

ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «КИБЕРБЕЗОПАСНОСТЬ» И СВЯЗАННЫХ С НИМ ТЕРМИНОВ

Язов Ю. К.¹

DOI: 10.21681/2311-3456-2025-1-2-6

Цель статьи: раскрытие содержания терминов с префиксом «кибер» и оценка обоснованности их применения в отечественной практике.

Методы исследования: семантический анализ, сравнение и сопоставление, онтология понятий и их системный анализ.

Полученный результат: отмечено широкое применение терминов с префиксом «кибер» и отсутствие их определений в отечественных документах. Проведен краткий анализ предложений специалистов по определению таких терминов, как «киберпространство», «кибербезопасность» и др. и отмечено, что в этих определениях не показано, чем же конкретно отличаются термины с префиксами «кибер» от применяемых сегодня терминов, таких как угроза безопасности информации, сетевая атака и т.д., и почему «новые» термины можно и целесообразно использовать.

Отмечено, что префикс «кибер» показывает их причастность к компьютерам, в том числе к Internet, информационно-телекоммуникационным системам и т.п. При этом имеет место важный признак такой причастности: в устройствах, системах, процессах, явлениях, к которым имеют отношения указанные слова с префиксом «кибер», обрабатывается (создается, передается, принимается, записывается, уничтожается и т.д.) информация в цифровой форме.

С учетом изложенного даются определения таких терминов, как «киберпространство», «кибербезопасность», «киберугроза», «кибератака» и др.

Ключевые слова: цифровая информация, информационное пространство, киберпространство, цифровая технология, киберугроза, киберфизическая система.

Термины с префиксом «кибер» (от англ. «cyber») стали широко применяться в зарубежной литературе еще с 90-х годов прошлого века. При этом префикс «кибер», добавляемый к обиходным словам, показывал их причастность к Internet, компьютерам, информационно-телекоммуникационным системам и т.п. В последние десять лет он очень распространился и в России. Однако в отечественных документах определение терминов, таких как «кибербезопасность», «киберугроза», «киберустойчивость», «киберпространство» и многие другие, которые широко наводнили не только прессу, но и научные издания, до сих пор фактически отсутствуют.

В целом ряде публикаций, некоторые из которых содержат весьма глубокие рассуждения и предложения, например [1–5], поднимался вопрос об определении терминов, связанных с префиксом «кибер», однако при этом не указывался основной признак, по которому термин с этим префиксом отличался от уже применяющихся в России терминов со сходным содержанием. Так, в [1] при анализе научной литературы выделены две отличительные черты применяющегося понятия «кибербезопасность»: наличие угрозы реализации компьютерной атаки и цифровые ресурсы, подлежащие компрометации. В [2] приведено несколько вариантов определения термина «кибербезопасность»:

- 1) с учетом перевода с английского как «информационная безопасность в сфере (области) информационных технологий, компьютерных технологий и управления»;
- 2) через «техническую трактовку» понятия как «информационная безопасность в киберпространстве», при этом киберпространство трактуется как «глобальная сфера внутри информационного пространства, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Internet, телекоммуникационные сети, компьютерные системы, а также встроенные в другие технические объекты процессоры и контроллеры, предназначенные для хранения, обработки, модификации и обмена данными»²;
- 3) через связь с целями информационной безопасности, определенными доктриной информационной безопасности Российской Федерации, как свойство (состояние) компьютерных информационно-управляющих телекоммуникационных инфраструктур сохранять заданную функциональную устойчивость при гарантированном соответствии требованиям информационной безопасности;
- 4) через соотношение понятий «информационная безопасность» и «кибербезопасность» как

¹ Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail: yazoff_1946@mail.ru

² Операции в киберпространстве, МО США, 2010 г.

информационная безопасность в инфосфере компьютерных информационно-управляющих и телекоммуникационных инфраструктур, где под инфосферой (то есть информационной сферой) понимается «совокупность информации, объектов информатизации, информационных систем, сайтов информационно-телекоммуникационной сети Internet, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и оборотом информации, развитием и использованием названных технологий, обеспечением информационной безопасности»³.

