УДК 343.98
DOI 10.52468/2542-1514.2025.9(3).114-123

CC BY 4.0

КИБЕРБЕЗОПАСНОСТЬ: ПОНЯТИЕ, СТРУКТУРА, МЕХАНИЗМ ПРАВОВОГО ОБЕСПЕЧЕНИЯ*

А.Б. Смушкин
Саратовская государственная юридическая академия, г. Саратов, Россия

Информация о статье
Дата поступления –
1 июля 2024 г.
Дата принятия в печать –
20 июня 2025 г.
Дата онлайн-размещения –
20 сентября 2025 г.

Ключевые слова
Безопасность, кибербезопасность, киберпространство, киберугрозы, информационный суверенитет, критическая информационная инфраструктура, криминалистика кибербезопасности, цифровая криминалистики, обеспечение устойчивости киберпространства, цифровые технологии, киберинцидент

Рассматриваются вопросы кибербезопасности в современных условиях, проводится дифференциация кибербезопасности и информационной безопасности. Констатируется, что кибербезопасность, как элемент общей информационной безопасности, связана, в первую очередь, с обеспечением безопасности от киберпреступлений и инцидентов в киберпространстве, не подпадающих под уголовную ответственность. По результатам анализа мнений различных авторов определено, что в структуру кибербезопасности входят: объекты обеспечения кибербезопасности, киберугрозы, субъекты кибербезопасности. Автором подробно рассмотрено содержание этих элементов. Особое внимание уделено разработке вопросов криминалистического обеспечения кибербезопасности как важного элемента противодействия преступным киберинцидентам.

CYBERSECURITY: CONCEPT, STRUCTURE, THE MECHANISM OF LEGAL ENSURING**

Alexander B. Smushkin
Saratov State Law Academy, Saratov, Russia

Article info
Received –
2024 July 1
Accepted –
2025 June 20
Available online –
2025 September 20

Keywords
Security, cybersecurity, cyberspace, cyber threats, information sovereignty, critical information infrastructure, cybersecurity forensics, digital criminalistics, ensuring the stability of cyberspace, digital technologies, cyber incident

Taking into account the attention paid by the head of state, legislators and law enforcement practitioners to information security, it is necessary to systematically investigate the category of "cybersecurity" as one of its subspecies.
The article undertakes a multifactorial analysis of cybersecurity issues in modern conditions. Special attention is paid to the development of issues of forensic cybersecurity as an important element of countering criminal cyber incidents.
The article is based on the use of materialistic dialectics as a universal method, as well as general scientific methods such as methods of analysis, synthesis, modeling, and extrapolation. Legal methods were also used - comparative legal, formal legal, technical legal.
It is argued that the concept and content of cybersecurity is derived from the general category of "security". The differentiation of cybersecurity and information security has been made. The author identifies the emergent properties of cybersecurity.
Much attention is paid to the elements of cybersecurity, the subjects and objects of this state, as well as the main categories of cybersecurity. The specific scope of application of cybersecurity measures (incident cyberspace) leads to the emergence of specific technological security facilities. Such objects include critical information infrastructure, software and databases of organizations, information technology devices of users, Internet of Things (IoT) devices. Among the most common cyber threats, the author includes: malicious software (viruses, malware, etc.), phishing and social engineering,

* Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312/.
** The research was carried out at the expense of the Russian Science Foundation grant No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

ISSN 2658-4050 (Online)

MITM (Man-in-the-middle) attacks - embedding into the system and intercepting traffic, denial of service attacks (DOS and DDOS-attacks), data leaks and privacy violations. Cybersecurity actors include users themselves, the state, law enforcement agencies and specialized non-governmental organizations for countering cyber threats - Group IB, Kaspersky Lab, developers of software complexes aimed at protecting in cyberspace, etc. Each cybersecurity subject has a certain set of rights and obligations. A range of unresolved issues has been identified and some ways of solving them have been outlined. The article also focuses on the issues of legal regulation of cybersecurity in Russia.
The author states that cybersecurity in modern conditions is a complex multilevel system, ensuring optimal functioning of which can be achieved only by complex, systematic measures that give a synergistic effect. At the same time, the forensic aspects of cybersecurity must necessarily be proactive, defining technical, tactical and methodological issues of forensic cybersecurity.

