DOI 10.47643/1815-1337_2020_11_182

НЕКОТОРЫЕ ПРОБЛЕМНЫЕ АСПЕКТЫ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАСОВ Валерий Александрович,
кандидат юридических наук, доцент кафедры земельного права и экологических экспертиз Красноярского государственного аграрного университета, доцент кафедры гражданского права и процесса Сибирского юридического института МВД России, действительный член РАЕН, член РАЮН, член Общественной палаты г. Красноярска, член Совета Красноярского регионального отделения общероссийской общественной организации «Ассоциация юристов России».
E-mail:vav.70@mail.ru;

МИХЕЕВ Денис Андреевич,
слушатель заочной формы обучения Сибирского юридического института МВД России, капитан полиции.
E-mail: vinny.90@mail.ru

Краткая аннотация: *в данной статье авторы, предприняли попытку научного анализа отдельных аспектов неправомерного воздействия на критическую информационную инфраструктуру в Российской Федерации. Актуальность данного научного исследования обусловлена реальной потребностью совершенствования уголовно-правовых норм об ответственности за преступления и административно-правовых норм в рассматриваемой сфере в целях создания эффективных механизмов уголовно-правового регулирования и административно-правового регулирования информационных правоотношений. Целесообразно, разработать и закрепить в КоАП РФ правовую норму о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации, содержащейся в КИИ РФ, если оно не повлекло причинение вреда КИИ РФ.*

Abstract: *In this article, the authors have made an attempt at a scientific analysis of certain aspects of the illegal impact on the critical information infrastructure in the Russian Federation. The relevance of this scientific study is due to the real need to improve criminal law norms on responsibility for crimes and administrative legal norms in the considered area in order to create effective mechanisms for criminal law regulation and administrative legal regulation of information legal relations. It is advisable to develop and consolidate in the Code of Administrative Offenses of the Russian Federation a legal norm on violation of the rules for the operation of storage, processing or transmission of computer information contained in the CII RF, if it did not cause harm to the CII RF.*

Ключевые слова: *киберпространство, глобальная сеть Интернет, уголовно-правовая ответственность, государственное принуждение, преступление, компьютерные преступления, компьютерные атаки, безопасность, информационные технологии, критически информационная инфраструктура, компьютерная информация, санкции, меры уголовно-правового воздействия.*

Keywords: *cyberspace, the global Internet, criminal liability, state coercion, crime, computer crimes, computer attacks, security, information technology, critical information infrastructure, computer information, sanctions, measures of criminal law.*

В последние два десятилетия Российское государство взяло курс на активную цифровизацию экономики, государства и общества. Одним из стратегических направлений государственной политики нашей страны по созданию условий для устойчивого развития цифровой экономики является обеспечение информационной безопасности государства и социума.

В сегодняшних реалиях достаточно часто появляется информация о хакерских атаках, которые грозят серьезными проблемами не только владельцам компьютеров, но и промышленным технологическим системам, и информационным системам жизнеобеспечения Российской Федерации, ее субъектов, муниципальных образований, и других объектов, входящих в критическую информационную инфраструктуру. Н.Р. Мехтиева пишет о том, что: «субъектами противостояния в кибервойне оказываются как отдельные государства, целенаправленно стремящиеся избежать военного столкновения путем перевода противоборства в информационную плоскость, так и анонимные интернет-сообщества, проводящие хакерские атаки против различных государств, их политических, экономических или информационных институтов». [1] Существуют даже специальные группировки, как например, Cloud Atlas, которая занималась кибершпионскими операциями, где главными целями хакеров были компании промышленной отрасли и правительственные организации России, Центральной Азии и отдельных регионов Украины (использование фишинговых спам рассылок и др.).[2] Следует согласиться с мнением Р.И. Захарченко и И.Д. Королева, которые полагают, что: «функционирование объектов критической информационной инфраструктуры в новой среде - киберпространстве, порождает новые уязвимости и угрозы, и требует разработки нового инструментария обеспечения устойчивости функционирование в условиях компьютерных атак».[3]

В последнее время, в информационном пространстве появляются заявления спецслужб США о причастности России к кибератакам на системы различных уровней власти США. Министр иностранных дел России С.В. Лавров, на пресс-конференции по итогам встречи глав МИД БРИКС, прокомментировал данную ситуацию: «Американские спецслужбы обвиняют в преступлениях группу хакеров под названием Energetic Bear, которая якобы действует в интересах России. Вопрос касательно обвинения в адрес России, что мы вмешиваемся в президентские выборы в США, - это мы слышим уже многие

[1]Мехтиева Н.Р. Информационные войны как «цифровой» аспект глобализации // Век глобализации. 2017. №3. С. 77–89.

[2]Кибершпионская группа Cloud Atlas расширила свой арсенал полиморфной малварьо // Хакер. URL: https://xakep.ru (дата обращения: 25.10.2020).

