Научная статья
УДК 34.096;004.056.53; DOI: 10.61260/2218-13X-2024-3-139-145

ПРАВОВЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМА КОНВЕРГЕНЦИИ ПОНЯТИЙНОГО АППАРАТА

Радченко Татьяна Викторовна;
Бакаев Анатолий Александрович;
✉Глобенко Оксана Александровна.
МИРЭА – Российский технологический университет, Москва, Россия
✉globenko@mirea.ru

Аннотация. Формирование глобального информационного пространства как явление несомненно положительное вместе с тем порождает новые угрозы национальной и международной безопасности. Ключевые характеристики киберпространтва (трансграничность, анонимность, быстрота) детерминируют рост числа пользователей информационными технологиями, но вместе с тем возрастает и динамика негативных воздействий на информационную инфраструктуру. Формирование успешной стратегии противодействия этим деструктивным явлениям невозможно без создания полноценного правового режима, позволяющего квалифицировать их без лакун и коллизий, с учетом трансдисциплинарного характера их природы.

Авторы исследования предлагают на основании междисциплинарного анализа проблемы определения правовой природы событий, происходящих в информационно-цифровом пространстве и обобщенно именуемых инцидентами либо киберинцидентами, законодательное закрепление ряда ключевых понятий и категорий, обеспечивающих единообразный подход в правоприменении, повышение эффективности правовых механизмов противодействия киберправонарушениям.

Ключевые слова: инцидент информационной безопасности, компьютерный инцидент, киберинцидент, кибепространство, цифровизация, правовое регулирование, объект критической информационной инфраструктуры

Для цитирования: Радченко Т.В., Бакаев А.А., Глобенко О.А. Правовые аспекты кибербезопасности: проблема конвергенции понятийного аппарата // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 139–145. DOI: 10.61260/2218-13X-2024-3-139-145.

Scientific article

LEGAL ASPECTS OF CYBER SECURITY: THE PROBLEM OF CONCEPTUAL CONVERGENCE

Radchenko Tatiana V.;
Bakaev Anatoliy A.;
✉Globenko Oksana A.
MIREA – Russian university of technology, Moscow, Russia
✉globenko@mirea.ru

Abstract. The formation of a global information space, as an undoubtedly positive phenomenon, at the same time gives rise to new threats to national and international security. The key characteristics of cyberspace (cross-border, anonymity, speed) determine the growth in the number of users of information technologies, but at the same time, the dynamics of negative impacts on the information infrastructure are also increasing. The formation of a successful strategy to counter these destructive phenomena is impossible without the creation of a full-fledged legal regime that allows them to be classified, without gaps and conflicts, taking into account the transdisciplinary nature of their nature.

The authors of the study propose, based on an interdisciplinary analysis of the problem of determining the legal nature of events occurring in the information and digital space and generally referred to as incidents or cyber incidents, the legislative consolidation of a number of key concepts and categories that ensure a uniform approach to law enforcement, increasing the effectiveness of legal mechanisms for combating cyber offenses.

Keywords: information security incident, computer incident, cyber incident, cyberspace, digitalization, legal regulation, critical information infrastructure object

For citation: Radchenko T.V., Bakaev A.A., Globenko O.A. Legal aspects of cyber security: the problem of conceptual convergence // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 139–145. DOI: 10.61260/2218-13X-2024-3-139-145.

Введение

Современные темпы цифровизации всех сфер и процессов производственной и социальной деятельности определяют формирование новой информационной картины мира, характеризующейся активной динамикой усложнения информационно-технологических систем, устройств и процессов, сложных не только в функционировании, но и в управлении, обслуживании, существующих в киберпространстве и соответственно порождающих киберриски, и нуждающихся в киберзащите. Понятие киберпространство (кибертерритория) как неологизм впервые было предложено писателем-фантастом У. Гибсоном, а затем включено в научно-техническую сферу благодаря созданию Т.Т. Бёрнерсом-Ли Всемирной паутины – World Wide Web или WWW [1] как некоего метафорического пространства, существующего в виртуальной реальности и отличного от реального интернета. В киберпространстве важная роль принадлежит не только технологиям, информации, передаваемой посредством использования сети Интернет, но и субъектам (в частности IT-компаниям), ответственным за осуществление различных операций с использованием информационно-коммуникационных технологий [2]. В этой связи особо важным становится формирование системы информационной безопасности (кибербезопасности), направленной на снижение различного рода уязвимостей и деструктивных внешних воздействий, как элемента и национальной, и международной безопасности, ввиду растущего числа успешных для злоумышленников атак. Так, согласно данным центра противодействия кибератакам Solar JSOC [3] в IV кв. 2023 г. было выявлено 437 тыс. подозрений на киберинцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на 20 % больше, чем в предыдущем квартале и на 68 % больше показателя IV кв. 2022 г.