1. Введение

Информационная безопасность поставлена Президентом РФ в качестве задачи, решение которой необходимо для достижения национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы»[1]. Высокое внимание, уделяемое данному направлению, подчеркивает также принятие в 2016 г. Доктрины информационной безопасности Российской Федерации[2], отражающей систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Подвидом информационной безопасности (наряду с физической безопасностью информации, безопасностью конечных точек, шифрованием данных и др.) является и кибербезопасность [1, с. 46]. Большое внимание, уделяемое Президентом РФ данному вопросу, насущно требует разработки понятия, структуры, субъектов и самой сущности данной категории.

Кибербезопасность же, как элемент общей информационной безопасности, связана, в первую очередь, с обеспечением безопасности от киберпреступлений и инцидентов в киберпространстве, не подпадающих под уголовную ответственность. Необходимость выделения отдельной категории кибербезопасности в науке и практике обусловлена неуклонным ростом числа киберпреступлений и увеличением ущерба от них. Так, глава МВД России Владимир Колокольцев на заседания коллегии МВД, посвященной вопросам противодействия *IT*-преступлениям, доложил, что «с 2020 года количество посягательств с использованием информационных технологий увеличилось на треть. Доля дистанционных деяний в общем массиве сейчас приближается к 40 %. …Суммарно за 2023 год и 4 месяца текущего (2024 г. – *А. С.*) года он [ущерб] превысил 210 миллиардов рублей. …Постоянно появляются новые способы совершения таких посягательств»[3]. Следует отметить, что выделяемые руководством МВД в статистических показателях *IT*-преступления (преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации) практически соответствуют преступлениям, выделяемым в Будапештской конвенции о киберпреступлениях (компьютерных преступлениях)[4]. Согласно рекомендациям ООН «термин “киберпреступность” охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети»[5]. В английском языке приставка *Cyber* указывает на связь с информацион-

[1] Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» (п. «л» ч. 8) // Президент России: офиц. сайт. URL: http://www.kremlin.ru/events/president/news/63728 (дата обращения: 27.05.2024).

[2] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[3] Владимир Колокольцев провел заседание коллегии МВД России, посвященное противодействию IT-преступности // МВД РФ: офиц. сайт. 2024. 4 июня. URL: https://мвд.рф/news/item/51089163 (дата обращения: 11.06.2024).

[4] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС «Гарант».

[5] Десятый конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правона-

ными технологиями[6]. Многие ученые трактуют киберпреступность именно как «преступность, связанную как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей» (см., напр.: [2–5]), либо, аналогично М.А. Простосердову, «информационно-телекоммуникационных сетей и образованного ими киберпространства [6, с. 30]. Указанные факторы предполагают рассмотрение терминов «*IT*-преступление» и «киберпреступление» в криминалистических целях противодействия киберпреступности и обеспечения кибербезопасности как синонимичных. Необходимость разработки мер противодействия этим угрозам приводит к повышению актуальности, в том числе, криминалистического обеспечения.

Некоторые аспекты информационной безопасности подвергались исследованию в трудах таких отечественных авторов, как И.В. Кубышкин, И.Л. Бачило, А.А. Стрельцов, И.А. Поляков, Г.Г. Горшенков, В.Н. Лопатин, Л.В. Богомолова, А.А. Баранова, В.А. Копылов, П.У. Кузнецов, Е.А. Красненкова, Н.Н. Куняев, Т.А. Полякова и др.

Вопросы кибербезопасности рассматривались в трудах отечественных и зарубежных авторов, таких как В.Г. Степанов-Егиянц, В.А. Мещеряков, А.П. Стельмах, А.В. Тонконогов, В.Б. Вехов, Д.В. Грибанов, Р.И. Дремлюга, Я.О. Кучин, И.Р. Бегишев, В.Ф. Джафарли, Ксяо Линг Ванг, М. Келемен, С. Сзао, И. Вайдова, Дж.Д. Ховард, Дж.С. Смит, У. Файяд, Г. Пятетский-Шапиро, К. Уилсон и др. Однако в связи со скоростью развития электронной техники, информационно-технологических устройств, появления новых форм информации (например, распределенной информации и др.), новых видов угроз (например, полиморфных вирусов, квантовых технологий, направленных на взлом систем идентификации и аутентификации), данные работы, сохраняя свое методологическое значение, в настоящее время уже несколько отстают от развития угроз кибербезопасности и методов противодействия им.

С началом специальной военной операции на территории Украины преступность в киберпространстве получила новый стимул и векторы развития, превращаясь практически в угрозу национальной безопасности, что обусловливает потребность в разработке вопросов обеспечения кибербезопасности.

2. Понятие безопасности

Категория «кибербезопасность» производна от общей дефиниции безопасности (естественно, с учетом специфической кибернетической сферы приложения). Безопасность – это многогранное понятие, однако в основном оно определяется как состояние объекта (например, «состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства»[7]). Аналогичный подход прослеживается и в других нормативных актах[8].

