УДК: 004.056
doi: 10.26583/bit.2024.1.10

Александр И. Толстой
*Национальный исследовательский ядерный университет «МИФИ»*
*Каширское ш., 31, Москва, 115409, Россия*
*e-mail: AITolstoj@mephi.ru, http://orcid.org/0000-0001-9265-1510*

# ТАКСОНОМИЯ ПОНЯТИЙ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

*Аннотация.* В статье на базе принятой ранее систематики понятий предложена классификация понятий, имеющая отношение к кибербезопасности (КБ) объектов и обладающая на данный момент максимальной однозначностью соответствия терминов, обозначающими эти понятия, и самими понятиями. При построении классификации применены основы теории таксономии (систематики), обоснован вывод, что рассмотренные структуры систем понятия будут иерархичными (основной принцип таксономии) при определенных условиях (например, при использовании только понятий, которые относятся к категориям предмета (объекта), процесса, или свойства). Рассмотренный подход позволил сформировать группу терминов, непосредственно связанных с понятиями из предлагаемой классификации. Показано, что совокупность введенных терминов можно рассматривать как терминосистему, относящуюся к области КБ объекта. Предложенные термины и их определения отличаются системностью в отношении самих терминов (определений) и соответствующих понятий, а также имеют универсальный характер применения, что позволяет их использование для практически любых объектов КБ, имеющих отношение к информации (например, информационные и автоматизированные системы, системы информатизации, социотехнические системы, киберфизические системы и информация как объект). Результаты работы имеют практическую значимость для образовательной области при формировании у обучающихся современной, методически обоснованной, понятийной базы.
*Ключевые слова: таксономия, понятие, термин, определение, безопасность, опасность, объект, кибербезопасность, состояние защищенности, актив, свойства кибербезопасности, угроза, ущерб, риск, обеспечение кибербезопасности.*
*Для цитирования: ТОЛСТОЙ, Александр И. ТАКСОНОМИЯ ПОНЯТИЙ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 158–175, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1615. DOI: http://dx.doi.org/10.26583/bit.2024.1.10.*

Alexander I. Tolstoy
*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),*
*Kashirskoe sh., 31 Moscow, 115409, Russia*
*e-mail: AITolstoj@mephi.ru, http://orcid.org/0000-0001-9265-1510*

## Cybersecurity concepts’ taxonomy

*Abstract.* Based on the previously accepted taxonomy of concepts, a classification of concepts is proposed that is related to cybersecurity (CS) of objects and currently has the maximum unambiguous correspondence between the terms denoting these concepts and the concepts themselves. When constructing the classification, an attempt was made to apply the fundamentals of the taxonomy theory (systematics), the results of which led to the conclusion that the considered structures of concept systems will be hierarchical (the basic principle of taxonomy) under certain conditions (for example, when using only concepts that relate to the categories of the subject (object)), process, or property). The approach considered made it possible to form a group of terms directly related to the concepts from the proposed classification. This set can be considered as a terminology system related to the object’s CS. The proposed terms and their definitions do not contradict similar ones being used, but are distinguished by

consistency in relation to the terms (definitions) themselves and corresponding concepts, and also have a universal application, which allows their use for almost any CS objects related to information (for example, information and automated systems, informatization systems, sociotechnical systems, cyber-physical systems and information as an object). The results obtained also have practical significance for education in the formation of a modern, methodologically sound conceptual base of students.
*Keywords: taxonomy, concept, term, definition, security, danger, object, cybersecurity, state of security, asset, cybersecurity properties, threat, damage, risk.*
*For citation: TOLSTOY, Alexander I. Cybersecurity concepts' taxonomy. IT Security (Russia), [S.l.], v. 31, no. 1, p. 158–175, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1615. DOI: http://dx.doi.org/10.26583/bit.2024.1.10.*

## Введение

Современная область профессиональной деятельности, относящейся к информационной безопасности (ИБ), обладает обширной русскоязычной терминологической базой [1], которая создавалась при существенном влиянии англоязычных терминов. При этом можно констатировать факт, что эта база в основном отражает современную систему понятий, относящихся к данной предметной области [2].