Складывающаяся ситуация демонстрирует положительную динамику роста событий нежелательного воздействия – киберинцидентов, что, в свою очередь, вполне закономерно, с учетом стремительного темпа цифровизации сферы бизнеса и расширения использования информационных систем в организациях практически всех отраслей. При этом, несмотря на стабильные показатели подтвержденных киберинцидентов, которые в среднем колеблются в пределах 2 %, их вредоносность возрастает, особенно в контексте повышения квалификации злоумышленников.

Теоретические основы

Систему эффективной киберзащиты невозможно выстроить как без четкого понимания функционирования и взаимодействия элементов IT инфраструктуры – операционных систем, бизнес-приложений, типов данных и систем защиты, так и разработки детализированного механизма правового регулирования этой сферы [4]. Хайдеггер М. подчёркивал, что любое современное общество можно охарактеризовать как «стремительный поток», поэтому неизбежно появление новых технологий, к которым должно приспособиться право [5]. Мы наблюдаем и констатируем сегодня отсутствие сформированной системы регулирующих сферу кибербезопасности правовых норм.

В этой связи представляется важным исследование вопроса о целесообразности, возможности и необходимости имплементации и унификации терминологии, используемой в сфере информационной безопасности (ИБ) в правовую, посредством единообразного закрепления на законодательном уровне понятий инцидент, инцидент ИБ и киберинцидент, которые, являясь несинонимичными, требуют их точной правовой квалификации и адекватного правового реагирования на указанные события. При существующей системе правового регулирования проявляется ряд актуальных проблем, возникающих при правовой оценке данных деяний:

– связанных с точным определением терминов и соотношением их с терминологией, используемой в сфере ИБ;

– определяющих применимые правила квалификации киберинцидента как правонарушения с учетом тяжести деяния и последствий.

В этой связи необходимо учитывать, что правовой режим киберпространства обладает определенными особенностями и своим понятийным аппаратом, имеющим межотраслевой характер. Таким образом, вопрос правовой квалификации инцидентов, инцидентов ИБ и киберинцидентов приобретает особую актуальность и значимость для обеспечения ИБ, даже в условиях идеального правового регулирования киберпространства.

Результаты исследования и их обсуждение

В контексте цифрового пространства, где информационные технологии играют ключевую роль в различных сферах деятельности, понимание и правовая регламентация исследуемых событий ИБ становится неотъемлемой частью обеспечения безопасности и защиты прав и интересов граждан, организаций и государства. Так, изучение правовой природы инцидента ИБ и киберинцидента как событий поражения системы ИБ выражает их значение как объектов юридического анализа и регулирования в контексте современных цифровых вызовов и угроз.

Анализируя доктрину, можно сказать, что в российском законодательстве понятия «инцидент», «инцидент ИБ», «киберинцидент», также как и понятие «кибер», официально не определены на законодательном уровне. Межу тем стоит отметить, что Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ФЗ № 187-ФЗ) вводит понятие компьютерного инцидента, определяя его как факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры (КИИ), сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Таким образом, такой инцидент является фактом, воздействующим на состояние работоспособности информационных систем, сетей или систем защиты информации, который не обязательно является следствием противоправных деяний (либо рассматривается безотносительно квалификации таких деяний по нормам административного или уголовного законодательства).

В то же время в регламентах организаций, занимающихся расследованием киберинцидентов, и других источниках, связанных с ИБ частного сектора, не включенного в сферу объектов КИИ, широко употребляется понятие «инцидент», под которым обычно понимают спонтанные снижение качества или прерывание предоставления IT-услуг или реализации бизнес-процессов.

Причиной таковых, как правило, являются различные технологические факторы, например, устаревшее оборудование, уязвимые личные устройства сотрудников, человеческий фактор, не связанный с умыслом на причинение вреда. По уровням объема и охвата операций такие инциденты типизируют как низкий, средний, высокий, критический.

Данное деление используется с целью определения приоритетности устранения ввиду влияния инцидента на бизнес-процессы и прогнозируемые затраты на восстановление.

Несколько иное определение у термина «инцидент ИБ» – это одно или несколько событий, с высокой вероятностью приводящих к угрозе ИБ и функционирования бизнес-процессов. Указанное определение коррелирует с подходом, определяющим регламентацию в ГОСТ Р ИСО/МЭК ТО 18044–2007 ФСТЭК России «Менеджмент инцидентов информационной безопасности», где под «инцидентом ИБ» понимают появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана незначительная вероятность компроментации бизнес-операций и создания угрозы ИБ, а также, которое привело или могло привести к нарушению функционирования информационного ресурса или угроз безопасности информации или нарушению требований по защите информации.