В информационной сфере законодатель исходит из того, что безопасность – это состояние защищенности: «безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак»[9]. Мы также полагаем необходимым пользоваться законодательным подходом.

М.А. Ефремова указывает, что «безопасность в широком смысле следует рассматривать и в статике – как состояние защищенности, и в динамике – как совокупность мер, предпринимаемых для обеспечения

рушителями (Вена, 10–17 апр. 2000 г.). Преступления, Связанные с использованием компьютерной сети: справ. док. для семинара-практикума по преступлениям, связ. с использованием компьютер. сети (п. 9) // Управление Организации Объединенных Наций по наркотикам и преступности: офиц. сайт. URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf.

[6] Кембриджский толковый словарь. URL: https://dictionary.cambridge.org/ru/словарь/англо-русский/cyber (дата обращения: 25.10.2024).

[7] Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности» (в ред. от 24.07.2023) // Собрание законодательства Российской Федерации. 2007. № 7. Ст. 837.

[8] См., напр.: Федеральный закон от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов» (ред. от 08.08.2024) // Собрание законодательства Российской Федерации. 1997. № 30. Ст. 3588; Федеральный закон от 10 января 2002 г. № 7-ФЗ «Об охране окружающей среды» (ред. от 08.08.2024) // Собрание законодательства Российской Федерации. 2002. № 2. Ст. 133; Указ Президента РФ от 31 декабря 2015 г. № 683 «О стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 1. Ст. 212 и др.

[9] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в ред. от 10.07.2023) // Собрание законодательства Российской Федерации. 2017. № 31 (ч. I). Ст. 4736.

этого состояния» [7, с. 56]. Нам же представляется, что названные ею статический и динамический элементы необходимо рассматривать одновременно, в синергии, поскольку само по себе «состояние защищенности», если оно не обусловлено объективными мерами, будет абсурдом. Поэтому, с учетом определения М.А. Ефремовой, под безопасностью можно понимать состояние защищенности, обусловленное комплексом мер, направленных на предотвращение возникновения угроз и их пресечение.

В зависимости от структурного уровня безопасность может быть личной, общественной (всего общества или отдельных коллективов), государственной и международной. Дифференциацию можно также проводить в зависимости от сферы жизнедеятельности, типа угроз и т. д.

Условно можно выделить следующие признаки (свойства) безопасности:

– отсутствие или блокировка угроз;

– возможность стабильного и устойчивого развития;

– наличие и достаточность системы мер предотвращения опасности;

– наличие системы мер прогнозирования рисков;

– доступность помощи;

– наличие строгих правил и процедур обеспечения безопасности;

– контроль и управление доступом.

Однако необходимо отметить, что безопасность на каждом своем структурном уровне и в каждой сфере жизнедеятельности приобретает индивидуальные, характерные эмерджентные признаки.

3. Понятие и сущность кибербезопасности

Используемое в отечественном правовом поле понятие «информационная безопасность» не является полностью тождественным рассматриваемому. Кибербезопасность – это состояние защищенности не от любых информационных угроз, а только от цифровых угроз в киберпространстве, и не от любых угроз, а только от киберугроз [8].

Одно из наиболее, на наш взгляд, удачных определений киберпространства предложено в Модельном законе государств – участников СНГ «О противодействии киберпреступности»: «киберпространство – цифровая среда, возникающая в результате взаимодействия людей, программного обеспечения и сервисов в информационно-телекоммуникационных сетях, включая сеть “Интернет”, посредством связанных с ними технологических устройств и сетей, не существующая в физической форме»[10].

Основными эмерджентными свойствами кибербезопасности, по нашему мнению, являются:

– сетевая подключенность устройств, подвергающихся кибератакам;

– посягательство на информацию только в цифровой форме;

– технологическая сложность информационных устройств, подвергающихся кибератакам;

– перманентное изменение ландшафта кибербезопасности;

– интеллектуальный анализ данных и взаимная интеграция различных мер обеспечения кибербезопасности как обязательное условие;

– гибкость и адаптивность систем обеспечения кибербезопасности;

– активная многоуровневая защита;

– фокусировка не только на отражении атак и пресечении инцидентов безопасности, но и, в значительной мере, на управлении рисками;

– глобальный охват – большинство кибератак сейчас носят трансграничный характер.

Таким образом, можно привести следующую схему дифференциации кибербезопасности и информационной безопасности:

• Различия по цели: у информационной безопасности целью является защита информации от любых угроз, у кибербезопасности – защита только цифровой информации от киберугроз.

