DOI 10.21672/2074-1707.2020.51.1.094-102
УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМЫЙ АТРИБУТ МНОГОУРОВНЕВОГО ЗАЩИЩЕННОГО КИБЕРПРОСТРАНСТВА

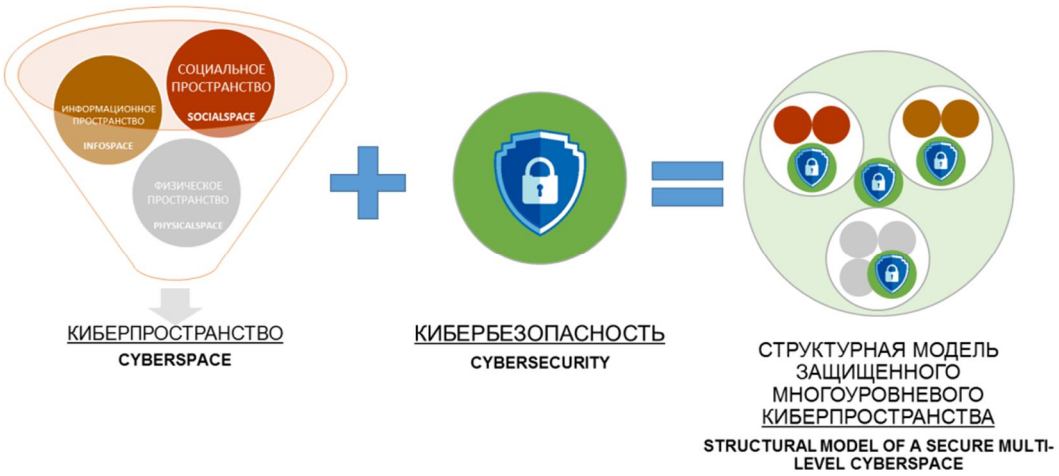
Статья поступила в редакцию 22.05.2020, в окончательном варианте – 11.09.2020.

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: https://orcid.org/0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: msanya@yandex.ru

В статье выполнен системный анализ ряда вопросов, связанных с проблематикой защищенного кибернетического пространства: дана характеристика понятия защищенного кибернетического пространства, приведены его характеристики, указаны границы, представлена структура и многоуровневая структурная модель. Предложена классификация киберугроз на 2020 г. Определено место и роль кибербезопасности в качестве неотъемлемого атрибута каждой структурной единицы, обеспечивающей защищенность кибернетического пространства. Проанализированы работы авторов, относящихся к тематике статьи. Для определения стратегии противодействия киберугрозам сформирована структура защищенного многоуровневого кибернетического пространства. В статье она представлена в виде структурной многоуровневой модели в нотации BPMN 2.0 и включает в себя социальное, физическое и информационное пространства. Для них неотъемлемым атрибутом является обеспечение кибербезопасности, определяющей, в том числе, конфиденциальность, целостность и доступность информации, представленной в цифровом виде. Для каждого уровня описаны структурные элементы, объекты и субъекты, которые в непрерывном взаимодействии друг с другом обеспечивают существование многоуровневого защищенного кибернетического пространства.

Ключевые слова: кибербезопасность, киберугрозы, цифровое информационное пространство, защищенное киберпространство, информационная безопасность, модель взаимосвязи открытых систем, цифровая личность, цифровая граница, BPMN 2.0

Графическая аннотация (Graphical annotation)



CYBER SECURITY AS AN ESSENTIAL ATTRIBUTE OF MULTILEVEL PROTECTED CYBER SPACE

The article was received by the editorial board on 22.05.2020, in the final version – 11.09.2020.

Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci (Engineering), Associate Professor, ORCID: https://orcid.org/0000-0001-9974-7144, e-mail: putyato.m@gmail.com

Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci (Engineering), Associate Professor, e-mail: msanya@yandex.ru

The article provides a systematic analysis of a number of issues related to the problem of protected cybernetic space: the concept of protected cybernetic space is characterized, its characteristics are given, borders are specified, and the structure and multi-level structural model are presented. The classification of cyber threats for 2020 is proposed. The place and role of cybersecurity as an integral attribute of each structural unit ensuring the security of the cybernetic space is defined. The authors ' works related to the subject of the article are analyzed. To determine the strategy for countering cyber threats, the structure of a protected multi-level cybernetic space was formed. In the article, it is presented as a structural multi-level model in BPMN 2.0 notation and includes social, physical and information spaces. For them, an integral attribute is ensuring cybersecurity, which determines, among other things, the confidentiality, integrity and availability of information presented in digital form. For each level, structural elements, objects and subjects are described, which in continuous interaction with each other ensure the existence of a multi-level protected cybernetic space.

