Научная статья
УДК 343.98
https://doi.org/10.36511/2078-5356-2024-4-180-185

Актуальные способы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Янгаева Марина Олеговна[1], Шепель Наталья Вячеславовна[2]
[1]Барнаульский юридический институт МВД России, Барнаул, Россия,
[2]Калининградский филиал Санкт-Петербургского университета МВД России, Калининград, Россия,
[1]marina-ymo@mail.ru
[2]shepelnv@mail.ru

Аннотация. Авторы, опираясь на статистические данные, а также практический опыт, определяют неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации как активно развивающееся направление. В статье проиллюстрированы три наиболее часто встречающихся способа воздействия на объекты критической информационной инфраструктуры Российской Федерации: *DDOS*-атака, заражение вредоносным программным обеспечением, использование уязвимостей программного обеспечения и оборудования субъекта критической информационной инфраструктуры Российской Федерации.

Ключевые слова: критическая информационная инфраструктура Российской Федерации, способ совершения преступления, вредоносное программное обеспечение, несанкционированный доступ, *DDOS*-атака, информационная безопасность

Для цитирования: Янгаева М. О., Шепель Н. В. Актуальные способы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 4 (68). С. 180–185. https://doi.org/10.36511/2078-5356-2024-4-180-185.

Original article

Current methods of unlawful influence on the critical information infrastructure of the Russian Federation

Marina O. Yangaeva[1], Natalia V. Shepel[2]
[1]Barnaul Law Institute of the Ministry of Internal Affairs of Russia, Barnaul, Russian Federation,
[2]Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia, Kaliningrad, Russian Federation,
[1]marina-ymo@mail.ru
[2]shepelnv@mail.ru

Abstract. The authors, relying on statistical data and practical experience, define illegal impact on the critical information infrastructure of the Russian Federation as an actively developing area. The article illustrates three most common methods of impact on objects of the critical information infrastructure of the Russian Federation: DDOS attack, infection with malware, exploitation of vulnerabilities in software and equipment of a subject of the critical information infrastructure of the Russian Federation.

Keywords: critical information infrastructure of the Russian Federation, method of committing a crime, malicious software, unauthorized access, DDOS attack, information security

For citation: Yangaeva M. O., Shepel N. V. Current methods of unlawful influence on the critical information infrastructure of the Russian Federation. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 4 (68), pp. 180-185. (In Russ.). https://doi.org/10.36511/2078-5356-2024-4-180-185.

В условиях складывающейся геополитической обстановки, усиления давления со стороны Запада, в том числе в информационном поле, особую актуальность приобретает вопрос обеспечения безопасности информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления объектов, функционирующих в различных сферах жизнедеятельности: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Основным методом противоправного воздействия по-прежнему остается проведение различных компьютерных атак в целях выведения из строя информационной инфраструктуры российских организаций независимо от форм собственности, нарушение государственного управления, нанесение ущерба российской экономике, подрыв авторитета власти и создание социальной напряженности. Наиболее атакуемыми в Российской Федерации являлись информационные ресурсы органов государственной власти, организаций сфер связи, науки и образования, промышленности и транспорта [1].

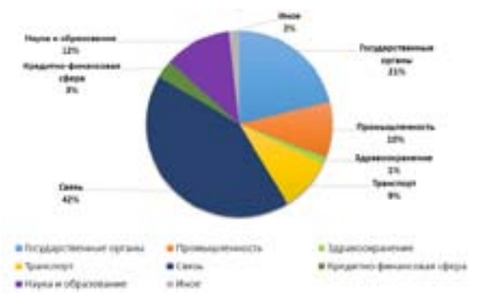

Рис. 1. Статистические данные атакуемых ресурсов Российской Федерации

По информации Лаборатории Касперского, основанной на данных статистики компьютерных инцидентов, выявленных у пользователей *Kaspersky Managed Detection and Response*, за первые шесть месяцев 2024 года в России и СНГ количество киберинцидентов на объектах критической информационной инфраструктуры Российской Федерации (далее — КИИ РФ) выросло на 39 % по сравнению с аналогичным периодом 2023 года. С наибольшим числом таких инцидентов столкнулись организации в сферах телекоммуникаций (рост более чем в 10 раз), строительства (рост в 2 раза) и информационных технологий (незначительное падение на 10 %). По общему числу всех зафиксированных инцидентов в лидерах организации в сфере телекоммуникации (340), СМИ (250) и здравоохранения (175) [2].