Следует отметить, что, начиная с конца 90-х годов прошлого века, в англоязычной научной и образовательной среде началось активное использование термина «кибербезопасность» (КБ) в таких областях, как информационная безопасность, безопасность систем связи, операционная безопасность, физическая и общественная (национальная) безопасность [3].

Ведущие зарубежные страны увидели в этом новую содержательную сущность в области национальной и международной безопасности [4].

Результатом является появление на международном и национальном уровне отдельных государств большого количества нормативных (стандарты) и правовых документов (например, стратегии КБ государств).

В РФ до 2016 г. термин «кибербезопасность» практически не встречался и не был принят. Только после включения технологии КБ в Перечень приоритетных технологический направлений ОПК РФ, утвержденный Правительством РФ (на основании Указа Президента РФ 20.07.2016 г. № 347), в стране наблюдается активность на уровне дискуссионного обсуждения проблематики, связанной с КБ на различных форумах, конференциях и в публикациях [4]. Причем больше всего внимание уделено анализу различных определений термина КБ [1, 4–6] и попыткам формулирования новых определений с учетом различных подходов [4, 5]. Например, можно найти варианты раскрытия термина и понятия КБ [4] через перевод определений с английского языка, через техническую трактовку понятия «киберпространство», через увязку с целями информационной безопасности, определенными в документе «Доктрина ИБ РФ»[1], через соотношение понятий ИБ и КБ. В практическом плане отсутствие единой понятийной базы в области КБ объясняет попытки применить определение термина КБ, взятого из международного стандарта ISO/IEC 27032[2], не имеющего аналога на национальном уровне, при исследовании угроз нарушения КБ для организаций инфраструктуры финансовых рынков [6]. Особенностью этого определения является утверждение, что область КБ является частью области ИБ. Еще одним примером практического решения – это разработка учебных планов подготовки профессионалов в области КБ в

[1]Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 05.12.2016 № 646.
[2]ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.

предположении, что понятия КБ и ИБ совпадают [7, 8, 9]. Имеются подходы, основанные на определения термина КБ, претендующие на уникальность области КБ [4, 5].

Фактически возникла ситуация, когда один и тот же термин имеет различные русскоязычные определения и отсутствуют результаты корректного соотношения терминов и понятий ИБ и КБ, учитывающих возможности существующей отечественной нормативной и методической базы в области ИБ. Эти факторы можно отнести к основным принципиальным причинам существования проблем развития КБ в России [4], что можно считать противоречием или фундаментальной проблемой, решение которой возможно только на системном уровне.

В данной работе приводятся результаты исследования, направленного на преодоление вышеобозначенного противоречия, на основе построения системы связанных понятий в области КБ, основанной на принципах систематики (таксономии). Следует отметить, что эту работу необходимо рассматривать, как развитие систематики понятий, примененной ранее для области ИБ [2]. Это позволило обосновано выбрать терминосистему области КБ, а также сформулировать систему определений этих терминов, не противоречащей принципах систематики (таксономии).

## 1. Основы систематики понятий

Формирование совокупности понятий в виде системы, определяющей границы определенной предметной области, позволяет определить место каждого понятия в системе и его взаимосвязь с другими понятиями, а также взаимосвязь данной системы с другими понятийными системами «Доктрина ИБ РФ»[3]

Анализ особенностей системы понятий в отношении, например, к такой предметной области как информационная безопасность позволил сделать следующие выводы [2]: систему понятий можно отнести к сложным системам; для описания такой системы трудно предложить единую классификацию понятий, входящих в систему; для полноты описания определенной предметной области, представляется целесообразным выделить в системе отдельные группы понятий, применить в пределах конкретной группы свою классификацию понятий и установить связи между такими группами.

Для построения системы понятий в области КБ предлагается использовать (аналогично [2]) таксономию (систематику) – теорию классификации и систематизации сложноорганизованных объектов [10–13]. При этом структура системы понятий определенной предметной области, построенная с учетом основного принципа таксономии (иерархичности) иметь вид, представленный на рис. 1 [2]. В такой структуре можно выделить отдельные понятия, находящихся на определенном уровне структуры системы (на рис. 1 показаны только четыре уровня: нулевой, первый, второй и третий). Элемент классификационной совокупности понятий определенного уровня структуры, связанный с понятием выше находящегося уровня, будем называть таксоном. Система понятий будет полностью таксономной, если ее структура будет иерархичной, т.е. будут отсутствовать связи между понятиями конкретного таксона подчинённого уровня, относящееся к одному уроню и будут отсутствовать связи между понятиями, принадлежащими разным таксонам.