Keywords: cybersecurity, cyber threats, digital information space, protected cyberspace, information security, open systems interconnection model, digital identity, digital border, BPMN 2.0

Введение. В условиях современного развития информационных цифровых сред в области информационной безопасности и защиты информации происходят трансформация и расширение определений и понятий, являющихся основополагающими в этой области. Информация, информационная среда, в которой она циркулирует, сформированное ими информационное пространство (ИПр), а впоследствии и единое информационное пространство переходят в цифровой вид. Стихийно развивающиеся цифровые процессы порождают большое количество сложных и мало связанных между собой цифровых систем: данные массово переводятся в цифровой вид и сливаются в единые базы данных без обеспечения необходимого уровня контроля и категоризации.

Такая ситуация приводит необходимости углубленного анализа ситуации и необходимости разработки системы мер по обеспечению необходимого уровня информационной безопасности (ИБ). Однако эти вопросы в существующей литературе рассмотрены недостаточно комплексно. Поэтому целью данной работы было устранение указанного недостатка.

Общая характеристика предметной области исследований. Процесс цифровизации предполагает, что к данным может обращаться любой процесс или система. Поэтому подтверждение и поддержка легитимности доступа и защиты современной архитектурой ИБ, с классическим подходом к реализации системы защиты, становится все более затруднительной.

На первое место выходят угрозы ИБ, структура, форма и методы реализации которых сосредоточены в той части ИПр, где данные передаются, обрабатываются и хранятся в цифровом виде. Появление новейших информационных технологий и систем, развитие и расширение функций социальных сетей, внедрение в социальные сети различных сервисов и их алгоритмизация формируют не просто отдельную систему внутри ИПр, а отдельную область – киберпространство (КПр). Так как КПр – это частный случай ИПр, то все характеристики последнего применимы и к КПр. Однако ввиду долгосрочного развития КПр, как неконтролируемой самостоятельно развивающейся среды, применить характеристики киберпространства к ИПр нельзя.

Аналогично информационному пространству, для информации в КПр существуют угрозы ИБ, которые могут нарушать доступность, целостность и конфиденциальность данных. Такие угрозы в терминологии, соответствующей рассматриваемой теме, называются киберугрозами. Согласно экспертным оценкам, прогнозы по преобладающим сферам киберугроз на начало 2020 г. [5, 14] представлены на рисунке 1.

Киберугрозы, представленные ниже, весьма разнообразны и по объекту воздействия, и по способам реализации. Однако все они направлены на КПр. Для использования средств предупреждения, выявления и устранения кибернетических угроз определено понятие «кибербезопасность».

Рисунок 1 – Классификация видов киберугроз на 2020 г.

Для противодействия киберугрозам необходимо четко представлять структуру и взаимосвязи компонентов киберпространства. Это позволит обеспечить необходимый уровень кибербезопасности каждого из компонент и кибернетического пространства в целом.

Управление субъектами киберпространства играет определяющую роль в возникновении, существовании и поддержке его основных свойств:

- многочисленность элементов;
- множество взаимных связей между ними;
- возможность применения специальных техник управления действиями этих элементов.

Указанные свойства определяют процессы развития киберугроз [4] и объективную необходимость внедрения средств обеспечения кибербезопасности.

Авторами в статье предложены определения, характеристики, границы и многоуровневая структурная модель КПр, где для каждого уровня определен процесс обеспечения кибербезопасности.

Определение понятий «киберпространство» и «кибербезопасность». Понятие киберпространства достаточно многогранно с точки зрения сформулированных и предложенных определений в различных областях научных исследований. В научном дискурсе насчитывается порядка 28-ми определений этого понятия. В основном различие или сходство определений обусловлено точкой зрения авторов и «плоскостью» рассмотрения проблемной области. Основные понятия могут быть представлены в виде следующих формулировок, основанных на [10, 11, 12, 13, 16], а также аналогичных по содержанию определениях в [9].

1. Киберпространство – это совокупность взаимосвязанных компонентов в виде информационных процессов или явлений со специфическими пространственно-временными характеристиками с носителем в форме компьютера или другого электронного устройства на базе информационно-телекоммуникационных сетей, преимущественно интернета, взаимодействие которых между собой оценивается соответствующей метрикой.

2. Киберпространство – среда, включающая три составляющих [1, 2, 4]:

2.1. Информационный аспект – статическая и динамическая информация в цифровом виде.

2.2. Физический аспект – аппаратно-программная и техническая инфраструктуры, обеспечивающие сбор, обработку, хранение и передачу данных.