[3]Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61.

годы. У них уже даже такая игра есть: кто больше вмешивается - Россия, Китай или Иран?.. Так что эти игры взрослых людей продолжаются давно, они нас не удивляют». [1]

Априори, все без исключения государства, пытаются создать действенные механизмы обеспечения безопасности инфраструктуры и информационных систем.[2] В России был принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»,[3] направленный на ее защиту.

Гражданское общество в современных реалиях - это постиндустриальное общество, в котором важнейшую роль играют наука, научно-технический прогресс и технология. Безусловно, это связано с компьютеризацией и развитием средств коммуникации в жизнедеятельности населения. Постоянное развитие и совершенствование компьютерной техники, специального программного обеспечения и глобальной сети Интернет имеет неотъемлемый положительный аспект эволюции информационных технологий.[4] Вместе с положительной реальностью в сеть Интернет проникла угроза противоправной деятельности, ставшая изнанкой виртуализации денежных отношений, безграничной коммуникации между пользователями, автоматизации товарных операций. На текущий момент наиболее остро стоят проблемы мошенничества, использования сети Интернет в незаконном обороте наркотиков, распространения идеологии экстремизма и терроризма, легализации доходов, добытых преступным путем.[5]

Телефоны, планшеты, телевизоры, фото и видео камеры (вебкамеры), автомобили, автоматизированные рабочие места, электронный документооборот и другое определяют изменение структуры человеческой деятельности. Распространение информационных технологий охватывает весь мир, об этом говорит статистика, почти 60 % населения Земли активно использует интернет в повседневной и рабочей деятельности.[6] Но, кроме простых - «физических» пользователей информационными технологиями также пользуются и государственные учреждения, российские юридические лица и индивидуальные предприниматели без образования юридического лица, которые обеспечивают работоспособность и взаимодействие различных систем – критически информационная инфраструктура (далее - по тексту КИИ), несанкционированное вмешательство в которые может нанести непоправимый вред.

Пункт «ж» статьи 71 Конституции РФ относит обеспечение безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных к ведению Российской Федерации[7] - это факт особой значимости. Об этом также прямо указано в Указе Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»,[8] в котором защита личности находится на одном уровне с обществом и государством.

Актуальность настоящей темы научного исследования вызвана развитием технических средств, которые в свою очередь определяют и развитие «новых» компьютерных преступлений,[9] что в свою очередь заставляет законодателя противостоять и изобличать данные преступные деяния.

Возникновение предпосылок определило принятие законодателем Федерального закона № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры», в котором определены основополагающие элементы «новой» сферы, а также принятие Федерального закона № 194-ФЗ от 26.07.2017 г. «О внесении изменений в УК РФ и статью 151 УПК РФ»[10], в результате чего в ст. 151 УК РФ подследственность уголовных дел (наряду со ст. 272, ст. 273 и ст. 274 УК РФ) передана органам ФСБ, а также органам, выявившим данное преступление – ст. 274.1 УК РФ.

В результате принятия указанных законов, законодательно была внесена весомая разница между ст.ст. 274 и 274.1 УК РФ. Во вновь появившейся норме отсутствовал факт причинения крупного ущерба, что во многом облегчило деятельность должностных лиц правоохранительных органов по документированию преступлений.

Обращает на себя внимание тот факт, что уголовно-правовые нормы, закрепляющие непосредственно ответственность за неправомерное воздействие на КИИ Российской Федерации конструктивно представлены триадой самостоятельных составов преступления (ч.ч. 1, 2, 3 ст. 274.1 УК РФ).

---

[1]Карпов А., Медведева А., Лобанов М. «Создать почву для новых санкций»: что стоит за очередными заявлениями спецслужб США о причастности России к кибератакам // https://russian.rt.com/world (дата обращения 20.10.2020).

[2] Курбатова С.М., Айснер Л.Ю. Национальная геоинформационная система - часть цифровой экономики // В сборнике: Современные проблемы землеустройства, кадастров и природообустройства. материалы Национальной научной конференции. ФГБОУ ВО «Красноярский государственный аграрный университет». Красноярск, 2020. С. 151-153.; Фастович Г.Г. Эффективность правоохранительной деятельности как критерий и качество функционирования государственного механизма // Аграрное и земельное право. 2018 г. № 2 (158). С. 11-15.

[3]Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) // URL: http://www.consultant.ru (дата обращения 20.09.2020).

[4]Власов В.А., Карлов А.Л., Прозорова Н.В. Уголовно-процессуальные средства обеспечения доступа к информации на технических устройствах: некоторые актуальные аспекты // Право и государство: теория и практика. 2019. № 11 (179). С. 145-147.