В основу формирования таксономии (систематики) понятий положено соглашение о том, что означает такие сущности, как «понятие», «термин» и «определение термина», а

[3]Рекомендации по межгосударственной стандартизации РМГ 19-96 «Рекомендации по основным принципам и методам стандартизации терминологии»». Введены в действие непосредственно в качестве рекомендаций по стандартизации Российской Федерации с 1 июля 1998 г. (Постановлением Государственного комитета Российской Федерации по стандартизации, метрологии и сертификации от 21 апреля 1998 г. N 135).

также «категории понятий»[3]. Связующими звеньями между термином и понятием являются определение (описание) понятия и определение самого термина. С учетом этого можно утверждать, что для определенной области знаний (предметной области) существует свой понятийный аппарат и связанная с ним терминосистема. Причем, понятие, относящееся к определенной области знаний, формируется параллельно с формированием понимания у человека.

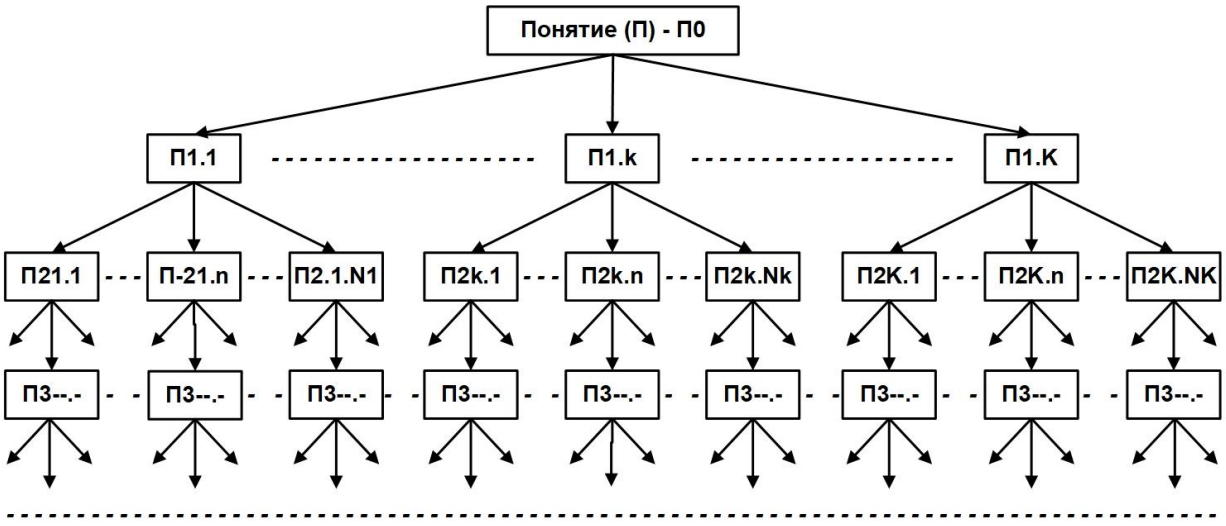


*Рис. 1. Структура системы понятий, состоящая из таксонов*

Следует также обратить внимание на требования к терминам[3], которые непосредственно согласуются с принципами таксономии [11]. Деривационная способность термина предполагает, что в определении конкретного термина могут использоваться термины, которые требуют своих определений. Соответственно в определениях терминов второго уровня будут использоваться свои термины со своими определениями и так далее. Главное, чтобы эти термины соответствовали единой терминосистеме определенной предметной области. Такая ситуация отвечает принципу иерархии, принятой в таксономии [11].