2.3. Социальный аспект – информационное взаимодействие субъектов с использованием информации и инфраструктуры.

Международный стандарт ISO/IEC 27032:2012 [19] дает следующее определение понятию КПр.

Киберпространство (кибернетическое пространство) – комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в интернете посредством соответствующих сетевых и коммуникационных технологий.

Так как понятие «киберпространство» до конца юридически и законодательно не определено, то в рамках текущего исследования и в дальнейшем мы будем использовать следующее обобщенное определение.

Киберпространство – это управляемое масштабируемое цифровое пространство, сформированное в результате непрерывного взаимодействия субъектов физического, информационного и социального пространств в отношении сбора, обработки, хранения и передачи данных в цифровом виде.

Понятие киберугрозы пока не определено на уровне официальных документов или стандартов. Поэтому возьмем за основу экспертное мнение от специалистов по информационной безопасности [15].

Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей.

По аналогии с безопасностью информации для информационного пространства, для киберпространства вводится определение «кибербезопасность».

Международный стандарт ISO/IEC 27032:2012 [19] дает следующее определение этого термина.

Кибербезопасность – свойство защищенности активов от угроз конфиденциальности, целостности, доступности в киберпространстве.

При этом есть более широкое определение этого понятия, а также понятий доступности, целостности, конфиденциальности согласно ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 [17].

Кибербезопасность – действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности (целостности, доступности и конфиденциальности).

В дальнейшем исследовании будем использовать определение кибербезопасности, представленное в ГОСТе, так как, по нашему мнению, оно дает наиболее полное и развернутое описание этого понятия.

Характеристики и границы киберпространства. Как и любое пространство, КПр должно иметь границы и определенные характеристики (показатели), позволяющие судить о его состоянии. Развернутая сетевая структура и множество взаимосвязей объектов КПр позволяют функционировать различным уровням взаимодействия, где возникают точки соприкосновения виртуальных коммуникаций. Они выражаются процедурами трансляции образов, текстовой и символьной передачей. При этом достигаются такие требования к комфортному участию, как мобильность, компактность, анонимность, распределенность ресурсов и связей [2].

Область киберпространства можно определить границами множества цифровых систем и устройств, которые работают с данными в рамках его инфраструктуры. При этом важной составляющей такой работы является обеспечение конфиденциальности, целостности и доступности информации в пределах КПр.

Устойчивые и безопасные связи обеспечивают успешное и непрерывное существование КПр; способность передавать, получать и обрабатывать информацию с сохранением ее семантических качеств и свойств. В то же время наличие механизмов управления формирует интеллектуальную основу поведения при дестабилизирующих воздействиях и угрозах на КПр.

С точки зрения национальной безопасности и суверенности государства отсутствие четко определенных границ КПр влечет серьезные угрозы. При этом возрастает вероятность проникновения типичных угроз нижнего уровня на верхний уровень функционирования элементов КПр. Таким образом, задавая четкую конфигурацию, мы можем выставить определенные виртуальные границы устройств, систем, уровней. Это в конечном итоге позволит говорить о совпадении физических, административных и цифровых границ КПр [1, 3, 4].

По нашему мнению, для киберпространства спектр основных характеристик включает в себя оценки показателей безопасности, доступности, непрерывности, масштабируемости, мобильности и разнородности.

Вышеописанные подходы к определению границ КПр опираются на инфраструктурные и технологические средства, тогда как непосредственное взаимодействие с ними человека не учитывается. Если же учесть такое взаимодействие, то границы КПр будут шире, охватывать каждого отдельного человека – и как «источника», и как «получателя» информации в цифровом виде в течение времени взаимодействия с устройствами.

Структурная модель киберпространства. На данный момент не представляется возможным определить подробную структуру КПр с учетом всех его характеристик. В изученных нами структурных схемах киберпространства определение составляющих его элементов, как правило, имеет локальный характер, а структуризация проводится в целях решения общей задачи научного исследования. Проведем сравнение и обобщение определений для представленных в литературе структур:

1. Структура киберпространства представляет собой абстрактную кибернетическую систему, состоящую из множества взаимосвязанных объектов, называемых элементами системы, способных воспринимать, хранить и перерабатывать информацию, а также обмениваться информацией [1].

2. Киберпространство – гибкий и подвижный гибрид физического и социального пространства, зависящий от функционирования информационного-коммуникационных сетей. Киберпространство является местом или пространством, которое контролирует существование и работу взаимосвязанных сетей компьютеров [2].

3. Структура киберпространства является многоуровневой, построенной на основе модели ISO/OSI или TCP/IP [4] (рис. 2).