Для обеспечения устойчивого функционирования КИИ РФ и противодействия компьютерным атакам в отношении нее 26 июля 2017 года был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — ФЗ от 26 июля 2017 года № 187-ФЗ). Закон раскрывает понятие КИИ и определяет ее как «объекты КИИ, а также сетей электросвязи, используемые для организации взаимодействия таких объектов» [3, с. 87]. К объектам КИИ РФ закон относит информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ РФ.

Для противодействия противоправным деяниям, направленным на объекты КИИ РФ, федеральным законом от 26 июля 2017 года № 194-ФЗ [4] в Уголовный кодекс Российской Федерации (далее — УК РФ) была добавлена статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Ежегодно органами безопасности Российской Федерации фиксируется рост числа компьютерных инцидентов, в первую очередь перебор аутентификационной информации, попытки внедрения вредоносного программного обеспечения или эксплуатация уязвимостей, *DDoS*-атаки.

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 4 (68)

Проанализировав судебные статистические данные за 2020–2023 года (рис. 2) по вопросу осуждения лиц, совершивших преступление, предусмотренное статьей 274.1 УК РФ [5], пришли к выводу, что с 2022 года заметно увеличилось число осужденных по данной статье лиц, а значит и фактов неправомерного доступа на объекты критической информационной инфраструктуры Российской Федерации.

Год	ч. 1 274.1 УК РФ	ч. 2 274.1 УК РФ	ч. 3 274.1 УК РФ	ч. 4 274.1 УК РФ	ч. 5 274.1 УК РФ
2020	3	3	1	1	0
2021	2	1	2	10	0
2022	6	3	4	41	0
2023	10	4	4	61	0

Рис. 2. Статистические данные судов Российской Федерации по количеству осужденных по статье 274.1 УК РФ

Рост числа компьютерных инцидентов возник из ряда проблем обеспечения информационной безопасности, актуальность которой в условиях проведения специальной военной операции многократно возросла. Установлено, что данные проблемы формируются следующими основными факторами:

— пренебрежение руководителями организаций существующими требованиями и методическими рекомендациями в области информационной безопасности, отсутствие у данных должностных лиц, а также у сотрудников организаций понимания необходимости своевременного устранения обнаруживаемых угроз информационной безопасности;

— неконкурентоспособность отечественного аппаратного и программного обеспечения;

— внешнеполитическая обстановка;

— выполнение не в полном объеме и (или) с нарушением установленных сроков выданных органами безопасности России рекомендаций по нейтрализации актуальных угроз;

— нехватка специалистов в области информационной безопасности, следствием которой является возложение соответствующих обязанностей на непрофильных специалистов;

— отсутствие основополагающих документов в области обеспечения безопасности информации в организациях;

— недостаток знаний в области информационной безопасности у пользователей.

На регулярной основе органами безопасности России проводятся контрольно-технические мероприятия по оценке защищенности информационных систем и сетей и мероприятия по оценке степени защищенности от компьютерных атак информационных ресурсов, находящихся в зонах ответственности организаций различных сфер КИИ РФ. В более чем половине проверенных систем и сетей выявлены уязвимости и недостатки настройки, позволяющие внешнему и внутреннему злоумышленнику нарушить их штатное функционирование и (или) получить несанкционированный доступ к обрабатываемой информации.