• Различия по охвату: в рамках информационной безопасности разрабатываются защитные меры для любой информации, у кибербезопасности защищается информация, размещенная в компьютерных сетях, системах и базах данных.

• Различия по защитным мерам: для информационной безопасности характерны физические, технические, административные и иные меры, для кибербезопасности – технологические и программные меры и инструменты.

Необходимо также рассмотреть возможность использования категории «Цифровая безопасность». Нам представляется, что, поскольку применительно к информации прилагательное «цифровая» используется для описания способа ее дискрет-

[10] Модельный закон «О противодействии киберпреступности» (принят на пятьдесят пятом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление № 55-20 от 14 апреля 2023 г.)) // СПС «Гарант».

ной передачи, то логичнее было бы использовать термин «безопасность цифровой информации» (как отдельного вида информации). Однако, с учетом активно используемых в последнее время оборотов, содержащих определение «цифровой», в контексте использования цифровых (электронных) устройств или рассмотрения этих устройств как объектов исследования («цифровая экономика», «цифровая криминалистика», «цифровая грамотность» и т. д.), мы полагаем, что категорию «цифровая безопасность» можно использовать как аналог категории «кибербезопасность».

Даже оперируя категорией «кибербезопасность», большинство документов не раскрывают ее сущность. Причем в некоторых случаях документ, имея в своем названии категорию «кибербезопасность», не то что не раскрывает, вообще не упоминает ее в тексте[11].

Модельный закон государств – участников СНГ «О противодействии киберпреступности» содержит следующее определение кибербезопасности: «сохранение конфиденциальности, целостности и доступности информации в киберпространстве, а также защищенности информационной инфраструктуры». Нам данное определение представляется вполне возможным к использованию.

4. Структура кибербезопасности

Для того чтобы определиться со структурой кибербезопасности в современных условиях, необходимо, в первую очередь, проанализировать научные подходы к элементам безопасности.

В.Л. Манилов называет следующие элементы безопасности: угрозы, интересы, факторы воздействия на них и методы обеспечения [9, с. 17]. По мнению А.И. Стахова, в число элементов безопасности входят субъекты безопасности, объекты безопасности, угрозы безопасности [10, с. 6]. Другие авторы предлагают сходные трактовки структуры [11, с. 20; 12, с. 6].

По результатам анализа мнений различных авторов можно констатировать, что в структуру кибербезопасности входят: объекты обеспечения кибербезопасности, киберугрозы, субъекты кибербезопасности.

Специфическая сфера приложения мер обеспечения кибербезопасности (инцидентное киберпространство) приводит к появлению специфических технологических объектов обеспечения безопасности. К таким объектам относятся критическая информационная инфраструктура, программное обеспечение и базы данных организаций, информационно-технологические устройства пользователей, устройства интернета вещей (*IoT*).

К числу объектов критической информационной инфраструктуры, по определению законодателя, относятся «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры»[12]. Именно они в первую очередь составляют фокус внимания российского подхода к кибербезопасности (см., напр.: [13]).

Базы данных организаций, подвергающиеся нарушению кибербезопасности, могут носить как открытый характер, так и характер ограниченного пользования. При этом мы полагаем необходимым включать в число данных баз и программное обеспечение не только объектов коммерческих и некоммерческих «частных» юридических лиц, но и базы и программное обеспечение государственных и муниципальных органов, не входящие в комплекс критической информационной инфраструктуры.

Кибербезопасность информационно-технологических устройств, в первую очередь, связана с их использованием как элемента сети либо безопасностью самих сетей как информационно-технологических устройств. Что касается компьютерных сетей как объекта кибербезопасности, то их следует дифференцировать на несколько уровней: нательная сеть (*Body area network*), персональная сеть (*Personal area network*, *PAN*), локальная сеть (*Local area network*, *LAN*), кампусная сеть (*Campus area network*, *CAN*), городская сеть (*Megapolis area network*, *MAN*) и глобальная сеть (*Wide area network*, *WAN*). Вмешательство в функционирование сетей любого уровня может иметь тяжелые последствия – от гибели носителя нательной сети вследствие несвоевременной реакции стимулятора или инсулиновой помпы до невозможности международного обмена информацией.

Термин «интернет вещей» был предложен Кэвином Эштоном в 1999 г. Как мы уже отмечали, «элементы концепции “интернет вещей” могут как

[11] См., напр.: Межгосударственный стандарт ГОСТ ISO/IEC 27014–2021 Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности. М.: Стандартинформ, 2021. v, 17 с.