В свою очередь, «событие ИБ» – зафиксированное состояние информационной (автоматизированнной) системы, указывающее на возможное нарушение безопасности информации, сбой средств защиты информации или ситуацию, которая может быть значимой для безопасности информации.

Под компьютерным инцидентом (киберинцидентом), согласно Национальному стандарту Российской Федерации ГОСТ 59709–2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» (утв. приказом Федерального агенства по техническому регулированию и метрологии) понимают факт нарушения и/или прекращения функционирования информационного ресурса, сети электросвязи, используемых для организации взаимодействия информационных ресурсов и/или нарушения безопасности обрабатываемой информации, в том числе произошедший в результате компьютерной атаки. Данное определение практически полностью продублировано из Федерального закона № 187-ФЗ.

В то же время понятие «кибреницидент», как уже было отмечено выше, не упоминается в законодательстве России, однако широко используется в системе обеспечения ИБ, а также в доктрине как обобщающее и синоним терминов «компьютерный инцидент», «инцидент ИБ», «киберпреступление», «компьютерная атака», что видится смешением этих понятий [6–8].

Таким образом, возможно констатировать, что ГОСТы, определяющие нормативные границы, демонстрируют неединообразный подход к определению указанных терминов. Более того, в определениях использованы оценочные признаки, сами по себе нуждающиеся в толковании: «нежелательные», «неожиданные», «спонтанные» и т.д. Единообразное понимание подобных признаков в правоприменении обычно затруднено. В этот ряд в таком случае можно поставить и случайные, произвольные, невольные, внезапные (события), что приведет к еще большему разночтению позиций правоприменителя.

Таким образом, понятийный аппарат минимально закреплен в юридико-технических нормах и четко не определен.

Между тем ни материальное, ни процессуальное действующиее законодательство не знают понятий «инцидент», «инцидент ИБ», «киберинцидент» при установлении оснований отдельных видов юридической ответственности, например, за неправомерный доступ к компьютерной информации или посягательствах на персональные данные.

Ситуативно инциденты несут вредоносность разной степени. Безусловно, посредством толкования правоприменитель придет к выводу о том, что инцидент – это событие, которое произошло в силу использования неправомерного доступа как способа совершения деяния. В случае инцидента ИБ возможна незначительная вероятность создания угрозы ИБ, тогда как нарушение или прекращение функционирования ресурса, то есть киберинцидент несопоставимо опаснее инцидента ИБ.

Также, особенно следует подчеркнуть, что киберинцидент может быть квалифицирован не только как деликт, результат злонамеренных действий, но и как случайный сбой, результаты которого могут быть предметом договорной регламентации

с той или иной компанией, частным лицом, представляя угрозу для ИБ организаций, индивидов или общества в целом. Сложный правовой контекст киберпространства создает множество серьезных задач, которые существенно затрудняют и классификацию инцидентов ИБ, киберинцидентов как конкретных событий с точки зрения правового анализа, и ставят вопросы точной и правильной юридической оценки произошедшего воздействия, что, в свою очередь, усложняет борьбу с киберугрозами. Субъекты киберугроз обладают разной степенью навыков и ресурсов, реально и потенциально угрожающих безопасности компаний и граждан, и в ряде случаев, с точки зрения установления юридического факта наличия правонарушения или преступления, в таком контексте также могут возникать сложности.

Киберинциденты могут проявляться в различных формах в первую очередь направленных на поражение конфиденциальности, целостности или доступности информационных систем и данных. Они могут быть обусловлены разнообразными мотивами: корыстными, экстремистскими, личными и даже хулиганскими. Рост использования облачных вычислений, устройств Интернета вещей и цифровых взаимосвязей расширил ландшафт угроз, позволяя злоумышленникам использовать различные уязвимости. Подобное многообразие способов и проявлений затрудняет разделение инцидентов на виды и формы [9]. Одной из основных сложностей, даже с учётом разнообразия законодательства, регулирующего отношения в сфере обеспечения ИБ, является отсутствие единого и четкого определения киберинцидента и его разграничения со смежными понятиями в российском законодательстве. Формы, способы совершения киберинцидентов стремительно трансформируются, что создает вызовы и для сферы регулирования и обеспечения ИБ, и для правоохранительных органов.