Стоит отметить, что получение несанкционированного доступа не всегда осуществляется посредством использования хакерских навыков. В ряде случаев свою роль играл человеческий фактор, позволявший условному взломщику физически проникнуть на охраняемый объект и подключиться к внутренним информационным ресурсам с дальнейшим взломом.

Важность обеспечения безопасности объектов КИИ РФ трудно переоценить, так как нарушение их функционирования либо вывод из строя может привести к серьезным последствиям для безопасности государства и общества.

В данной статье не будем останавливаться на рассмотрении действующего законодательства в сфере КИИ РФ, лишь отметим, что разработанная система мер по обеспечению безопасности критической информационной инфраструктуры Российской Федерации при должном подходе позволяет адекватно реагировать на возникающие угрозы. Также поясним, что сам факт прохождения в соответствии с ФЗ от 26 июля 2017 года № 187-ФЗ [6] процедуры категорирования и последующего внесения объекта в реестр значимых объектов КИИ РФ не является целью и не обеспечивает безопасность.

Практика работы органов безопасности России свидетельствует о том, что чем большей зрелостью в вопросах обеспечения информационной безопасности обладал субъект (выполнение требований и методических рекомендаций по информационной безопасности, наличие в штате квалифицированных специалистов по информационной безопасности, своевременное устранение выявляемых уязвимостей и недостатков и т. д.), тем выше была его готовность к резкому возрастанию напряженности в российском информационном пространстве. В отношении таких субъектов возможности злоумышленников ограничивались лишь распределенными компьютерными атаками типа отказ в обслуживании на внешние

информационные ресурсы, периодически приводившими к непродолжительным нарушениям доступности данных информационных ресурсов, но не оказавшими существенное влияние на основную деятельность организаций.

Вместе с тем совокупность выявленных проблем позволяет говорить о том, что защищенность информационных ресурсов субъектов КИИ РФ от компьютерных атак остается недостаточной.

В качестве основных целей злоумышленников следует выделить:

— остановку (нарушение) производств и технологических процессов;

— получение информации об оборонном потенциале государства, объемах и характеристиках производимого вооружения;

— получение несанкционированного доступа к информационным ресурсам;

— нарушение предоставления государственных услуг;

— оказание информационно-психологического воздействия на население, в том числе для создания социальной напряженности, снижения привлекательности Российской Федерации в качестве внешнеторгового партнера.

Далее приведем наиболее часто встречающиеся способы воздействия на информационные ресурсы субъектов критической информационной инфраструктуры Российской Федерации:

1. Проведение *DDOS*-атак

В отдельных случаях в целях обхода средств защиты и блокировок злоумышленниками использовались малораспространенные подходы к проведению *DDoS*-атак, например единовременное повышение нагрузки на целевой сайт с задействованием легитимных сервисов (перевода текстов, проверки доступности хостов, скорости работы сайтов и др.).

Так, в период проведения Петербургского международного экономического форума 2022 года наблюдались вызванные *DDoS*-атаками перебои функционирования информационных ресурсов организаций, задействованных в проведении мероприятия. В частности, был выведен из строя сегмент информационно-телекоммуникационной сети, отвечавший за аккредитацию участников мероприятия, что привело к задержке выступления Президента Российской Федерации примерно на 1 час.

2. Заражение вредоносным программным обеспечением (далее — ВПО)

Наибольшее число компьютерных инцидентов, связанных с внедрением ВПО, было выявлено на объектах государственных органов и оборонной промышленности. Основным способом доставки модулей ВПО являлись целевые рассылки фишинговых сообщений. Таким образом, можно выделить следующие виды:

— целевая рассылка фишинговых сообщений, содержащих ссылки для загрузки ВПО, на официальные адреса электронной почты организаций. В письмах использовалась тематика, связанная с СВО, в частности некоторые вредоносные файлы доставлялись под видом повесток в военкомат в рамках частичной мобилизации. Такие действия злоумышленников зафиксированы в 40 организациях в различных федеральных округах Российской Федерации. В ряде случаев подтверждены факты успешного внедрения модулей ВПО и несанкционированной передачи информации;