[12] Пункт 7 ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ.

использоваться при совершении преступления при взломе различных систем (при взломе системы контроля и управления доступом – нарушение неприкосновенности жилища, кражи; системы видеонаблюдения – нарушение неприкосновенности частной жизни; взлом банковских приложений или приложений для оплаты – кража и т. д.), так и нести на себе прямые или косвенные признаки совершения их владельцами преступлений» [14, с. 455–456]. Важность исследования кибербезопасности систем интернета вещей подчеркивают и зарубежные авторы [15; 16].

А.З. Таков придерживается мнения, что «киберугрозы – это совокупность условий и факторов, при которых нарушается частная и общественная безопасность, создается информационная опасность. Киберугрозы с объективной стороны – это действия, предпринимаемые преступниками в цифровом пространстве» [17, с. 233].

По мнению Д.А. Камбулова, к основным источникам киберугроз относятся национальные государства, террористические организации, преступные группы, хакеры, вредоносные инсайдеры [18, с. 1657–1658].

По мнению О.Г. Ковалева и Н.В. Семенова, «основными субъектами кибербезопасности в настоящее время являются должностные лица государственных органов, органов местного самоуправления, наделенных соответствующими полномочиями, среди которых особо выделяются правоохранительные структуры, а также специальные службы (Генеральная прокуратура, Министерство внутренних дел, Следственный комитет, Федеральная служба безопасности, Министерство обороны, Федеральная служба охраны, Министерство юстиции Российской Федерации и подведомственная ему Федеральная служба исполнения наказаний, а также Росгвардия)» [19]. Нам же представляется, что субъектов обеспечения кибербезопасности нужно трактовать несколько шире и относить к их числу самих пользователей, государство, правоохранительные органы и специализированные негосударственные организации по противодействию киберугрозам – *Group IB*, «Лаборатория Касперского», разработчиков программных комплексов, направленных на защиту в киберпространстве, и т. д. Субъекты кибербезопасности – это в первую очередь те, кто ее обеспечивает, а не только борется с последствиями ее нарушения. Субъекты кибербезопасности имеют определенный комплекс прав и обязанностей, связанных с владением или пользованием информационным ресурсом, предусмотренный Федеральным закон от 27 июля 2006 г. № 149-ФЗ[13], а также прав, предусмотренных Уголовно-процессуальным кодексом РФ, при участии в уголовном процессе в качестве специалистов.

5. Механизм кибербезопасности

Мы полагаем, что по своей сути механизм обеспечения кибербезопасности представляет собой комплекс стратегий, методов и мер, направленных на защиту информационных систем, сетей и данных в инцидентном киберпространстве от различных киберугроз. Применение этих механизмов помогает предотвратить, обнаружить и реагировать на инциденты безопасности.

Среди общих методов, составляющих механизм обеспечения кибербезопасности, доступных любому пользователю, можно выделить: своевременную установку обновлений и исправлений, идентификацию и аутенитификацию пользователей, установку и своевременное использование брандмауэров и антивирусного программного обеспечения.

М.М. Безкоровайный и А.Л. Татузов, кроме общих методов обеспечения безопасности киберпространства, выделяют также группы специальных и интеллектуальных методов. К специальным методам обеспечения безопасности киберпространства они относят:

– анализ топологической структуры и выработку рекомендаций по ее изменению, способов и конкретных алгоритмов их реализации;

– новые методы криптографической защиты, основанные не только на чисто вычислительных механизмах реализации стойкости, но и на использовании преимуществ многосвязной архитектуры связей и большого числа добропорядочных пользователей;

– методы информационной безопасности на основе социальных сервисов для противодействия кибер-атакам с применением специальных процедур анализа группового поведения.

В интеллектуальные методы они включают:

– методы интеллектуальной идентификации пользователей;

– предотвращения вирусных и других атак;

– выявления атак и проникновений;

– ситуационного анализа состояния информационной безопасности;

[13] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 08.08.2024) // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3448.

ISSN 2542-1514 (Print)

– новые методы криптографической защиты, основанные на нейросетевых технологиях [20, с. 26].

С данным подходом можно согласиться, однако к спектру методов необходимо также добавить организационные и криминалистические, рассматривающие организационное, технико- и тактико-криминалистическое обеспечение кибербезопасности, привлечение сообществ практиков в области кибербезопасности.