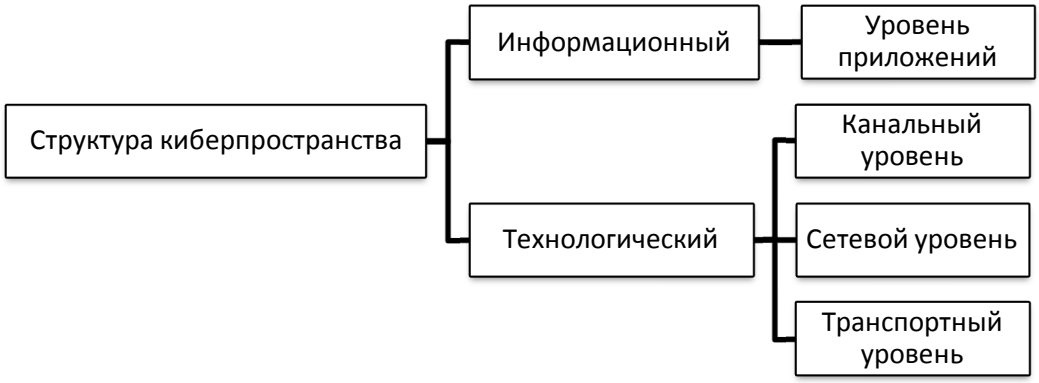


Рисунок 2 – Структура киберпространства по [4]

4. Структура социокиберфизической системы состоит из 4-х уровней [6] (рис. 3).

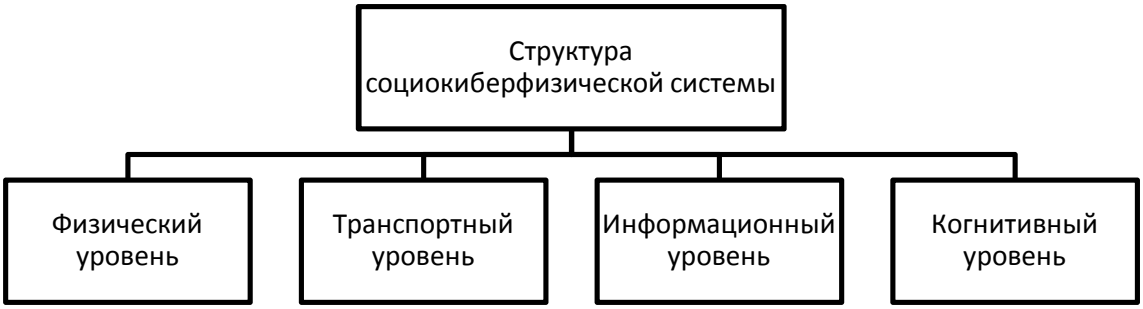


Рисунок 3 – Структура социокиберфизической системы [6]

Данная структура социокиберфизической системы, как и сама система, не ассоциируется автором с киберпространством. При этом функции и задачи этих структур достаточно схожи. Поэтому мы считаем возможным добавить указанную структуру к остальным.

Представленные структурные схемы КПр отражают его суть. Однако они недостаточно подробно определяют его для целей дальнейших исследований. Ввиду этого предложим модифицированную структуру КПр и структурную модель, построенную в нотации BPMN 2.0. Исходя из сформулированного определения, киберпространство охватывает три области: физическое, информационное и социальное пространства (рис. 4, 5).