Указанные определения, кроме первого, достаточно близко раскрывают суть понятия «киберпространство», поскольку оно связывается с компьютерными системами информационно-телекоммуникационными сетями, однако из них не видно, чем же конкретно отличается информационное пространство от киберпространства, и это не дает возможность достаточно ясно определить и обосновать целесообразность использования других широко применяемых сегодня терминов с префиксом «кибер», таких как «кибербезопасность» в сопоставлении с термином «информационная безопасность», «киберугроза», «кибератака», «киберустойчивость», «киберпреступление», «кибертерроризм» и многие другие [5–8]. Надо отметить, что количество таких терминов постоянно растет, некоторые из них вполне состоятельные, например, термин «киберфизические системы», а некоторые вызывают даже недоумение, например, термин киберполицейский, что оказывается соответствует не киборгу, а полицейскому, занимающемуся вопросами кибербезопасности. Вместе с тем, имеет место важный признак причастности тех или иных слов с префиксом «кибер» к Internet, компьютерам, информационно-телекоммуникационным системам: в устройствах, системах, процессах, явлениях, в ходе выполнения действий, к которым имеют отношения указанные слова, обрабатывается (создается, передается, принимается, записывается, уничтожается и т.д.) информация в цифровой форме (в [1] – это цифровые ресурсы).

Известно, что информация может представляться в документационной, аналоговой или в цифровой форме. Документационная информация содержится (в буквенно-цифровом виде, в виде иероглифов и т.д.) на бумаге или иных носителях. Аналоговая информация может содержаться в звуке (в частности речи), в виброакустических и гидроакустических колебаниях, в электрическом токе, в электромагнитных колебаниях и др. Она представляется, как правило, в виде непрерывных сигналов.

3 Доктрина информационной безопасности Российской Федерации. Указ Президента РФ от 5 декабря 2016 г. №646.

Цифровая информация – это информация, для обработки которой (генерации, фиксации, приема, передачи, сбора, представления, записи, хранения, копирования, уничтожения, модификации и т.д.) применяются исключительно цифровые технологии. При этом цифровая технология представляет собой совокупность методов, процессов и инструментов, основанных на использовании цифровых данных⁴ и цифровых устройств их обработки. Сегодня на основе цифровых технологий функционируют, например: компьютеры и компьютерные сети, в том числе глобальная сеть Internet; системы искусственного интеллекта и машинного обучения; системы распределённого реестра (блокчейн); «интернет вещей» (IoT, Internet of Things – объединение разных устройств в общую сеть, в которой они могут собирать информацию, обрабатывать её и обмениваться данными между собой, с человеком и серверами в дата-центре или облаке), в том числе промышленный «интернет вещей» (IIoT – Industrial Internet of Things); системы сбора и аналитической обработки больших данных (Big Data); киберфизические системы и др. Цифровая информация получается путем соответствующего аналого-цифрового преобразования документационной или аналоговой информации.

С учетом изложенного становится достаточно прозрачным понятие «киберпространство» как часть информационного пространства, в котором циркулирует цифровая информация и функционируют цифровые устройства ее обработки. Ведь в соответствии с п. 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утверждённой Указом Президента РФ от 9 мая 2017 № 203, информационное пространство – совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

По сути, информационное пространство, кроме цифровой информации и цифровых устройств, содержит также аналоговую информацию и соответствующие устройства для ее обработки, то есть для генерации, фиксации, приема, передачи, сбора, представления, хранения и т.д. Выделяя его составляющую – «киберпространство», можно сразу ограничить предмет рассмотрения только цифровой информацией и устройствами ее обработки.

Аналогичным образом можно трактовать и иные термины, связанные с префиксом «кибер». В частности, **киберугроза** представляет собой угрозу безопасности цифровой информации и угрозу безопасности

4 Цифровые данные – это информация, представленная в виде цифровых кодов. Для представления таких данных сегодня используется, преимущественно, двоичное, третичное, десятичное и шестнадцатеричное исчисления.

функционирования устройств ее обработки. Киберугрозы – это лишь часть множества угроз безопасности информации и тем более угроз информационной безопасности.

Следует подчеркнуть различие понятий «безопасность информации» и «информационная безопасность». В Доктрине информационной безопасности, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, введено понятие информационной безопасности Российской Федерации как 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. Аналогичным образом было введено и понятие информационной безопасности организации как «состояния защищенности интересов (целей) организации в условиях угроз в информационной сфере». Из этого следует, что безопасность информации касается только самой информации, а информационная безопасность – значительно более широкое понятие, охватывающее интересы людей, организаций (предприятий) и государства в информационной сфере. Кроме защиты самой информации, при обеспечении информационной безопасности должна осуществляться также «защита от информации» (навязывания ложной, тенденциозной, социально вредной и иной неприемлемой для личности, общества и государства информации), а также применение мер, направленных на обеспечение прав граждан на информированность и получение ими достоверной и своевременной информации. В этом смысле спектр угроз информационной безопасности значительно шире спектра угроз безопасности информации.