— в областной медицинский информационно-аналитический центр одного из субъектов Российской Федерации было удаленно установлено ВПО, осуществляющее компьютерную атаку на информационные ресурсы многофункционального центра предоставления государственных услуг. Кроме того, в результате несанкционированного доступа к почтовому серверу республиканского учреждения здравоохранения была произведена рассылка более 760 тысяч сообщений электронной почты мошеннического характера;

— зафиксированы утечки данных государственных органов, персональных данных клиентов крупных операторов связи, компаний, осуществляющих почтовую связь и курьерскую деятельность, сервисов доставки еды и товаров, медицинских организаций, транспорта, компаний сферы услуг, средств массовой информации и др.;

— некомпетентность системного администратора в совокупности с практически отсутствующей защитой корпоративной сети привела к заражению вирусом-шифровальщиком информационной сети муниципального предприятия и фактической блокировке финансовых потоков организации. Кроме того, возможности ВПО позволяли получить доступ к системе управления светофорным оборудованием крупного регионального центра, неправомерное использование которого могло привести к образованию транспортного коллапса и большим человеческим жертвам вследствие дорожно-транспортного происшествия;

— несоблюдение элементарных требований безопасности, касающихся регулярного обновления парольной именной группы и сохранения высокого уровня защиты от случайного подбора, приводило к получению несанкционированного доступа к системам видеонаблюдения предприятий и организаций.

3. Использование уязвимостей программного обеспечения и оборудования субъектов КИИ РФ:

— незадекларированные возможности оборудования автоматической пожарной сигнализации, систем оповещения и управления эвакуацией со встроенным *GSM*-модулем, технические характеристики которых позволяют определять местоположение по географическим координатам и принимать различные команды из центра управления за рубежом, что использовалось иностранной стороной для целеуказания;

— фиксировались факты использования заложенных производителями незадекларированных возможностей медицинского оборудования и информационных систем в одном из учреждений, подведомственных Федеральному медико-биологическому агентству России, вследствие чего получен несанкционированный доступ к программному обеспечению томографа производства компании *Siemens* с последующим выведением его из строя. Доступ к оборудованию осуществлялся из-за пределов России;

— в результате эксплуатации уязвимости с последующим получением несанкционированного доступа к информационным ресурсам АО «Сервис-ТВ» была произведена подмена содержимого таблиц с телевизионным контентом, в расписании телепрограмм ряда крупных российских операторов телевидения размещены сообщения, содержащие недостоверную информацию в отношении проведения СВО на территории Украины;

— массовые факты подмены контента и (или) нарушения функционирования информационных ресурсов государственных органов, организаций сфер связи, промышленности, науки и образования, здравоохранения, транспорта, кредитно-финансовой сферы и средств массовой информации, произошедшие в результате успешной эксплуатации критической уязвимости CVE-2022-27228 (CMS *Bitrix*24). Примечательно, что сведения об указанной уязвимости за несколько месяцев до возникновения указанных компьютерных инцидентов были размещены в Банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России и распространены по каналам Национального координационного центра по компьютерным инцидентам.

Подводя итог, можно сделать вывод о том, что для осуществления качественного расследования неправомерного воздействия на КИИ РФ сотрудникам правоохранительных органов необходимо знать актуальные способы совершения данных преступлений, а субъектам КИИ РФ необходимо превентивно выстраивать все процессы, связанные с мониторингом и своевременным реагированием на компьютерный инцидент. При этом важно постоянно проводить проверку защищенности объектов КИИ РФ, а также регулярно осведомлять сотрудников организации о вопросах информационной безопасности и уголовной ответственности за неправомерное воздействие на КИИ РФ.