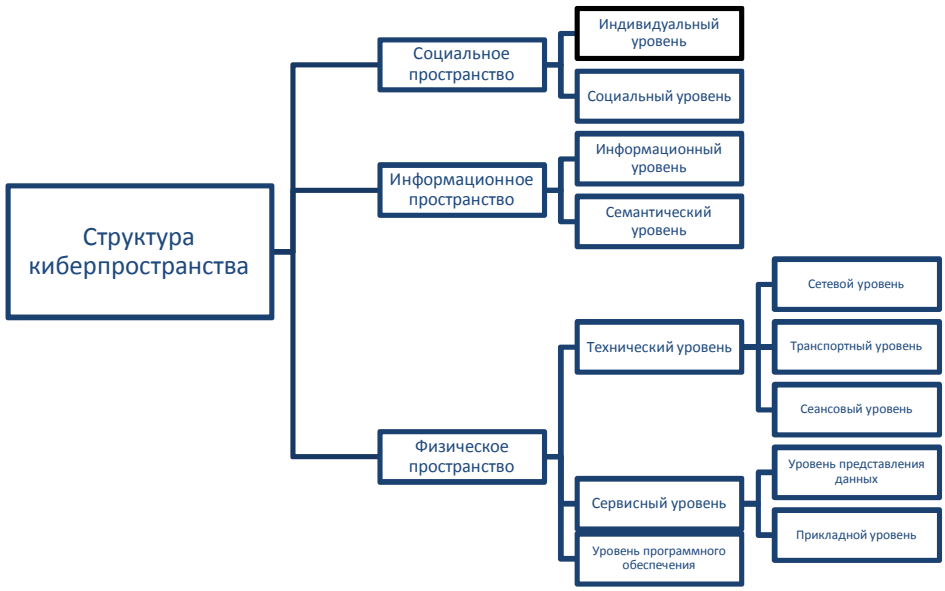


Рисунок 4 – Модифицированная иерархическая структура киберпространства

Рисунок 5 – Структурная модель киберпространства в нотации BPMN 2.0

Физическое пространство можно определить через программно-аппаратную инфраструктуру взаимосвязи открытых систем (ВОС), регламентированную ГОСТ Р ИСО/МЭК 7498-1-99 [18]. Подобный подход с использованием модели ISO/OSI, схожей по составу с ВОС, был представлен одним из исследователей ранее [4]. Однако для описания роли физического пространства как канала доступа к КПр, определим дополнительный уровень программного обеспечения, который формирует возможности взаимодействия с другими элементами.

Технический уровень позволяет определить субъект физического пространства как *устройство*, а объект – как *пакет данных*.

Сервисный уровень позволяет определить субъект физического пространства как *интерфейс*, а объект – как *протокол*.

Уровень программного обеспечения позволяет определить субъект физического пространства как *приложение*, а объект – как *цифровые данные*.

Информационное пространство включает обобщенный информационный уровень и семантический уровень. Информационный уровень представлен в структуре социокиберфизической системы [6, 7, 8] и в структуре КПр [4].

Информационный уровень позволяет определить субъект информационного пространства как *базу данных*, а объект – как *блок данных*.

Семантический уровень позволяет определить субъект информационного пространства как *базу знаний*, а объект – как *семантический блок*.

Социальное пространство включает персональный уровень и социальный уровень.

Индивидуальный (персональный) уровень позволяет определить субъект социального пространства как *человека*, а объект – как *сообщение*.

Социальный уровень позволяет определить субъект социального пространства как *социальную группу*, а объект – как *сообщение*.

Представленная структурная модель позволяет перейти к определению контроля целостности, конфиденциальности и доступности информации для каждого уровня, процесс обеспечения безопасности которых формирует понятие защищенного киберпространства.

Структурная модель защищенного киберпространства. Опираясь на предложенную структурную модель, добавим уровень кибербезопасности, в котором организован непрерывный процесс обеспечения состояния защищенности информации в КПр (рис. 6).

В рамках непрерывного процесса обеспечения кибербезопасности опишем процессы для каждого из структурных элементов.