К организационным мерам можно отнести также мониторинг и прогнозирование рисков, разработку стратегий смягчения рисков, обучение сотрудников кибергигиене, распознаванию киберугроз и реагированию на них

К основным мерам обеспечения кибербезопасности относятся: надежные сложные пароли, двухфакторная аутентификация; регулярная проверка учетной записи; своевременное обновление программных средств защиты; мониторинг сетевой активности; обучение и самообразование; регулярное резервное копирование; шифрование данных; безопасность при онлайн-покупках и посещении подозрительных сайтов; осторожность при использовании общественных *Wi-Fi* сетей; разработки использования стратегий ограничения доступа и контроля за доступом; проверка используемых электронных носителей информации; сотрудничество с организациями, созданными для противодействия и расследования компьютерных инцидентов.

Стратегии кибербезопасности в зарубежных странах содержат хотя и различные, но во многом близкие подходы: использование сил быстрого реагирования на компьютерные инциденты, максимальное распространение информации о положительных практиках противодействия злоумышленникам, ответственность операторов сетей за недостаточное использование мер безопасности, неинформирование соответствующих структур и т. д., особые условия хранения и использования персональных данных пользователей и др., что позволяет анализировать и заимствовать удачные практики для использования в нашей стране.

В стратегическом плане механизм обеспечения кибербезопасности включает в себя контроль доступа как первый уровень противодействия киберинцидентам; уровень системной защиты, включающий необходимое программное обеспечение; предупреждение инцидентов и защиту информационных систем; анализ рисков для систем и сетей различного уровня; обнаружение, пресечение и иное реагирование на компьютерные инциденты; расследование совершенных киберпреступлений и иных киберинцидентов. Во многом кибербезопасность включает в себя также технологический суверенитет, снижение зависимости от вендоров, использование отечественного программного обеспечения.

Насущно необходима именно Стратегия кибербезопасности РФ как единый концептуальный документ. Можно согласиться с М.А. Простосердовым, что в нее должны войти: защита стратегических и правительственных объектов (энергетики, нефтяного, газового и военно-промышленного комплекса, ЖКХ и т. д.); обеспечение безопасности граждан, организаций и государства как в сфере компьютерной информации, так и в сфере экономических отношений (отношений собственности и отношений в сфере экономической деятельности); совершенствование законодательства; борьба с анонимностью; международное сотрудничество; развитие специальных правоохранительных органов; развитие информационных технологий; повышение цифровой грамотности населения [6, с. 178].

6. Выводы

Подводя итог, можно констатировать, что, несмотря на масштабные разработки в области обеспечения безопасности в киберпространстве, цифровой гигиены и оперативного реагирования на компьютерные инциденты, не решены многие вопросы в области обеспечения кибербезопасности критической информационной инфраструктуры, а также юридических лиц и граждан в киберпространстве. Отсутствует комплексный подход к решению вопросов обеспечения кибербезопасности критической информационной инфраструктуры с привлечением всех субъектов, предусмотренных п. 8 ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», несмотря на принятие данного закона. Критическая информационная инфраструктура обладает сложной архитектурой, что усложняет ее защиту и повышает сложность управления киберрисками. В значительной степени этому способствует и недостаточный объем специализированной подготовки сотрудников правоохранительных органов в рассматриваемой сфере. Сохраняются уязвимости в программном обеспечении. Активизация киберугроз в период санкционной войны и проведения специальной военной операции на территории Украины приводит к массовым атакам на информационные ресурсы российских органов власти. Так, на момент написания данной статьи почти месяц как остаются недоступными в результате хакерской

атаки сайты государственной автоматизированной системы «Правосудие» (https://sudrf.ru/)[14] и Судебного департамента при Верховном Суде РФ (http://www.cdep.ru/). Ограниченный доступ к передовым технологиям также снижает безопасность критической информационной инфраструктуры.

С учетом трансграничного характера многих киберинцидентов можно отметить, что только внутригосударственные меры обеспечения безопасности в киберпространстве не всегда могут быть достаточно эффективными. Необходима организация международного сотрудничества в данной сфере.

Негативно влияет на безопасность в киберпространстве и недостаточный программный и технологический суверенитет. Использование программных комплексов, разработанных за рубежом, может приводить к атакам, утечкам информации, перехвату управления через бэкдоры (англ. *back door* – букв. «задняя дверь», т. е. «черный ход») – дефекты алгоритма программы, намеренно встроенные в нее разработчиком для последующего несанкционированного доступа или перехвата управления.

Таким образом, кибербезопасность в современных условиях представляет собой состояние защищенности киберпространства электронных устройств субъекта, обусловленное сложной многоуровневой системой, обеспечение оптимального функционирования которой может быть достигнуто только комплексными, систематическими мерами, дающими синергетический эффект.

