УДК 004.056

***С.П. Серёдкин*[1]**

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Россия*

СОВРЕМЕННЫЙ ВЗГЛЯД НА ТОЛКОВАНИЕ ПОНЯТИЯ КИБЕРБЕЗОПАСНОСТЬ

Аннотация. В данной работе проведен анализ понятий «кибербезопасность» и «информационная безопасность», раскрываются различия между ними, приводится эволюция происхождения значений, анализируются наиболее значимые сферы совпадений, а также возможные способы и области использования. Даётся оценка современным понятиям и сопоставление их с мировыми тенденциями, предлагается точка зрения автора на толкование термина кибербезопасность.

Ключевые слова: кибербезопасность, киберугрозы, информационная безопасность, информационные системы, интеллектуальные цифровые технологии, цифровизация, информация, угрозы, автоматизированные системы управления, критическая информационная инфраструктура

S.P. Seryodkin1

[1]*Irkutsk State Transport University, Irkutsk, Russia*

MODERN VIEW ON THE INTERPRETATION OF THE CONCEPT OF CYBERSECURITY

Abstract. In this paper, the concepts of "cybersecurity" and "information security" are analyzed, the differences between them are revealed, the evolution of the origin of meanings is given, the most significant areas of coincidence are analyzed, as well as possible ways and areas of use. The assessment of modern concepts and their comparison with global trends is given, and the author's point of view on the interpretation of the term cybersecurity is proposed. the main directions of possible changes in the terms under consideration.

Keywords: cybersecurity, cyber threats, information security, information systems, intelligent digital technologies, digitalization, information, threats, automated control systems, critical information infrastructure

Введение. Тенденции современного развития информационных технологий, стремительная цифровизация экономики имеют доминирующее значение на современном этапе и формируют ряд проблем, связанных с обеспечением информационной безопасности [1].

Веб ресурсы организаций, объекты критической информационной инфраструктуры (КИИ), информационные системы государственного управления в последнее время подвергаются беспрецедентному воздействию кибератак со стороны недружественных государств и отдельных хакерских групп. Внедрение в инструментарий бизнес процессов информационно цифровых технологий (ИЦТ), цифровизация отраслей экономики и как следствие возрастание количества компьютерных атак, всё это способствовало увеличению исследований в области кибербезопасности. Использование термина «кибербезопасность» и замена ею понятия «информационная безопасность» в последние годы вызывают не однозначное восприятие.

Сути этих точек зрения у профессионалов в области безопасности. В работе приводятся различия между данными определениями, и описана связь этих понятий с информационной безопасностью.

Отсутствие единой терминологии в этом вопросе порождает неоднозначное понимание сути представляемого материала как в средствах массовой информации, так и в научном сообществе, требует конкретизации и дополнительного разъяснения ключевых мнений и областей применения, все это обуславливает актуальность темы исследования.

Целью данной работы является попытка проанализировать термины «кибербезопасность» и «информационная безопасность», обосновать различия и сходства,

раскрыть области использования, а также предложить точку зрения автора по толкованию и применению понятия – «кибербезопасность».

