективная сторона напрямую не раскрыта в ст. 274.2 УК РФ. Принимая во внимание формальную конструкцию составов, следует сделать вывод, что субъективная сторона нарушения специальных правил по смыслу ч. 1 ст. 274.2 УК РФ и нарушения требований к пропуску трафика по ч. 2 ст. 274.2 УК РФ выражается виной в виде прямого умысла. При этом содержание мотивов и целей не влияет на квалификацию преступления.

В случае, когда соответствующие нарушения были допущены по неосторожности, вследствие небрежного отношения к соблюдению эксплуатационных требований и иных правил, содеянное в зависимости от обстоятельств дела может быть квалифицировано по ст. 274 УК РФ либо по ч. 3 ст. 2741 УК РФ.

Выводы

Подводя итог, следовало бы еще раз подчеркнуть, что само решение о создании в России замкнутого контура защиты информационной безопасности посредством внедрения ТСПУ и выстраивания соответствующей системы отношений между государством и операторами связи, можно только приветствовать. По большому счету неважно, какие конкретно внешние или внутренние причины приблизили реализацию реформы в сфере телекоммуникаций. Полагать, что «суверенный Рунет» есть сугубо российская история, экстраординарная реакция на экстраординарные обстоятельства, пожалуй, неверно. Этому способствовали гораздо более сложные и глубинные процессы. Подтверждением данной мысли является опыт ряда зарубежных стран, которые либо уже реализовали соответствующие реформы, либо активно продвигаются в этом направлении.

Вместе с тем модель уголовно-правового обеспечения отношений в сфере централизованного управления ТСПУ, получившую свое оформление в ст. 274.2 УК РФ, вряд ли можно признать свободной от недостатков и противоречий. И дело не только в продолжении весьма спорной ветки развития отечественного уголовного законодательства, связанной с расширением в Особенной части УК РФ составов с административной преюдицией. Хотя данный подход во многом исключил саму возможность дифференциации ответственности за данное преступление. Проблема в самом условии предварительного двукратного привлечения к административной ответственности за соответствующее деяние в течение года. Весьма уязвимым также является решение об использовании категории должностного лица, которому

законодатель решил придать свое «автономное» значение исключительно к ст. 274.2 УК РФ.

Востребованность и качество нормы довольно скоро будут верифицированы практикой. И в этом отношении стоит только полагаться на время. Доктрина же традиционно, надеясь на лучшее, должна готовиться к худшему, обсуждая и вырабатывая возможные перспективные шаги по изменению закона и преодолению проблем правоприменения.

Список литературы

Бокшицкий, В. И., Мельцева, И. С. (2017). Совершенствование защиты общественно значимых информационных ресурсов. *Вопросы кибербезопасности*, *S2*(20), 11–14. https://www.elibrary.ru/zvzggl

Дремлюга, Р. И. (2022). *Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение*: монография. Москва: Юрлитинформ. https://www.elibrary.ru/hsbxrm

Дремлюга, Р. И., Коробеев, А. И., Федоров, А. В. (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. *Всероссийский криминологический журнал*, *11*(3), 607–614. EDN: https://www.elibrary.ru/zhnbdp. DOI: https://doi.org/10.17150/2500-4255.2017.11(3).607-614

Ельчанинова, Н. Б. (2020). Защита критической информационной инфраструктуры как новый институт правового обеспечения информационной безопасности. *Информационное общество*, *2*, 58–65.

Ефремова, М. А. (2018). *Уголовно-правовая охрана информационной безопасности*: монография. Москва: Юрлитинформ. https://www.elibrary.ru/zihcgl

Жарова, А. К. (2022). Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях. *Безопасность бизнеса*, *1*, 19–26. EDN: https://www.elibrary.ru/mnaski. DOI: https://doi.org/10.18572/2072-3644-2022-1-19-26

Красинский, В. В., Машко, В. В. (2023). Кибертерроризм: криминологическая характеристика и квалификация. *Государство и право*, *1*, 79–91. EDN: https://www.elibrary.ru/omupsq. DOI: https://doi.org/10.31857/S102694520024122-5

Лузянин, С. Г., Трощинский, П. В. (2018). Обеспечение национальной безопасности Китая на современном этапе (нормативно-правовой аспект). *Журнал зарубежного законодательства и сравнительного правоведения*, *1*, 60–69. EDN: https://www.elibrary.ru/yshope. DOI: https://doi.org/10.12737/art.2018.1.8

Пикуров, Н. И. (2009). *Квалификация преступлений с бланкетными признаками состава*: монография. Москва: Российская академия правосудия.