СПИСОК ЛИТЕРАТУРЫ

1. Богомолова Л. В. Информационная безопасность: что это такое в современных реалиях / Л. В. Богомолова // Вестник науки и образования. – 2023. – № 1-1 (132). – С. 45–48.

2. Сериева М. М. Киберпреступность как новая криминальная угроза / М. М. Сериева // Новый юридический вестник. – 2017. – № 1. – С. 104–106.

3. Номоконов В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 1 (24). – С. 45–55.

4. Немов М. В. Киберпреступность как новая криминальная угроза / М. В. Немов // Эпоха науки. – 2017. – № 9. – С. 47–51.

5. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность / А. С. Алпеев // Вопросы кибербезопасности. – 2014. – № 5. – С. 39–42.

6. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук / М. А. Простосердов. – М., 2016. – 232 с.

7. Ефремова М. А. Уголовно-правовая охрана информационной безопасности : дис. ... д-ра юрид. наук / М. А. Ефремова. – М., 2017. – 427 с.

8. Баландин А. Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий / А. Ю. Баландин // Правовая политика и правовая жизнь. – 2023. – № 3. – С. 260–270. – DOI: 10.24412/1608-8794-2023-3-260-270.

9. Манилов В. Л. Теория и практика организации системы обеспечения национальной безопасности России : автореф. дис. … д-ра полит. наук / В. Л. Манилов. – М., 1995. – 36 с.

10. Стахов А. И. Безопасность в правовой системе Российской Федерации / А. И. Стахов // Безопасность бизнеса. – 2006. – № 1. – С. 2–7.

11. Авдеев М. А. Теоретические и правовые основы обеспечения личной и имущественной безопасности участников уголовного судопроизводства : дис. … канд. юрид. наук / М. А. Авдеев. – М., 2009. – 170 с.

12. Кондрашов Б. П. Общественная безопасность и административно-правовые средства ее обеспечения / Б. П. Кондрашов. – М. : Щит-М, 1998. – 296 с.

13. Мосечкин И. Н. Проблемы уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации / И. Н. Мосечкин // Всероссийский криминологический журнал. – 2023. – Т. 17, № 1. – С. 22–34. – DOI: 10.17150/2500-1442.2023.17(1).22-34.

[14] В настоящее время доступ пользователей к сайту восстановлен. – *Примеч. ред.*

14. Смушкин А. Б Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности / А. Б Смушкин // Всероссийский криминологический журнал. – 2020. – Т. 14, № 3. – С. 453–460. – DOI: 10.17150/2500-4255.2020.14(3).453-460.

15. Casarosa F. Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework / F. Casarosa // Computer Law & Security Review. – 2024. – Vol. 53. – Art. 105982. – DOI: 10.1016/j.clsr.2024.105982.

16. Weber R. H. Cybersecurity in the Internet of Things: Legal aspects / R. H. Weber, E. Studer // Computer Law & Security Review. – 2016. – Vol. 32, Iss. 5. – P. 715–728. – DOI: 10.1016/j.clsr.2016.07.002.

17. Таков А. З. Проблемы обеспечения кибербезопасности в современных цифровых системах / А. З. Таков // Пробелы в российском законодательстве. – 2023. – Т. 16, № 5. – С. 232–236.

18. Камбулов Д. А. Угрозы кибербезопасности / Д. А. Камбулов // StudNet. – 2021. – Т. 4, № 7. – С. 1657–1658.

19. Ковалев О. Г. Кибербезопасность современной России: теоретические и организационно-правовые аспекты / О. Г. Ковалев, Н. В. Семенова // Столыпинский вестник. – 2021. – Т. 3, № 1. – URL: https://stolypin-vestnik.ru/wp-content/uploads/2021/02/Kovalev_O_G_Semenova_N_V_Kiberbezopasnost.pdf.

20. Безкоровайный М. М. Кибербезопасность – подходы к определению понятия / М. М. Безкоровайный, А. Л. Татузов // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 22–27.

REFERENCES

1. Bogomolova L.V. Information security: what is it in modern realities. *Vestnik nauki i obrazovaniya*, 2023, no. 1-1 (132), pp. 45–48. (In Russ.).

2. Serieva M.M. Cybercrime as a new criminal threat. *Novyi yuridicheskii vestnik*, 2017, no. 1, pp. 104–106. (In Russ.).

3. Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat. *Kriminologiya: vchera, segodnya, zavtra*, 2012, no. 1 (24), pp. 45–55. (In Russ.).