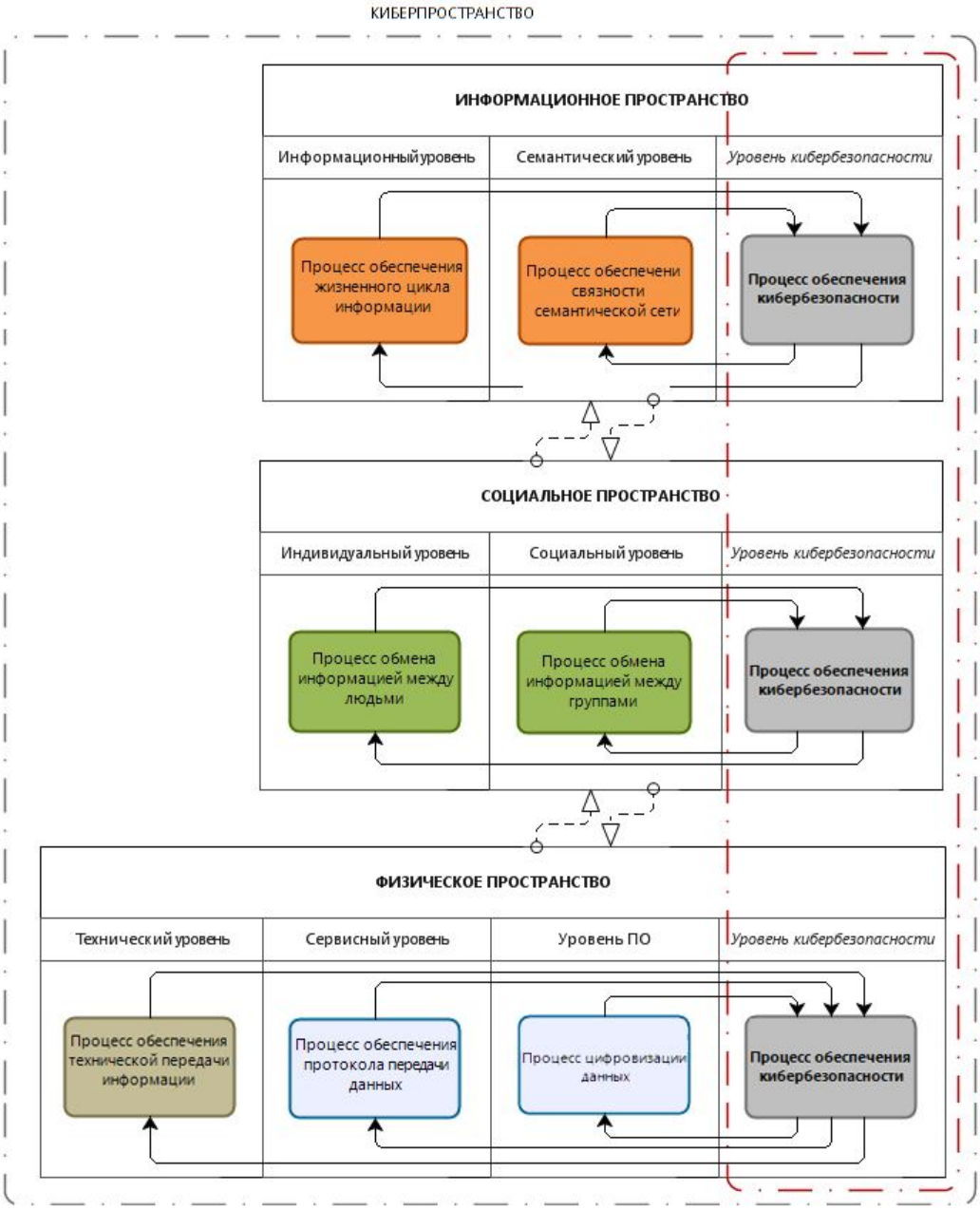


Рисунок 6 – Структурная модель защищенного киберпространства в нотации BPMN 2.0

Социальное пространство реализует информационный обмен на индивидуальном и социальном уровнях, а также между ними, формируя *процесс обмена информацией*. При этом на *индивидуальном уровне* происходит общение между людьми, а на *социальном уровне* – между *социальными группами*.

Физическое пространство объединяет три уровня: на *техническом уровне* реализуется *процесс технической передачи информации*, на *сервисном уровне – процесс обеспечения протокола передачи данных*, а на *уровне программного обеспечения – процесс цифровизации данных*. При этом обмен данными происходит при участии всех указанных уровней.

Информационное пространство реализует этапы обработки информации на информационном и семантическом уровнях, формируя при этом *процесс обеспечения жизненного цикла информации* на *информационном уровне* и *процесс обеспечения связности семантической сети* на *семантическом уровне*.

Для каждого из пространств определен уровень кибербезопасности. Составляющие процесса обеспечения кибербезопасности интегрируются в существующие процессы на этом уровне, поддерживая на необходимом уровне конфиденциальность, целостность и доступность информации.

Выводы. В статье дано авторское определение понятия киберпространства, основанное на опубликованных результатах исследований по этой теме. Также выбрано определение кибербезопасности, что обеспечивает возможности формулирования подходов, направленных на предупреждение, выявление и устранение кибернетических угроз.

Для определения стратегии противодействия киберугрозам представлены характеристики, определены границы и сформирована структура защищенного многоуровневого киберпространства.

Характеристиками КПр являются безопасность, доступность, непрерывность, масштабируемость, мобильность и разнородность.

Границы КПр вариативны и охватывают каждого отдельного человека как «источника», так и «получателя» информации в цифровом виде в течение времени взаимодействия с устройствами.

Обеспечение необходимого уровня кибербезопасности и формирование защищенного многоуровневого КПр представлено в виде многоуровневой модели с использованием нотации BPMN 2.0.

Структурная модель защищенного КПр включает в себя социальное, физическое и информационное пространства. Для каждого из них неотъемлемым атрибутом является кибербезопасность.

Библиографический список

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

2. Добринская Д. Е. Киберпространство: территория современной жизни / Д. Е. Добринская // Вестник Московского университета. Серия 18. Социология и политология. – 2018. – Т. 24, № 1. – С. 52–70.