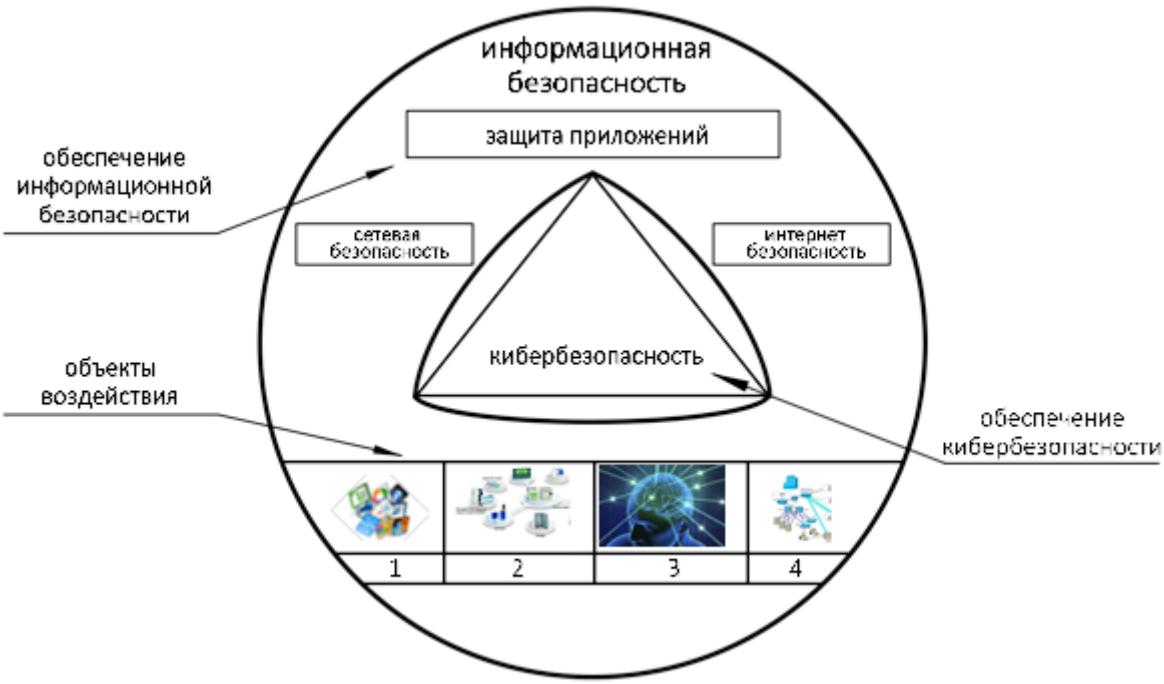
Информационная база исследования. Вопросам исследования данной области посвящены многие научные статьи, из которых можно выделить работы М.М. Бескоровайного [12], Т.Н. Малик, А. А. Бессоновой, В.В. Герасимова, К.В. Мирошниченко [13], в которых зафиксированы основные подходы к определению информационной и кибернетической безопасностей. В связи с принятием в 2006 году Федерального Закона «Об информации, информационных технологиях и защите информации» [1] было законодательно закреплено понятие термина «информационная безопасность» и положено начало повсеместного использования данного термина во всех правовых документах, в данное время этот термин считается приемлемым и понятным. В доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 года № 646, информационная безопасность определена как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз» [2]. В нормативно правовых документах безопасность информации [данных] трактуется как состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность [3]. В действующей в Российской Федерации системе нормативно правовых актов и документов четко определены понятия, связанные с информационной безопасностью. Определений и понятий относительно термина кибербезопасность в Российском законодательстве не закреплено. В официальных документах РФ по защите информации термин «кибербезопасность» не выделяется из понятия «информационная безопасность» и не применяется отдельным термином. Если говорить о сфере применения термина «кибербезопасность», то в основном данное определение можно встретить в средствах массовой информации (СМИ), в тезисах и докладах по вышеупомянутой тематике. В научных публикациях данное определение встречается довольно редко. В то же время в большинстве зарубежных стран толкование понятия кибербезопасность выделяется в самостоятельное определение. Так Национальный институт стандартов и технологий США (NIST) дает определение кибербезопасности как «способность защищать или защищать использование киберпространства от кибератак» [4]. Хотя есть и другие определения – у CISA (Сертифицированный аудитор информационных систем) есть свое определение, как и у ISO (Международная организация по стандартизации), – большинство из них похожи.

Понятие термина «кибербезопасность»: «кибер» происходит от греческого слова κυβερνητικός и означает искусство управления. Термин «кибербезопасность» (cybersecurity) получил распространение в середине 1990-х гг. сначала в США, затем в Европе, а позднее – и в других странах [5]. В зарубежных стандартах дается довольно полное понятие термина – кибербезопасность. В источнике [6] «Кибербезопасность - условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными». Определение понятия кибербезопасность по мнению автора в источнике [7] более ёмко дает определение: «Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов».