Понятие «киберинцидент» до сих пор остается отчасти оценочным, поскольку закреплено на уровне отраслевого регулирования. Как правило, специалисты в сфере ИБ квалифицируют этот феномен либо как правонарушение особого рода (с возможностью причлечения к дисциплинарной ответственности), либо в качестве не влекущего ответственности события. Не всегда устранение последствий кибервоздействия ведет к установлению лица, его совершившего. Более того, инциденты часто трангранични [10].

В силу признания в доктрине под киберпреступлениями как наиболее общественно опасными воздействиями на сферу ИБ и киберинцидентов, и инцидентов информационной безопасности, и компьютерных инцидентов следует признать, что все эти понятия иллюстрируют комплекс сложившихся проблем и указывают на необходимость борьбы с ними [11]. Именно по этой причине необходимо закрепление на законодательном уровне понятийно-категориального аппарата.

Возможным решением анализируемой проблемы видится закрепление определения «компьютерныйо инцидент», предложенного в Федеральном законе № 187-ФЗ, в законодательстве, регулирующим общеправовую сферу. Поскольку законодательство о КИИ де-юре и де-факто не распространяется на все категории бизнеса в Российской Федерации, то альтернативы чёткого регулирования общедоступного киберпространства в настоящее время не имеется, что влечёт за собой правовой пробел в части защиты объектов, не относящихся к КИИ. Однако при интеграции раскрываемого понятия в частноправовые отношения указанная дефиниция тем не менее не позволит исчерпывающе определить все существенные признаки, поскольку для юридической квалификации киберинцидента мало установления лишь наличия такого события/факта, так как процессуальная система отношений требует не только установить факт, но и доказать его. Факт считается доказанным, когда он установлен допустимыми, достоверными, относимыми и достаточными доказательствами.

В целом режим, созданный регуляторами для защиты КИИ, логичен и профессионален, но не учитывает всех аспектов процессуального доказывания.

Таким образом, проблема понимания правовой природы киберинцидента как обобщающего понятия порождает проблемы квалификации как деяния, имеющего признаки состава преступления.

Заключение

Отсутствие исчерпывающего определения понятия киберинцидента существенно затрудняет его имплементацию в правовую сферу киберпространства. Для юридической квалификации киберинцидента мало лишь наличия такого события. Более того, с учетом высоких темпов развития технологий и появления новых видов угроз, важно не только разработать четкое определение киберинцидентов, но и постоянно новеллизировать, обеспечивая адекватное отражение динамично меняющихся реалий ИБ. В связи с этим законодательство должно быть гибким и адаптируемым, чтобы эффективно реагировать на новые вызовы в сфере кибербезопасности.

Преступная деятельность в киберпространстве и IT-сфере высокоинтеллектуальна и, соответственно латентна, способы ухода от ответственности постоянно совершенствуются, поэтому алгоритмы правового реагирования должны соответствовать этим вызовам. Однако их создание и эффективное использование возможно лишь при глубоком понимании сути процесса: при активном диалоге не только юристов, но междисциплинарном диалоге со специалистами в сфере ИБ.

Список источников

1. History of the Web. World Wide Web Foundation. URL: https://webfoundation.org/about/vision/history-of-the-web/ (дата обращения: 21.06.2024).

2. Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law // Edward Elgar Publishing. 2015. 176 p.

3. Группа компаний «Солар» – ведущий поставщик ИБ-решений в России. URL: https://zoom.cnews.ru/soft/news/line/2024-05-16_solar_nesanktsionirovannyj (дата обращения: 22.05.2024).

4. Ищанова Р.К. Обеспечение кибербезопасности // Большая Евразия: Развитие, безопасность, сотрудничество. 2019. № 2-1. С. 367–368.

5. Rustad M.L. Global Internet Law in a Nutshell // West Academic Publishing, 2013. 525 p.

6. Смирнов В.М., Кузина А.В. Расследование киберинцидентов в условиях кибератак. М.: МосУ МВД имени В.Я. Кикотя, 2023. С. 114–116.

7. Усанов И.В. Диалектический материализм и электронно-цифровая криминалистика // Вестник Саратовской государственной академии. 2023. С. 270–277.

8. Позволенко В.А., Воробьева А.А. Лингвистическая идентификация в расследовании киберинцидентов // Наука настоящего и будущего. 2021. С. 154–155.

9. Ронжина Н.А., Глазатов А.А. Развитие системы кибербезопасности в Российской Федерации как основное условие обеспечения национальной информационной безопасности // Право. Безопасность. Чрезвычайные ситуации. 2023. № 1 (58). С. 24–34.

10. Lester Evans Cybersecurity: What you need to know about computer and cyber security? Social engineering, the Internet of things. P.: Bravex Publications, London. 2019. 230 p.