4. Nemov M.V. Cybercrime as a new criminal threat. *Epokha nauki*, 2017, no. 9, pp. 47–51. (In Russ.).

5. Alpeev A. Terminology of security: cybersecurity, information security. *Voprosy kiberbezopasnosti*, 2014, no. 5, pp. 39–42. (In Russ.).

6. Prostoserdov M.A. *Economic crimes committed in cyberspace and measures to counteract them*, Cand. Diss. Thesis. Moscow, 2016. 232 p. (In Russ.).

7. Efremova M.A. *Criminal law protection of information security*, Doct. Diss. Moscow, 2017. 427 p. (In Russ.).

8. Balandin A.Y. Cyber security and information security. Demarcation of legal categories. *Pravovaya politika i pravovaya zhizn'*, 2023, no. 3, pp. 260–270. DOI: 10.24412/1608-8794-2023-3-260-270. (In Russ.).

9. Manilov V.L. *Theory and practice of the organization of the national security system of Russia*, Doct. Diss. Thesis. Moscow, 1995. 36 p. (In Russ.).

10. Stakhov A.I. Security in the legal system of the Russian Federation. *Bezopasnost' biznesa = Business security*, 2006, no. 1, pp. 2–7. (In Russ.).

11. Avdeev M.A. *Theoretical and legal foundations of ensuring personal and property security of participants in criminal proceedings*, Cand. Diss. Moscow, 2009. 170 p. (In Russ.).

12. Kondrashov B.P. *Public safety and administrative and legal means of ensuring it*. Moscow, Shchit-M Publ., 1998. 296 p. (In Russ.).

13. Mosechkin I.N. Problems of the Criminal Law Protection of Critical Information Infrastructure of the Russian Federation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 1, pp. 22–34. DOI: 10.17150/2500-1442.2023.17(1).22-34. (In Russ.).

14. Smuskin A.B. Some Aspects of Using the Concept of «the Internet of Things» in Crime Counteraction. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460. (In Russ.).

15. Casarosa F. Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework. *Computer Law & Security Review*, 2024, vol. 53, art. 105982. DOI: 10.1016/j.clsr.2024.105982.

16. Weber R.H., Studer E. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 2016, vol. 32, iss. 5, pp. 715–728. DOI: 10.1016/j.clsr.2016.07.002.

17. Takov A.Z. Cybersecurity issues in modern digital systems. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian legislation*, 2023, vol. 16, no. 5, pp. 232–236. (In Russ.).

18. Kambulov D.A. Cyber security threats. *StudNet*, 2021, vol. 4, no. 7, pp. 1657–1658. (In Russ.).

19. Kovalev O.G., Semenova N.V. Cybersecurity in modern Russia: theoretical and organizational and legal aspects. *Stolypinskii vestnik*, 2021, vol. 3, no. 1, available at: https://stolypin-vestnik.ru/wp-content/uploads/2021/02/Kovalev_O_G_Semenova_N_V_Kiberbezopasnost.pdf. (In Russ.).

20. Bezkorovainy M., Tatuzov A. Cybersecurity - approaches to the definition. *Voprosy kiberbezopasnosti*, 2014, no. 1 (2), pp. 22–27. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Смушкин Александр Борисович – кандидат юридических наук, доцент, ведущий научный сотрудник проектного офиса научных программ и исследований, доцент кафедры криминалистики
Саратовская государственная юридическая академия
410056, Россия, г. Саратов, ул. им. Н.Г. Чернышевского, 104
E-mail: Skif32@yandex.ru
ORCID: 0000-0003-1619-8325
ResearcherID: AAM-2853-2020
Scopus AuthorID: 57202012484

INFORMATION ABOUT AUTHOR

Alexander B. Smushkin – Candidate of Law, Associate Professor; Leading Researcher, Project Office of Scientific Programs and Research; Associate Professor, Department of Criminology
Saratov State Law Academy
104, im. N.G. Chernyshevskogo ul., Saratov, 410056, Russia
E-mail: Skif32@yandex.ru
ORCID: 0000-0003-1619-8325
ResearcherID: AAM-2853-2020
Scopus AuthorID: 57202012484

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Смушкин А.Б. Кибербезопасность: понятие, структура, механизм правового обеспечения / А.Б. Смушкин / Правоприменение. – 2025. – Т. 9, № 3. – С. 114–123. – DOI: 10.52468/2542-1514.2025.9(3).114-123.

BIBLIOGRAPHIC DESCRIPTION

Smushkin A.B. Cybersecurity: concept, structure, the mechanism of legal ensuring. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 3, pp. 114–123. DOI: 10.52468/2542-1514.2025.9(3).114-123. (In Russ.).