Трунцевский, Ю. В. (2019). Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов. *Журнал российского права*, *5*(269), 99–106. EDN: https://www.elibrary.ru/krnlwx. DOI: https://doi.org/10.12737/art_2019_5_9

Хисамова, З. И., Бегишев И. Р. (2022). Цифровая преступность в условиях пандемии: основные тренды. *Всероссийский криминологический журнал*, *16*(2), 185–198. https://doi.org/10.17150/2500-4255.2022.16(2).185-198

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, *4*, 18–19. https://doi.org/10.1016/S1353-4858(19)30051-0

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, *103*, 102761. https://doi.org/10.1016/j.cities.2020.102761

Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, *55*(10), 2252–2257. https://doi.org/10.1016/j.ifacol.2022.10.043

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158. https://doi.org/10.1016/j.cose.2023.103158

Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, *61* (6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, 105809. https://doi.org/10.1016/j.clsr.2023.105809

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/j.clsr.2012.11.005

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, *55*(10), 2246–2251. https://doi.org/10.1016/j.ifacol.2022.10.042

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, *40*, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. D*iscourse, Context & Media*, *51*, 100666. https://doi.org/10.1016/j.dcm.2022.100666

Сведения об авторе

Русскевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
Адрес: 125993, Российская Федерация, г. Москва, ул. Садовая-Кудринская, 9
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование выполнено в рамках государственного задания «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023-0006)». Регистрационный номер: 1022040700002-6-5.5.1.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77.51 / Отдельные виды преступлений
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 6 февраля 2023 г.
Дата одобрения после рецензирования – 13 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.28

Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security

Evgeniy A. Russkevich

Kutafin Moscow State Law University
Moscow, Russian Federation

Keywords

Communication network,
communication operator,
criminal liability,
cyber resilience,
cybercrime,
digital technologies,
information security,
Internet,
law,
legislation

Abstract

Objective: to acquire new knowledge about the liability for violating the rules of managing technical means of counteracting the threats to information security; to elaborate theoretical recommendations and proposals for improving legislation and law enforcement.

Methods: the methodological basis of the research is a set of scientific cognition methods, including abstract-logic, dogmatic, comparison, etc.

Results: based on studying documents and publications, the following conclusions were made: 1) the measures taken at the national level for regulating the relations associated with introduction of technical means of counteracting the threats generally comply with the provisions of the Doctrine on information security of the Russian Federation; 2) one of the main directions of development of the foreign legislation on telecommunications is building a system of public-private interaction, in which communication operators would perceive the information security problem not as their internal task but as an element of the overall security of the state. In this regard, one may clearly trace the statement of the need to efficiently control the activities of communication operators, first of all, in the sphere of the newly introduced standards providing cyber resilience; 3) regulation of relations in the sphere of managing the technical means of counteracting threats in Russia is characterized by their multiplicity, multi-leveledness,

hence, rather predictable complexity; 4) the model of communication operators' liability for violations in the field of exploitation of technical means of counteracting threats, implemented in Article 274.2 Of the Russian Criminal Code, is not optimal. Rather disputable is the approach to describing the administratively prejudicial elements of crime. Despite the significance of the relations, the possibility of a criminal-legal reaction to a particular incident appears not in connection with the occurrence of certain publicly dangerous consequences and not even with the traditional recurrence, but only with the third documented violation. We consider more preferable the model of criminalization of violating the management of technical means of counteracting threats depending on infliction of substantial harm to the rights and legal interests of citizens or organizations, or the legally protected interests of the society or the state.

Scientific novelty: the novelty of the research is mainly due to the actual underdevelopment of the issues related to the legal definition and implementation of criminal liability for violating the rules of centralized management of technical means of counteracting the threats to sustainability, security and integrity of functioning of the telecommunication network Internet and the general purpose communication network in the territory of the Russian Federation.