11. Нестерович С.А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. 2018. С. 16–22.

References

1. History of the Web. World Wide Web Foundation. URL: https://webfoundation.org/about/vision/history-of-the-web/ (data obrashcheniya: 21.06.2024).

2. Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law // Edward Elgar Publishing. 2015. 176 p.

3. Gruppa kompanij «Solar» – vedushchij postavshchik IB-reshenij v Rossii. URL: https://zoom.cnews.ru/soft/news/line/2024-05-16_solar_nesanktsionirovannyj (data obrashcheniya: 22.05.2024).

4. Ishchanova R.K. Obespechenie kiberbezopasnosti // Bol'shaya Evraziya: Razvitie, bezopasnost', sotrudnichestvo. 2019. № 2-1. S. 367–368.

5. Rustad M.L. Global Internet Law in a Nutshell // West Academic Publishing, 2013. 525 p.

6. Smirnov V.M., Kuzina A.V. Rassledovanie kiberincidentov v usloviyah kiberatak. M.: MosU MVD imeni V.Ya. Kikotya, 2023. S. 114–116.

7. Usanov I.V. Dialekticheskij materializm i elektronno-cifrovaya kriminalistika // Vestnik Saratovskoj gosudarstvennoj akademii. 2023. S. 270–277.

8. Pozvolenko V.A., Vorob'eva A.A. Lingvisticheskaya identifikaciya v rassledovanii kiberincidentov // Nauka nastoyashchego i budushchego. 2021. S. 154–155.

9. Ronzhina N.A., Glazatov A.A. Razvitie sistemy kiberbezopasnosti v Rossijskoj Federacii kak osnovnoe uslovie obespecheniya nacional'noj informacionnoj bezopasnosti // Pravo. Bezopasnost'. Chrezvychajnye situacii. 2023. № 1 (58). S. 24–34.

10. Lester Evans Cybersecurity: What you need to know about computer and cyber security? Social engineering, the Internet of things. P.: Bravex Publications, London. 2019. 230 p.

11. Nesterovich S.A. Problemy rassledovaniya kiberprestuplenij, kotorye stoyat pered sotrudnikami sledstvennyh organov // Vestnik nauki i obrazovaniya. 2018. S. 16–22.

Информация о статье:
Статья поступила в редакцию: 13.08.2024; одобрена после рецензирования: 28.08.2024;
принята к публикации: 30.08.2024
Information about the article:
The article was submitted to the editorial office: 13.08.2024; approved after review: 28.08.2024;
accepted for publication: 30.08.2024

Сведения об авторах:
Радченко Татьяна Викторовна, доцент кафедры Правовое обеспечение национальной безопасности Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, Москва, пр. Вернадского, д. 78), кандидат юридических наук, доцент, e-mail: radchenko@mirea.ru, https://orcid.org/0000-0002-0450-9459, SPIN-код: 7431-1920
Бакаев Анатолий Александрович, заведующий кафедрой Правовое обеспечение национальной безопасности Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, Москва, пр. Вернадского, д. 78), доктор исторических наук, кандидат юридических наук, доцент, e-mail: bakaev@mirea.ru, https://orcid.org/0000-0002-9526-0117, SPIN-код: 5283-9148
Глобенко Оксана Александровна, доцент кафедры Правовое обеспечение национальной безопасности Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, Москва, пр. Вернадского, д. 78), кандидат юридических наук, доцент, e-mail: globenko@mirea.ru, https://orcid.org/0009-0001-4984-4728, SPIN-код: 1278-8429

Information about the authors:
Radchenko Tatyana V., associate professor of the department of Legal support of national security at the Institute of cybersecurity and digital technologies of the Russian technological university MIREA (119454, Moscow, Vernadsky ave., 78), candidate of law, associate professor, e-mail: radchenko@mirea.ru, https://orcid.org/0000-0002-0450-9459, SPIN: 7431-1920
Bakaev Anatoliy A., head of the department of Legal support of national security at the Institute of cybersecurity and digital technologies of the Russian technological university MIREA (119454, Moscow, Vernadsky ave., 78), doctor of historical sciences, candidate of law, associate professor, e-mail: bakaev@mirea.ru, https://orcid.org/0000-0002-9526-0117, SPIN: 5283-9148
Globenko Oksana A., associate professor of the department of Legal support of national security at the Institute of cybersecurity and digital technologies of the Russian technological university MIREA (119454, Moscow, Vernadsky ave., 78), candidate of law, associate professor, e-mail: globenko@mirea.ru, https://orcid.org/0009-0001-4984-4728, SPIN: 1278-8429