Список источников

1. TADVISER. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#.2A_2024:_.D0.94.D0.BE.D0.BB.D1.8F_.D0.B7.D0.B0.D0.BA.D0.B0.D0.B7.D0.BD.D1.8B.D1.85_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0_.D1.80.D0.BE.D1.81.D1.81.D0.B8.D0.B9.D1.81.D0.BA.D0.B8.D0.B5_.D0.BA.D0.BE.D0.BC.D0.BF.D0.B0.D0.BD.D0.B8.D0.B8_.D0.B7.D0.B0_.D0.B3.D0.BE.D0.B4_.D0.B2.D1.8B.D1.80.D0.BE.D1.81.D0.BB.D0.B0_.D1.81_10.25_.D0.B4.D0.BE_44.25 (дата обращения: 25.09.2024).

2. URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-pervom-polugodii-2024-goda-zafiksirovan-kratnyj-rost-atak-na-sfery-telekoma-i-stroitelstva (дата обращения: 25.09.2024).

3. Ефремова М. А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 86–92.

4. 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»: федеральный закон от 26 июля 2017 года № 194-ФЗ // Доступ из СПС «КонсультантПлюс» (дата обращения: 20.09.2024).

5. Судебная статистика Российской Федерации за 2020–2023 годы. URL: https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения: 25.09.2024).

6. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 года № 187-ФЗ // Доступ из СПС «КонсультантПлюс» (дата обращения: 25.09.2024).

References

1. TADVISER. State. Business. Technologies. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8% D1%80%D0%B5#.2A_2024:_.D0.94.D0.BE.D0.BB.D1.8F_.D0.B7.D0.B0.D0.BA.D0.B0.D0.B7.D0.BD.D1.8B.D1.85_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0_.D1.80.D0.BE.D1.81.D1.81.D0.B8.D0.B9.D1.81.D0.BA.D0.B8.D0.B5_.D0.BA.D0.BE.D0.BC.D0.BF.D0.B0.D0.BD.D0.B8.D0.B8_.D0.B7.D0.B0_.D0.B3.D0.BE.D0.B4_.D0.B2.D1.8B.D1.80.D0.BE.D1.81.D0.BB.D0.B0_.D1.81_10.25_.D0.B4.D0.BE_44.25 (accessed 25.09.2024). (In Russ.)

2. URL https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-pervom-polugodii-2024-goda-zafiksirovan-kratnyj-rost-atak-na-sfery-telekoma-i-stroitelstva (accessed 25.09.2024). (In Russ.)

3. Efremova M. A. Criminal liability for unlawful impact on the critical information infrastructure of the Russian Federation. *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia,* 2022, vol. 13, no. 4 (50), pp. 86–92. (In Russ.)

4. On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Criminal Procedure Code of the Russian Federation in Connection with the Adoption of the Federal Law “On the Security of the Critical Information Infrastructure of the Russian Federation”: federal law no. 194-FZ of July 26, 2017. Access from the reference legal system «ConsultantPlus»(accessed 25.09.2024). (In Russ.)

5. Judicial Statistics of the Russian Federation for 2020–2023. URL: https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (accessed 25.09.2024). (In Russ.)

6. On the security of the critical information infrastructure of the Russian Federation: federal law no. 187-FZ of July 26, 2017. Access from the reference legal system “ConsultantPlus” (accessed 25.09.2024). (In Russ.)

Информация об авторе

М. О. Янгаева **—** кандидат юридических наук, доцент, доцент кафедры криминалистики Барнаульского юридического института МВД России;

Н. В. Шепель — кандидат юридических наук, доцент, доцент кафедры уголовного процесса Калининградского филиала Санкт-Петербургского университета МВД России.

Information about the author

M. O. Yangaeva — Candidate of Sciences (Law), Associate Professor, associate professor of the criminalistics department of the Barnaul Law Institute of the Ministry of Internal Affairs of Russia;

N. V. Shepel — Candidate of Sciences (Law), Associate Professor, associate professor of the criminal procedure department of the Kaliningrad branch of the Saint Petersburg University of the Ministry of Internal Affairs of Russia.