Парадигма исследования. Учитывая тот факт, что, начиная с 2015г в России термин «кибербезопасность» массово тиражируется не только в журналистской среде и СМИ, но и на правительственном уровне, справедливо возникает вопрос у специалистов о правомочности употребления данного термина. Безусловно, в этой практике сказывается массовый характер использования данного термина на международном уровне. В связи с данной тенденцией у специалистов справедливо возникает вопрос о необходимости стандартизации подходов в толковании вышеуказанных терминов.

Приведем несколько определений, имеющих отношение к выше упомянутым понятиям: «Информационное пространство – совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей» [8]; «Киберпространство - сложная сущность, которая реально существует в виде глобальной совокупности процессов взаимодействия людей, программного обеспечения и сервисов Интернет в сетях (включая подключенное к ним технологическое оборудование), но которая при этом никак не проявляется в какой-либо известной, материальной форме» [9]; «Угроза информационной безопасности - совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации» [3]; «Киберугроза {cyber threat} – потенциальная причина нежелательного инцидента кибербезопасности, который может нанести вред системе, людям, обществу, организации или другим объектам в киберпространстве» [10].

Корреляция областей функционирования и объектов воздействия кибербезопасности и информационной безопасности приведена на рис.1.



Примечание:
Объекты воздействия;
1.Программное обеспечение.
2.Прогаммно-аппаратные и др. средства управления.
3.Интелект человека и массовое сознание.
4.Каналы связи, обеспечивающие передачу информационных потоков и систем управления.

Рис. 1. Корреляция областей функционирования и объектов воздействия

Как видно из приведенного рисунка, кибербезопасность является частью информационной безопасности и обеспечивает защиту приложений, сетевую безопасность, интернет безопасность объектов особо важной информационной инфраструктуры.

Анализируя приведенные выше материал и рассуждения, хотелось бы выразить точку зрения к толкованию термина «кибербезопасность» и по возможности аргументировать её:

1. По составу выражения- использование в термине «кибербезопасность» приставки «кибер» эволюционно указывает на принадлежность данного термина к управлению, т.е. обеспечение информационной безопасности объектов управления.

2. Целью кибератак на объекты защиты является деструктивное воздействие, в первую очередь, на структуру управления. Именно такого рода угрозы по замыслу злоумышленников должны привести к катастрофам техногенного характера, имеющих как социальное, так и политическое значение.

3. Для деструктивного воздействия на объекты управления злоумышленникам необходимо использовать сложные угрозы, для создания которых необходимы прогрессивные высокотехнологические информационные технологии, в которых используются программные продукты управленческого характера. Тестирование злоумышленниками данных атак с функцией поиска уязвимостей, это не что иное, как кибератака.

4. Противодействие данному виду высокотехнологичных угроз, т.е обеспечение информационной безопасности объектов управления по логике можно толковать как кибербезопасность.

Подытоживая сказанное можно считать, что кибербезопасность – состояние защищенности информационной инфраструктуры от высокотехнологичных угроз, направленных на объекты управления с целью вывода этих объектов из штатного режима функционирования.

Выводы. Представленная в статье информация определяет предмет толкования термина «кибербезопасность» как мало исследованной темы, по которой недостаточно информации по однозначному толкованию и использованию данного определения**.** Данная тема в настоящее время находится в изучении и требует дополнительного исследования и анализа.

Изложенные в статье доводы могут быть полезны специалистам по защите информации, а также государственным служащим в сфере информационной безопасности для совершенствования нормативно-правовой базы по защите информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://cyberleninka.ru/.

2. «Доктрина информационной безопасности Российской Федерации». Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

3. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

4. https://www.nist.gov/.