3. Мещеряков Р. В. Информационные иерархические системы / Р. В. Мещеряков // Известия Томского политехнического университета. Инжиниринг георесурсов. – 2009. – Т. 314, № 5. – С. 151–154.

4. Пилюгин П. Л. Проблемы определения границ в информационном пространстве / П. Л. Пилюгин // T-Comm – Телекоммуникации и транспорт. – 2017. – Т. 11, № 8. – С. 37–44.

5. Прогноз развития киберугроз и средств защиты информации 2020. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast#part21, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.03.2020).

6. Смирнов А. В., Теоретические основы построения социокиберфизических систем / А. В. Смирнов, В. В. Безручко, О. О. Басов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2019. – Т. 46, № 3. – С. 532–539.

7. Смирнов А. В. Приобретение знаний в социокиберфизических системах в процессе информационного взаимодействия ресурсов / А. В. Смирнов, Т. В. Левашова // Информационно-управляющие системы. – 2017. – № 6. – С. 113–122.

8. Смирнов А. В. Модели поддержки принятия решений в социокиберфизических системах / А. В. Смирнов, Т. В. Левашова // Информационно-управляющие системы. – 2019. – № 3. – С. 55–70.

9. Тонконогов А. В. Кибернетическое общество как реальность XXI века / А. В. Тонконогов // Закон и право. – 2018. –№ 9. – С. 23–26.

10. Хаханов В. И. Развитие киберпространства и информационная безопасность / В. И. Хаханов, С. В. Чумаченко, Е. И. Литвинова, А. С. Мищенко // Радіоелектроніка, інформатика, управління. – 2013. – № 1. – С. 151–157.

11. Хаханов В. И. Метрика алгебры векторной логики для кибернетического пространства / В. И. Хаханов, А. С. Мищенко, В. В. Вареца // Радиоэлектроника и информатика. – 2010. – № 3. – С. 39–42.

12. Хаханов В. И. Эволюция кибернетического пространства / В. И. Хаханов, А. В. Хаханова, В. В. Закарян // Радиоэлектроника и информатика. – 2010. – № 2. – С. 61–67.

13. Хаханов В. И. Инфраструктура диагностирования вредоносных программ в индивидуальном кибернетическом пространстве / В. И. Хаханов, С. В. Чумаченко, А. С. Мищенко, А. В. Зацарный, Ю. В. Хаханова // Автоматизированные системы управления и приборы автоматики. – 2010. – № 153. – С. 19–32.

14. Positive technologies. Кибербезопасность 2019–2020: тенденции и прогнозы, Москва, 2019. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2019-2020-rus.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 29.03.2020).

15. Technologies P. Киберугроза. 2020. – Режим доступа: https://www.securitylab.ru/news /tags/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D0%B0/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.04.2020).

16. Yves T. Актуальные проблемы анализа киберпространства / T. Yves, С. В. Чумаченко, В. И. Хаханов // Автоматизированные системы управления и приборы автоматики. – 2011. – № 154. – С. 59–75.

17. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Ч. 1-1. Терминология, концептуальные положения и модели. – Москва : Стандартинформ, 2014. – 81 с.

18. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 1. Базовая модель. – Москва : Госстандарт России, 2006. – 58 с.

19. ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity. – Germany : JTC 1/SC 27, 2012. – 58 p.

References

1. Bezkorovaynyy M. M., Tatuzov A. L. Kiberbezopasnost I podkhody k opredeleniyu ponyatiya [Cybersecurity and approaches to defining a concept]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2014, no. 1 (2), pp. 22–27.

2. Dobrinskaya D. E. Kiberprostranstvo: territoriya sovremennoy zhizni [Cyberspace: the territory of modern life]. *Vestnik Moskovskogo universiteta. Seriya 18. Sotsiologiya i politologiya* [Moscow University Bulletin. Series 18. Sociology and Political Science], 2018, vol. 24, no. 1, pp. 52–70.

3. Meshcheryakov R. V. Informatsionnye ierarhicheskie sistemy [Information hierarchical systems]. *Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesursov* [Bulletin of the Tomsk Polytechnic University. Georesource engineering], 2009, vol. 314, no. 5, pp. 151–154.

4. Pilyugin P. L. Problemy opredeleniya granits v informatsionnom prostranstve [Problems of defining boundaries in the information space]. *T-Comm – Telekommunikatsii i Transport* [T-Comm – Telecommunications and Transport], 2017, vol. 11, no. 8, pp. 37–44.