[5]Молоков В.В. Отдельные вопросы противодействия преступлениям в сфере нелегального оборота наркотиков, совершаемым с использованием сети Интернет // Научный компонент. 2019. № 1(1). С. 4-11.

[6]Вся статистика интернета на 2020 год - цифры и тренды в мире и в России //https://www.web-canape.ru (дата обращения 20.09.2020).

[7]Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения 20.09.2020).

[8]Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // URL: http://www.consultant.ru (дата обращения 20.09.2020).

[9]Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств: монография. СПб., 2016.

[10]Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 194-ФЗ // URL: http://www.consultant.ru (дата обращения 20.09.2020).

В период с 1 января 2018 г. по первое полугодие 2020 г. в Российской Федерации согласно данным Судебного Департамента ВС РФ за совершение преступлений, предусмотренных ч. 4 ст. 274.1 УК РФ было осуждено четыре лица. Из них все в 2019 году,[1] в отношении двух лиц, также в 2019 году за совершение преступлений, предусмотренных ч. 1 ст. 274.1 УК РФ, уголовные дела прекращены по иным основаниям по основной статье (в связи с деятельным раскаянием и добровольным возмещением ущерба). Три из четырех уголовных дел были выявлены в Дальневосточном Федеральном округе и только одно в Южном Федеральном округе. В июле 2020 вступили в законную силу еще два решения суда по преступлениям, предусмотренным ч. 2 и ч. 4 ст. 274.1 УК РФ (Амурская область,[2] и Республика Хакасия).[3] По одному уголовному делу за совершение преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, в Центральном районном суде г. Волгограда назначено заседание.[4]

Учитывая, что точка отправления, в части документирования преступлений правоохранительными органами, предусмотренных ст. 274.1 УК РФ положена с 2019 г., в свою очередь информация о фактах посягательств противоправной деятельности, в отношении лиц, деятельность которых не удалось задокументировать и/или доказать (факты «компьютерных» инцидентов на объектах КИИ) - является закрытой либо с ограниченным доступом, тем самым затрудняет анализ данных субъектами КИИ, а затем прагматично и действенно применить рациональные знания к материальным и людским ресурсам, что в свою очередь будет способствовать устойчивому функционированию при проведении в отношении субъекта КИИ компьютерных атак, а именно предотвращение.

Предметом преступлений, указанных в исследуемой статье, является охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации. Объект преступлений, закрепленных в ст. 274.1 УК РФ - безопасность КИИ РФ, поскольку КИИ может функционировать в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической, химической промышленности и других сферах, дополнительным объектом может быть информационная безопасность в любой сфере деятельности государства и общества. Субъективная сторона преступлений, предусмотренных частями 1 и 2 ст. 274.1, характеризуется прямым умыслом, а деяние, предусмотренное частью 3 ст. 274.1, может совершаться и по неосторожности. Субъект преступления, предусмотренного частью 3, - специальный: лицо, на которое возложена обязанность соблюдать правила эксплуатации соответствующих средств, систем и сетей, а также обязанность соблюдать правила доступа к соответствующим информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Государственная поддержка по поддержанию, развитию и улучшению организаций отсутствует, в связи с чем логично почему данную нишу, связанную

с защитой и разработкой конкретных мер безопасности субъектами КИИ мер безопасности заняли частные организации. Но первостепенно стоит отметить, что разработка данных мер носит не комплексный, а точечный характер, во многом это обусловлено Постановлением Правительства от 08.02.2018 г. № 127,[5] в котором представлен перечень категорий значимости.

Организационно-распорядительный порядок деятельности субъектов КИИ регламентирует в большей массе ФЗ-187, Постановление Правительства РФ от № 162 от 12.02.2018 г.,[6] а также взаимодействие в рамках предупреждения и ликвидации последствий компьютерных атак с органами ФСБ, которые надзирают за соблюдением защиты сведений осуществляющих государственную тайну. Следует упомянуть, что все преступления, выявленные с 2019 года по статье 274.1 УК РФ выявлены сотрудниками органов ФСБ.

Данные обстоятельства не способствует выработке единого подхода в практике и науке по применению ст. 274.1 УК РФ, что подтверждается разницей мнений. Принятие указанной статьи и практика привлечения к уголовной ответственности определило рассмотрение исследуемого преступления не по совокупности, а обособленно, что конечно идет вразрез с мнением ученых.[7] В результате отсутствия единства позиций, централизованной системы, способствующей обновлению данных и статистических сведений, затрудняет полноценное осуществление своих функций и задач субъектами КИИ, что в свою очередь создает условия для совершения преступлений заинтересованными лицами.[8]

[1]Данные судебной статистики / Судебный Департамент Верховного Суда Российской Федерации // URL: http:// http://www.cdep.ru (дата обращения 20.09.2020).
[2]Благовещенский городской суд Амурской области URL: https://blag-gs--amr.sudrf.ru (дата обращения 20.09.2020).
[3]Абаканский городской суд Республики Хакасия URL: https://abakansky--hak.sudrf.ru (дата обращения 20.09.2020).
[4] Центральный районный суд г. Волгограда URL: https://zent--vol.sudrf.ru (дата обращения 20.09.2020).