Тесно связан с понятием «киберугроза» широко применяемый сегодня термин «кибератака». В общем случае атака – это процесс реализации угрозы, а значит кибератака это процесс реализации киберугрозы. Однако при этом нужно иметь в виду следующее. Как правило, атака на компьютер реализуется с использованием протоколов межсетевое взаимодействия и именуется как сетевая атака, под которой понимаются «действия с применением программных и (или) программно-технических средств и с использованием сетевого протокола, направленные на несанкционированный доступ к информации, воздействие на нее или на ресурсы автоматизированной информационной системы»⁵. Таким образом,

кибератака, реализуемая в информационно-телекоммуникационной сети или в информационной системе, является, по сути, синонимом сетевой атаки.

Особо следует остановиться на определении понятия «кибербезопасность». Оно охватывает понятия, во-первых, «безопасности цифровой информации» и, во-вторых, безопасность функционирования цифровых устройств ее обработки в условиях существования и реализации киберугроз. В связи с изложенным **кибербезопасность** – это состояние защищенности цифровой информации и устройств ее обработки от киберугроз. К таким устройствам могут относиться компьютеры и их программные и программно-аппаратные элементы, компьютерные (информационные) системы, промышленные программно-аппаратные комплексы, автоматизированные системы управления технологическим производством, информационно-телекоммуникационные сети и т.д.

В некоторых публикациях, наряду с термином «кибербезопасность», стал применяться термин «киберустойчивость». Как правило, при этом имеют в виду устойчивость функционирования компьютера, компьютерной системы и иных цифровых устройств в условиях реализации киберугроз. Этот термин не применяется к информации. С учетом изложенного под **киберустойчивостью** следует понимать способность цифровых устройств противостоять киберугрозам.

Аналогичным образом можно определить такие термины, как:

- ❖ «киберпреступление» – преступление, связанное с нарушением безопасности цифровой информации, устройств ее обработки, а также с причинением материального, финансового или иного ущерба гражданам, учреждениям, организациям, предприятиям и государству путем противоправных действий в киберпространстве;
- ❖ «кибермошенничество» – это один из видов киберпреступлений, целью которого является причинение материального, финансового или иного ущерба путем хищения с использованием компьютерной сети личной информации граждан (например, номеров банковских счетов, паспортных данных, кодов, паролей и т.п.);
- ❖ «кибертерроризм» (от лат. terror – страх, ужас) – система взглядов (идеология) и преднамеренная деятельность отдельных лиц, групп, организаций и спецслужб иностранных государств, направленная на использование компьютеров и информационно-телекоммуникационных сетей в террористических целях. Такими целями могут быть, например, преднамеренное нарушение функционирования информационно-телекоммуникационных сетей, значимых объектов критической информационной инфраструктуры страны, в том

5 ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Приказ руководителя Ростехрегулирования от 18 декабря 2008 № 532 – СТ.

числе информационных систем органов власти, автоматизированных систем управления, функционирующих в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сферы и иных сфер финансового рынка, топливно-энергетического комплекса, в области атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической, химической и иных отраслей промышленности. По сути, «кибертерроризм» – это использование киберпространства для террористической деятельности. Аналогичным образом можно определить и иные иногда встречающиеся термины:

- ❖ «кибершпионаж» – шпионаж с использованием киберпространства;
- ❖ «кибервойна» – война в киберпространстве;
- ❖ «кибернадзор» – введение строгого общественного контроля в киберпространстве.

Наконец, следует остановиться еще на одном важном термине, который широко стал применяться в различных научных школах и, в частности, учеными Санкт-Петербурга, специализирующимися в области безопасности информации – на термине «киберфизическая система» (от англ. cyber-physical system – CPS) [9–12]. Это понятие возникло в связи с интеграцией вычислительных ресурсов и управляемых с их помощью физических процессов. В такой системе датчики, оборудование и информационные системы соединены на протяжении всей цепочки создания продукции или предоставления услуг с возможным выходом за рамки одного предприятия или

бизнеса. Элементы этой системы взаимодействуют друг с другом с помощью стандартных интернет-протоколов для прогнозирования, самонастройки и адаптации к изменениям.