5.file:///C:/Users/Seredkin_SP/Downloads/gosudarstvennoe-regulirovanie-sfery-kiberbezopasnosti-problemy-atributsii-atak-i-lokalizatsii-dannyh.pdf].

6. ISO/IEK 27032 2012 «Information technology — Security techniques — Guidelines for cybersecurity».

7. IEC TS 62443-1-1:2009 «Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models».

8. ГОСТ Р 59797-2021 «Информационные технологии. Сложные системы. Интероперабельность. Основные положения».

9. ISO/IEC 27032:2012 «Information technology — Security techniques — Guidelines for cybersecurity».

10. "Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации" (утв. Президентом РФ 03.02.2012 N 803).

11. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

12.file:///C:/Users/%D0%A1%D0%B5%D1%80%D0%B3%D0%B5%D0%B9/Downloads/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya.pdf.

13. Информационная безопасность регионов России (ИБРР-2021). И 74 XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27-29 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021. – 427 с.

14. Ясенев В.Н., Дорожкин А.В., Матвеев В.А., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2018 – 182с.

15. https://www.secuteck.ru/thematic-plan-2023?ysclid=ligydpfhdn670884186.

16. https://d-russia.ru/category/kiberbezopasnost.

REFERENCES

1. https://cyberleninka.ru /.

2. "The Doctrine of information security of the Russian Federation". Approved by Decree of the President of the Russian Federation dated December 5, 2016 No. 646.

3. GOST R 53114-2008 "Information protection. Ensuring information security in the organization. Basic terms and definitions".

4. https://www.nist.gov /.

5.file:///C:/Users/Seredkin_SP/Downloads/gosudarstvennoe-regulirovanie-sfery-kiberbezopasnosti-problemy-atributsii-atak-i-lokalizatsii-dannyh.pdf].

6. ISO/IEK 27032 2012 "Information technology — Security techniques — Guidelines for cybersecurity".

7. IEC TS 62443-1-1:2009 "Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models".

8. GOST R 59797-2021 "Information technologies. Complex systems. Interoperability. The main provisions".

9. ISO/IEC 27032:2012 "Information technology — Security techniques — Guidelines for cybersecurity".

10. "The main directions of state policy in the field of ensuring the safety of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation" (approved by the President of the Russian Federation on 03.02.2012 N 803).

11. Decree of the President of the Russian Federation No. 400 dated July 2, 2021 "On the National Security Strategy of the Russian Federation".

12.file:///C:/Users/%D0%A1%D0%B5%D1%80%D0%B3%D0%B5%D0%B9/Downloads/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya.pdf.

13. Information security of Russian regions (IBRD-2021).And 74th XII St. Petersburg Interregional Conference. St. Petersburg, October 27-29, 2021: Materials of the conference / SPOISU. – St. Petersburg, 2021. – 427 p.

14. Yasenev V.N., Dorozhkin A.V., Matveev V.A., Sochkov A.L., Yasenev O.V. Under the general editorship of Prof. Yaseneva V.N. INFORMATION SECURITY: A textbook. – Nizhny Novgorod: Nizhny Novgorod State University named after N.I. Lobachevsky, 2018 – 182s.

15. https://www.secuteck.ru/thematic-plan-2023? ysclid=ligydpfhdn670884186.

16. https://d-russia.ru/category/kiberbezopasnost.

Информация об авторе

Сергей Петрович Серёдкин – к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Sergei Petrovich Seryodkin – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Современный взгляд на толкование понятия кибербезопасность // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2023. – №2(18). – С.17-22– DOI: 10.26731/2658-3704.2023.2(18).17-22 – Режим доступа: http://ismm-irgups.ru/toma/218-2023, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 17.06.2023)

For citations

Seryodkin S.P. Modern view on the interpretation of the concept of cybersecurity // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: elektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2023. No. 2(18). P. 17-22. DOI: 10.26731/2658 3704.2023.2(18).17-22 [Accessed 17/06/23]