[5]Постановление Правительства РФ от 08.02.2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры российской федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (с изменениями от 13 апреля 2019 г.) // URL: https://fstec.ru (дата обращения 20.09.2020).
[6]Постановление Правительства РФ от № 162 от 12.02.2018 г. «Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // URL: https://fstec.ru (дата обращения 20.09.2020).
[7]Евдокимов К.Н. «Актуальные вопросы квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела» // Российский следователь. 2015. № 10. (дата обращения 20.09.2020).
[8] Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5.

Период избыточного ограничения доступа к информации, который затрудняет и ограничивает потребности субъектов КИИ, в свою очередь затрудняет выполнение требований законодательства РФ, может оказать негативное последствие на обеспечение безопасности КИИ, без использования положительного опыта. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ и повлекшее причинение вреда, указанное в ч. 3 ст. 274.1 УК РФ влечет уголовно-правовую ответственность, а в административном законодательстве административно-правовая ответственность не закреплена.

Соответственно, можно сделать следующий вывод: объекты критической информационной инфраструктуры требуют не только уголовно-правовой охраны, но и должны быть закреплены в КоАП РФ. Целесообразно, разработать и закрепить в КоАП РФ правовую норму о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации, содержащейся в КИИ РФ, если оно не повлекло причинение вреда КИИ РФ.

Библиография:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Консультант Плюс». URL: http://www.consultant.ru (дата обращения 20.09.2020).
2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) // URL: http://www.consultant.ru (дата обращения 20.09.2020).
3. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 194-ФЗ // URL: http://www.consultant.ru (дата обращения 20.09.2020).
4. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // URL: http://www.consultant.ru (дата обращения 20.09.2020).
5. Постановление Правительства РФ от 08.02.2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры российской федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (с изменениями от 13 апреля 2019 г.) // URL: https://fstec.ru (дата обращения 20.09.2020).
6. Постановление Правительства РФ от № 162 от 12.02.2018 г. «Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // URL: https://fstec.ru (дата обращения 20.09.2020).
7. Власов В.А., Карлов А.Л., Прозорова Н.В. Уголовно-процессуальные средства обеспечения доступа к информации на технических устройствах: некоторые актуальные аспекты // Право и государство: теория и практика. 2019. № 11 (179). С. 145-147.
8. Вся статистика интернета на 2020 год - цифры и тренды в мире и в России //https://www.web-canape.ru (дата обращения 20.09.2020).
9. Данные судебной статистики / Судебный Департамент Верховного Суда Российской Федерации. // URL: http:// http://www.cdep.ru (дата обращения 20.09.2020).
10. Евдокимов К.Н. «Актуальные вопросы квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела» // Российский следователь. 2015. № 10. (дата обращения 20.09.2020).
11. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61.
12. Карпов А., Медведева А., Лобанов М. «Создать почву для новых санкций»: что стоит за очередными заявлениями спецслужб США о причастности России к кибератакам // https://russian.rt.com/world (дата обращения 20.10.2020).
13. Кибершпионская группа Cloud Atlas расширила свой арсенал полиморфной малварьо // Хакер. URL: https://xakep.ru (дата обращения: 25.10.2020).
14. Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государств: монография. СПб., 2016.
15. Курбатова С.М., Айснер Л.Ю. Национальная геоинформационная система - часть цифровой экономики // В сборнике: Современные проблемы землеустройства, кадастров и природообустройства. материалы Национальной научной конференции. ФГБОУ ВО «Красноярский государственный аграрный университет». Красноярск, 2020. С. 151-153.
16. Мехтиева Н.Р. Информационные войны как «цифровой» аспект глобализации // Век глобализации. 2017. №3. С. 77–89.
17. Молоков В.В. Отдельные вопросы противодействия преступлениям в сфере нелегального оборота наркотиков, совершаемым с использованием сети Интернет // Научный компонент. 2019. № 1(1). С. 4-11.
18. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5.
19. Фастович Г.Г. Эффективность правоохранительной деятельности как критерий и качество функционирования государственного механизма // Аграрное и земельное право. 2018 г. № 2 (158). С. 11-15.
20. Благовещенский городской суд Амурской области // URL: https://blag-gs--amr.sudrf.ru (дата обращения 20.09.2020).
21. Абаканский городской суд Республики Хакасия // URL: https://abakansky--hak.sudrf.ru (дата обращения 20.09.2020).
22. Центральный районный суд г. Волгограда // URL: https://zent--vol.sudrf.ru (дата обращения 20.09.2020).