## 2. Формирование корневых таксонов системы понятий «безопасность» и «кибербезопасность»

Понятие, которому соответствует термин «кибербезопасность» («КБ») может быть отнесено к одному из видов понятия «безопасность» (Б) [2, 14, 15]: например: информационная безопасность (ИБ), экономическая Б, экологическая Б, национальная Б, промышленная Б, энергетическая Б, международная Б и т.д. Соответствующий таксон показан на рис. 2.

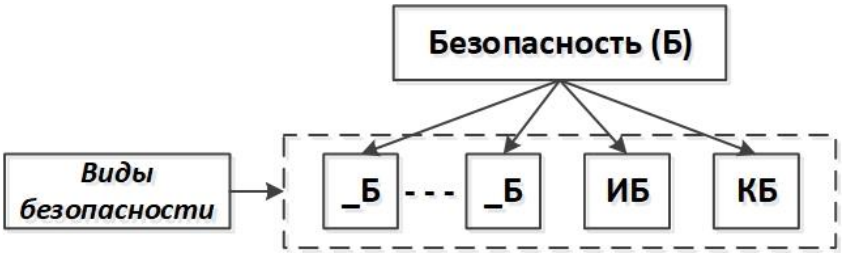


*Рис. 2. Корневой таксон понятия «безопасность»*

Определить понятие, которое представляет такой термин, на основе терминов, входящих в этот термин затруднено, особенно в случае терминов «КБ» и «ИБ» [2, 14, 15]. Если используется термин «КБ» (или «ИБ»), то всегда необходимо уточнять к какому понятию этот термин относится. Следствием этого является большое количество существующих определений этих терминов (и, соответственно, определений понятий), что нарушает одно из важнейших требований, предъявляемых к термину, представляющем конкретное понятие – однозначное соответствие между термином и понятием. С учетом этого, ранее было предложено [2] понятие «ИБ» отнести к понятиям в широком смысле. Далее будем также относить понятие «КБ» к понятиям в широком смысле.

Для того, чтобы повысить уровень согласованности между понятием (термином) и определением, будет ответ на вопрос: «КБ чего?». Принципиальным ответом будет, учитывая категории понятий[3]: «КБ предмета (объекта)». Это частично разрешает проблему наличия у одного и того же понятия (термина) большого количества разноплановых определений. Например, в монографии Д.П. Зегжды [5] представлен обширный перечень таких определений, которые относятся к понятию (термину) «КБ». Их можно отнести и к категории процесс (действие), и к категории свойство, и даже к такой сущности, которая не может быть однозначно сопоставлена с принятыми категориями понятий[3].

В данном месте зафиксируем вывод о том, что систематизацию понятий в области КБ можно осуществить только для понятия «КБ объекта», также, как и для понятия «ИБ объекта» [2].

На рис. 3 представлены корневые таксоны понятий «КБ» и «ИБ». Поскольку в них присутствуют понятия, представленные терминами «КБ объекта» и «ИБ объекта», имеющие определенный уровень согласованности с соответствующими понятиями, то такие понятия будем относить к понятиям в узком смысле [2].

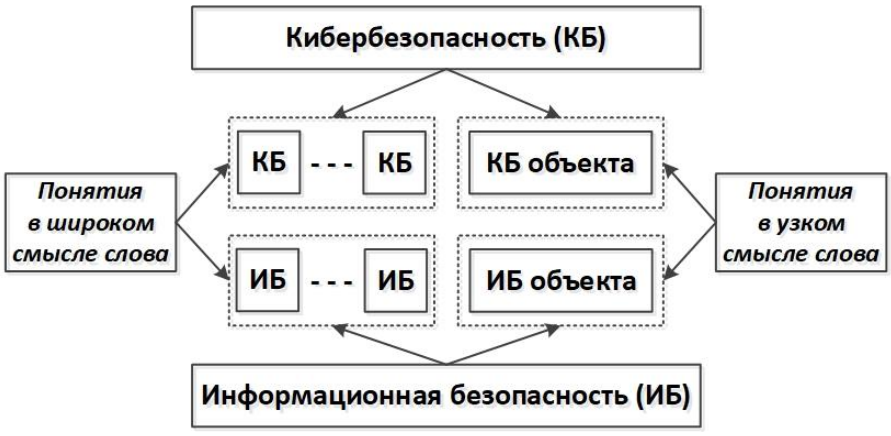


*Рис. 3. Корневые таксоны понятий «кибербезопасность» и «информационная безопасность»*

Следует отметить, что на уровне корневых таксонов, относящихся к систематике понятий «КБ» и «ИБ» различий нет.