С учетом изложенного под киберфизической системой сегодня понимают сложную распределенную систему, состоящую из совокупности вычислительных и физических элементов, которая постоянно получает данные из окружающей среды и использует их для управления физическими и вычислительными процессами. Эти системы уже достаточно широко стали применяться в промышленном производстве и робототехнике, в здравоохранении, энергетике, сельском хозяйстве, в интенсивно развивающемся сегодня «интернет вещей» (реализации концепций «умного дома», «умного города» и т.п.). «Вычислительные элементы» в таких системах – это компьютеры и иные цифровые устройства, что и обуславливает применение префикса «кибер».

Таким образом, появление и широкое применение терминов с префиксом «кибер» является вполне объективным фактом, отражающим широкое внедрение в практику цифровых технологий. Применение этих терминов позволяет сузить рассматриваемое информационное пространство до той части, которая связана с обработкой цифровой информации и применением для этого цифровых устройств. Они не заменяют в полном смысле и не отменяют существующие термины, распространяемые на все информационное пространство, а лишь конкретизируют предметную область.

Литература

1. Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей / А. С. Марков // Вопросы кибербезопасности. 2022. № 1 (47), с. 2–9. DOI:10.21681/2311-3456-2022-1-2-9
2. Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века / А. Ю. Добродеев // Вопросы кибербезопасности. 2021. № 4 (44), с. 61–72. DOI:10.21681/2311-3456-2021-4-61-72
3. Стародубцев Ю. И. Структурно-функциональная модель киберпространства / Ю. И. Стародубцев, П. В. Закалкин, С. А. Иванов // Вопросы кибербезопасности. 2021. № 4 (44), с. 16–24. DOI:10.21681/2311-3456-2021-4-16-24
4. Дылевский, И. Н. О взглядах администрации США на киберпространство как новую сферу ведения военных действий / И. Н. Дылевский, С. И. Базылев, О. В. Заливхин и др. // Военная мысль. 2020. №10, с. 22–29.
5. Карцхия А. А., Макаренко Г. И., Сергин М. Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31), с. 18–23. DOI:10.21681/2311-3456-2019-3-18-23
6. Архипова Е. А. Современное понимание терминов «кибернетическая безопасность» и «информационная безопасность» // Yung Scientis, 2019, № 12 (76), pp. 315–320. DOI:10.32839/2304-5809/2019-12-76-67
7. Башкиров Н. Взгляды военного и политического руководства США на защиту инфраструктуры от киберугроз // Зарубежное военное обозрение. 2018, № 12, с. 13–17.
8. Журовель В. П. Противодействие угрозе кибертерроризма // Зарубежное военное обозрение. 2018, № 55, с. 12–16.
9. Мещеряков Р. В., Исхаков С. Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022. № 5 (51), с. 82–99. DOI:10.21681/2311-3456-2022-5-82-99
10. Коршунов Г. И. Моделирование физических сред для оптимизации цифрового управления в киберфизических системах // НикСС. – 2023. – № 1 (41), с. 23–28. DOI: 10.21685/2307-4205-2023-1-3
11. Бурый А. С. Информационные структуры умного города на основе киберфизических систем / А. С. Бурый, Д. А. Ловцов // Правовая информатика. – 2022. – № 4. – С. 15–26. DOI: 10.21681/1994-104-2022-4-15-26
12. Фатин А. Д., Павленко Е. Ю. Анализ моделей представления киберфизических систем в задачах обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2020. – № 2. с. 109–121.
13. Язов В. О научных специальностях «кибербезопасность» и «методы и системы защиты информации, информационная безопасность» // Вопросы кибербезопасности. 2022. №2 (48). С. 5–6.

CYBERSECURITY TERMS AND DEFINITIONS

Yazov Yu. K.⁶

Keywords: digital information, Information space, Cyberspace, Digital technology, Cyber threats, Cyber-Physical Systems (CPS).

The goal of article: is disclosure content of terms with the prefix «cyber» and assessment validity of their use in domestic national practice.

The method of research: is semantic analysis, comparison and contrast, ontology of concepts and their system analysis.

The result of the research: is widespread use of terms with the prefix «cyber» and the absence of their definitions in domestic national documents. A brief analysis of the proposals of specialists to define such terms as «cyberspace», «cybersecurity», etc. has defined. It is noted that these definitions do not show exactly how the terms with the prefixes «cyber» differ from terms used today, such as information security threat, network attack, etc., and why «new» terms can and should be used. It is noted that the prefix «cyber» shows their involvement with computers, including the Internet, information and telecommunication systems, etc. In this case, there is an important sign of such involvement: in devices, systems, processes, phenomena, to which these words with the prefix «cyber» are related, information in digital form is processed (created, transmitted, received, recorded, destroyed, etc.). Based on the above, definitions of such terms as «cyberspace», «cybersecurity», «cyber threat», «cyberattack» are provided.