5. *Prognoz razvitiya kiberugroz i sredstv zashchity informatsii 2020* [Cyber Threats and Information Security Forecast 2020], 2019. Available at: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast#part21 (accessed 26.03.2020)

6. Smirnov A. V., Bezruchko V. V., Basov O. O. Teoreticheskiye osnovy postroyeniya sotsiokiberfizicheskikh system [Theoretical foundations of building sociocyberphysical systems]. Nauchnyye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika [Scientific Bulletin of Belgorod State University. Series: Economics. Informatics], 2019, vol. 46, no. 3, pp. 532–539.

7. Smirnov A. V., Levashova T. V. Priobreteniye znaniy v sotsiokiberfizicheskikh sistemakh v protsesse informatsionnogo vzaimodeystviya resursov [Acquisition of knowledge in sociocyberphysical systems in the process of information interaction of resources]. *Informatsionno-upravlyayushchiye sistemy* [Information and Control Systems], 2017, no. 6, pp. 113–122.

8. Smirnov A. V., Levashova T. V. Modeli podderzhki prinyatiya resheniy v sotsiokiberfizicheskikh sistemakh [Decision support models in sociocyberphysical systems]. *Informatsionno-upravlyayushchiye sistemy* [Information and Control Systems], 2019, no. 3, pp. 55–70.

9. Tonkonogov A. V. Kiberneticheskoye obshchestvo kak realnost XXI veka [Cybernetic society as a reality of the XXI century]. *Zakon i pravo* [Law and Legislation], 2018, no. 9, pp. 23–26.

10. Khakhanov V. I., Chumachenko S. V., Litvinova Ye. I., Mishchenko A. S. Razvitiye kiberprostranstva i informatsionnaya bezopasnost [Cyberspace development and information security]. *Radíoelektronika, ínformatika, upravlínnya* [Radioelektronika, Informatics, Management], 2013, no. 1, pp. 151–157.

11. Khakhanov V. I., Mishchenko A. S., Varetsa V. V. Metrika algebry vektornoy logiki dlya kiberneticheskogo prostranstva [Metric of the algebra of vector logic for cybernetic space]. *Radioelektronika i informatika* [Radioelectronics and Informatics], 2010, no. 3, pp. 39–42.

12. Khakhanov V. I., Khakhanova A. V., Zakaryan V. V. Evolyutsiya kiberneticheskogo prostranstva [Evolution of cybernetic space]. *Radioelektronika i informatika* [Radioelectronics and informatics], 2010, no. 2, pp. 61–67.

13. Khakhanov V. I., Chumachenko S. V., Mishchenko A. S., Zatsarnyy A. V., Khakhanova Yu. V. Infrastruktura diagnostirovaniya vredonosnykh programm v individualnom kiberneticheskom prostranstve [Infrastructure for diagnosing malware in the individual cyber space]. *Avtomatizirovannyye sistemy upravleniya i pribory avtomatiki* [Automated control systems and automation devices], 2010, no. 153, pp. 19–32.

14. *Positive technologies. Kiberbezopasnost 2019–2020: tendentsii i prognozy* [Cybersecurity 2019–2020: Trends and Forecasts], 2019. Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics /cybersecurity-2019-2020-rus.pdf (accessed 29.03.2020).

15. Technologies P. *Kiberugroza* [Cyber threat], 2020. Available at: https://www.securitylab.ru/news/tags /%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D0%B0/ (accessed 15.04.2020)

16. Yves T., Chumachenko S. V., Khakhanov V. I. Aktualnyye problemy analiza kiberprostranstva [Actual problems of cyberspace analysis]. *Avtomatizirovannyye sistemy upravleniya i pribory avtomatiki* [Automated control systems and automation devices], 2011, no. 154, pp. 59–75.

17. *GOST R 56205-2014 IEC/TS 62443-1-1:2009. Seti kommunikatsionnyye promyshlennyye. Zashchishchennost (kiberbezopasnost) seti i sistemy. Chast 1-1. Terminologiya, kontseptualnyye polozheniya i modeli* [GOST R 56205-2014 IEC / TS 62443-1-1: 2009 Industrial communication networks. Security (cybersecurity) of the network and system. Part 1-1. Terminology, conceptual provisions and models.]. Moscow, Standartinform Publ., 2014. 81 p.

18. *GOST R ISO/MEK 7498-1-99. Informatsionnaya tekhnologiya (IT). Vzaimosvyaz otkrytykh sistem. Bazovaya etalonnaya model. Chast 1. Bazovaya model* [GOST R ISO / IEC 7498-1-99. Information technology (IT). Interconnection of open systems. Basic reference model. Part 1. Basic model]. Moscow, Gosstandart of Russia, 2006. 58 p.

19. *ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity.* Germany, JTC 1/SC 27, 2012. 58 p.