## 3. Ключевые понятия, относящиеся к понятию «кибербезопасность объекта»

Ответ на вопрос «Кибербезопасность чего?» (объекта) не гарантирует высокий уровень выполнения требования однозначного соответствия между понятием и соответствующим ему термином «КБ объекта».

Для того, чтобы повысить уровень однозначности между понятием и соответствующим ему термином «КБ объекта» предлагается расширить ответ на вопрос «Безопасность (Б) чего?» (вопрос № 1) и дополнительно ответить на следующие вопросы: «Что собой представляет объект в понятии «КБ объекта?» (2), «Безопасность (Б) от чего?» (3), «Безопасность (Б) где?» (4). При этом воспользуемся опытом ответа на подобные вопросы в отношении понятия «ИБ объекта» [2]. На рис. 4 представлены ответы на эти вопросы.


*Рис. 4. Структура вопросов и ответов, уточняющих особенности понятия «КБ объект»*

Развернутый ответ на первый вопрос предполагает обратить внимание на те части объекта КБ, которые имеют заметную ценность для организации, частью которой является этот объект. Такой частью объекта является его актив (ГОСТ Р ИСО/МЭК 27000-2021[4]). При этом понятие, которое представляет термин «актив объекта КБ», относится к категории «предмет».

Активы объекта рекомендуется (ГОСТ Р ИСО/МЭК 27003-2021[5]) разделить на основные (основные процессы организации и информация, относящаяся к этим процессам) и вспомогательные (например, аппаратное и программное обеспечение, вспомогательные процессы, инфраструктура организации).

В случае КБ объекта перечень активов будет аналогичным перечню активов объекта ИБ [2] со следующими уточнениями. Во-первых, к активам может быть отнесен сам объект КБ. Во-вторых, разделение на основные и вспомогательные активы может быть иным. Чаще всего, к основным активам относят сам объект КБ, основные процессы объекта и связанные с ними основные процессы организации, аппаратное и программное обеспечение (активы, относящиеся к среде обработки информационных активов), коммуникационное оборудование, конечные устройства и сетевые коммуникации. Причем информация может быть и не отнесена к основным активам. В основе такого разделения

[4]ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
[5]ГОСТ Р ИСО/МЭК 27003-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

лежит особенность объекта КБ и цели, которые должны быть достигнуты в отношении КБ объекта [5].

При ответе на второй вопрос необходимо учесть понятие, определяемое термином «кибер» (сокращение от «кибернетический», «кибернетика») и непосредственно определяющий особенности объекта КБ (киберобъекта или кибернетического объекта).

Академик Глушков В.М. дал классическое определение термина «кибернетика» (от греч. κυβερνητική – «искусство управления») – это наука об общих закономерностях получения, хранения, передачи и преобразования информации в сложных управляющих системах (не только технических, а и любых биологических, административных и социальных системах) [16].

Если ориентироваться на это определение, то объект КБ будет иметь отношение к обработке (получению, хранению, передаче и преобразованию) информации и к различным аспектам управления. В практическом плане такие объекты можно назвать информационными объектами, использующими для обработки информации определенные информационные технологии (ИТ).

Сравнение с ответами на второй в отношении понятия «ИБ объекта» (рис. 4) показывает с общей позиции похожесть объектов КБ и ИБ. Однако рассмотрение особенностей практического использования этих объектов выявляет и явные различия. Во-первых, аспекты управления, относящиеся к КБ объекта, будут существенно шире, чем аналогичные для ИБ объекта. Во-вторых, объекты КБ, как правило, реализуют ИТ, относящиеся к сетевым технологиям и к интернету, а объект ИБ может использовать любые технологии обработки информации (включая, например, и использование документов в «бумажном» виде или при передаче информации в виде различных сигналов).