References

1. Markov A. S. Kiberbezopasnost' i informacionnaja bezopasnost' kak bifurkacija nomenklatury nauchnyh special'nostej/ A. S. Markov // Voprosy kiberbezopasnosti. 2022. № 1 (47), s. 2–9. DOI:10.21681/2311-3456-2022-1-2-9
2. Dobrodeev A. Ju. Kiberbezopasnost' v Rossijskoj Federacii. Modnyj termin ili prioritnoe tehnologicheskoe napravlenie obespechenija nacional'noj i mezhdunarodnoj bezopasnosti XXI veka/ A. Ju. Dobrodeev // Voprosy kiberbezopasnosti. 2021. № 4 (44), s. 61–72. DOI:10.21681/2311-3456-2021-4-61-72
3. Starodubcev Ju. I. Strukturno-funkcional'naja model' kiberprostranstva/ Ju. I. Starodubcev, P. V. Zakalkin, S. A. Ivanov// Voprosy kiberbezopasnosti. 2021. № 4 (44), s. 16–24. DOI:10.21681/2311-3456-2021-4-16-24
4. Dylevskij, I. N. O vzgljadah administracii SShA na kiberprostranstvo kak novuju sferu vedenija voennyh dejstvij/ I. N. Dylevskij, S. I. Bazylev, O. V. Zalivhin i dr. // Voennaja mysl'. 2020. № 10, s. 22–29.
5. Karchija A. A., Makarenko G. I., Sergin M. Ju. Sovremennye trendy kiberugroz i transformacija ponjatija kiberbezopasnosti v uslovijah cifrovizacii sistemy prava // Voprosy kiberbezopasnosti. 2019. № 3 (31), s. 18–23. DOI:10.21681/2311-3456-2019-3-18-23
6. Arhipova E. A. Sovremennoe ponimanie terminov «kiberneticheskaja bezopasnost'» i «informacionnaja bezopasnost'»/ E. A. Arhipova // Yung Scientis, 2019, № 12 (76), pp. 315–320.
7. Bashkurov N. Vzglyady voennogo i politicheskogo rukovodstva SShA na zashhitu infrastruktury ot kiberugroz // Zarubezhnoe voennoe obozrenie. 2018., № 12, s. 13–17.
8. Zhuravel' V. P. Protivodejstvie ugroze kiberterrorizma // Zarubezhnoe voennoe obozrenie. 2018., № 5, s. 12–16.
9. Meshherjakov R. V., Ishakov S. Ju. Issledovanie indikatorov komprometacii dlja sredstv zashhity informacionnyh i kiberfizicheskikh sistem // Voprosy kiberbezopasnosti. 2022. № 5 (51), s. 82–99. DOI:10.21681/2311-3456-2022-5-82-99
10. Korshunov G. I. Modelirovanie fizicheskikh sred dlja optimizacii cifrovogo upravlenija v kiberfizicheskikh sistemah // NiKSS. – 2023. – № 1 (41), s. 23–28. DOI: 10.21685/2307-4205-2023-1-3.
11. Buryj A. S. Informacionnye struktury umnogo goroda na osnove kiberfizicheskikh sistem / A. S. Buryj, D. A. Lovcov // Pravovaja informatika. – 2022. – № 4. – S. 15–26. DOI: 10.21681/1994-104-2022-4-15-26
12. Fatin A. D., Pavlenko E. Ju. Analiz modelej predstavlenija kiberfizicheskikh sistem v zadachah obespechenija informacionnoj bezopasnosti // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2020. – № 2. s. 109–121.
13. Jazov V. K. O nauchnyh special'nostjah «kiberbezopasnost'» i «metody i sistemy zashhity informacii, informacionnaja bezopasnost'» // Voprosy kiberbezopasnosti. 2022. № 2 (48). S. 5–6.



⁶ Yuri K. Yazov, Dr.Sc. of Technical Sciences, Professor, Chief Researcher of the State Research and Testing Institute for Technical Information Protection Problems of the Federal Service for Technical and Export Control of Russia, Voronezh, Russia. E-mail: yazoff_1946@mail.ru