Practical significance: the main provisions and conclusions of the research can be used for improving the mechanism of criminal-legal protection of information security, further development of the Russian doctrine of criminal law on liability for crimes in the sphere of computer information.

For citation

Russkevich, E. A. (2023). Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security. *Journal of Digital Technologies and Law, 1*(3), 650–672. https://doi.org/10.21202/jdtl.2023.28

References

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Bokshitskii, V., & Meltseva, I. (2017). Improving the protection of socially significant information resources. *Voprosy Kiberbezopasnosti*, *S2*(20), 11–14. (In Russ.).

Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, *2019*(4), 18–19. https://doi.org/10.1016/S1353-4858(19)30051-0

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, *103*, 102761. https://doi.org/10.1016/j.cities.2020.102761

Dremliuga, R. I. (2022). *Criminal-legal protection of digital economy and information society against cybercriminal infringements: doctrine, law, law enforcement*: monograph. Moscow: Yurlitinform. (In Russ.).

Dremliuga, R. I., Korobeev, A. I., & Fedorov, A. V. (2017). Cyberterrorism in China: Criminal Law and Criminological Aspects. *Russian Journal of Criminology*, *11*(3), 607–614. (In Russ.). https://doi.org/10.17150/2500-4255.2017.11(3).607-614

Efremova, M. A. (2018). *Criminal-legal protection of information security*: monograph. Moscow: Yurlitinform. (In Russ.).

Elchaninova, N. B. (2020). Protection of critical information infrastructure as a new institute of legally enforcing information security. *Information Society*, *2*, 58–65. (In Russ.).

Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, *55*(10), 2252–2257. https://doi.org/10.1016/j.ifacol.2022.10.043

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158. https://doi.org/10.1016/j.cose.2023.103158

Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Khisamova, Z. I., & Begishev, I. R. (2022). Digital crime in the context of a pandemic: main trends. *Russian Journal of Criminology*, *16*(2), 185–198. (In Russ.). https://doi.org/10.17150/2500-4255.2022.16(2).185-198

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, 105809. https://doi.org/10.1016/j.clsr.2023.105809

Krasinsky, V. V., & Mashko, V. (2023). Cyberterrorism: criminological characteristics and qualification. *State and Law*, *1*, 79–91. (In Russ.). https://doi.org/10.31857/S102694520024122-5

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Luzyanin, S. G., & Troshchinsky, P. V. (2018). Ensuring China's national security at the present stage (normative and legal aspect). *Journal of Foreign Legislation and Comparative Law*, *1*, 60–69. (In Russ.). https://doi.org/10.12737/art.2018.1.8

Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/j.clsr.2012.11.005

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Pikurov, N. I. (2009). *Qualification of crimes with blanket characteristics of the components of crime*: monograph. Moscow: Russian State Academy of Justice. (In Russ.).

Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, *55*(10), 2246–2251. https://doi.org/10.1016/j.ifacol.2022.10.042

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, *40*, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Truntsevsky, Yu. V. (2019). Unlawful impact on critical information infrastructure: the criminal liability of its owners and operators. *Journal of Russian Law*, *5*(269), 99–106. (In Russ.). https://doi.org/10.12737/art_2019_5_9

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. *Discourse, Context & Media*, *51*, 100666. https://doi.org/10.1016/j.dcm.2022.100666

Zharova, A. K. (2022).The legal regulation of relations in the sphere of prevention of possible information technology vulnerabilities. *Bezopasnost biznesa*, *1*, 19–26. (In Russ.). https://doi.org/10.18572/2072-3644-2022-1-19-26

Author information

Evgeniy A. Russkevich – Doctor of Juridical Sciences, Associate Professor, Professor of the Department of Criminal Law, Kutafin Moscow State Law University
Address: 9 Sadovaya-Kudrinskaya Str., 125993 Moscow, Russian Federation
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research was performed as part of a state order «Russian legal system under the realities of digital transformation of the society and state: adaptation and prospects of reacting to the modern challenges and threats (FSMW-2023-0006)». Registration number: 1022040700002-6-5.5.1.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 6, 2023
Date of approval – April 13, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023