Первое, что можно уверено утверждать при ответе на третий вопрос, это то, что безопасность объекта – это ситуация, когда отсутствует опасность [14] по отношению к этому объекту. Важным является определить понятие (термин) «опасность» как источник потенциального вреда (ГОСТ Р 51897-2021[6]) или источник деструктивного воздействия на объект КБ (или объект ИБ). На рис. 5 показана типовая схема противоборства заинтересованных сторон, относящихся к области КБ – объект (субъект КБ, источник потенциального вреда, опасность), который реализует деструктивное воздействие на активы объекта КБ, стремящегося сохранить свою безопасность (объект КБ).

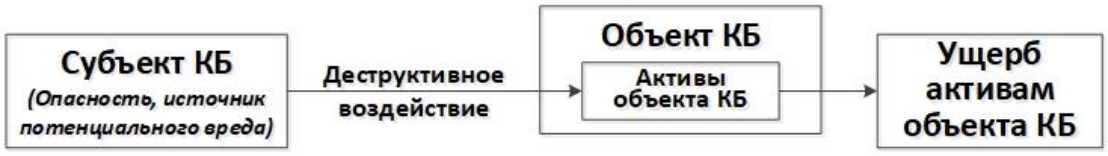


*Рис. 5. Схема противоборства объекта и субъекта КБ*

Было замечено [5], что в отличии от целей обеспечения ИБ (сохранение данных, сведений, знаний) целью обеспечения КБ является обеспечить стабильность функционирования объектов в условиях целенаправленного разрушающего воздействия.

Таким образом, опасность как источник деструктивного воздействия (субъект КБ) стремится нанести разрушающий ущерб активам объекта КБ или объекту КБ в целом и всей организации, если объект является ее частью. Поэтому деструктивное воздействие опасности на объект КБ будем связывать с целенаправленной кибератакой, наносящей

[6]ГОСТ Р ГОСТ Р 51897-2021 Менеджмент риска. Термины и определения.

ущерб активам объекта КБ. Причем понятие (термин) «ущерб» имеет определенную специфику в отношении понятия (термина) «актив».

Во-первых, вид ущерба непосредственно связаны с изменением определенных свойств (характеристик, параметров) актива. Такими свойствами актива объекта ИБ можно считать так называемые свойства ИБ: доступность, целостность, конфиденциальность, а также неоказуемость, достоверность подлинность (аутентичность) и подотчетность (ГОСТ Р ИСО/МЭК 13335-1-2006[7]). Для активов объекта КБ определим следующие свойства КБ: целостность, доступность, возможно конфиденциальность (когда информация отнесена к основным активам объекта КБ) и устойчивость (киберустойчивость).

Последнее свойство КБ является важным, когда к основным активам объекта КБ относят сам объект КБ. При этом в качестве внутреннего свойства такого актива определяют факторы устойчивости, поддержание которых в допустимых пределах обеспечивает объекту КБ состояние устойчивости, получившее название киберустойчивости[2] [17]. Такой подход дает существенные отличительные признаки области КБ от области ИБ [5].

При этом становится также обоснованным утверждение, что КБ объекта определяется состоянием защищенности активов объекта КБ, при котором деструктивное воздействие опасностей на этот объект не приводит к такому изменению свойств активов объекта КБ, которое можно признать недопустимым ущербом.

Таким образом, при систематике понятий в области КБ необходимо рассматривать понятия, относящиеся к категории «предмет» («объект») и к категории «свойство».

Ответ на четвертый вопрос: с киберпространством[2]. Анализ различных определений термина «киберпространство» [5, 17] показал, что киберпространство может определяться и как взаимозависимая сеть ИТ-структур, и как интерактивная область, образованная цифровыми сетями, и как электронная сфера деятельности, и как виртуальное пространство, и как составная среда, образованная за счет взаимодействия людей, программных средств и сервисов через интернет.

Пространство не может быть и сферой, и средой. В данном случае необходимо признать, что понятие «киберпространство» требует уточнения.

Из Толкового словаря русского языка[8]:

*Сфера* – это область, пределы распространения чего-нибудь (например, сфера деятельности, сфера влияния).

*Пространство* – это одна из форм (наряду со временем) существования бесконечно развивающейся материи, характеризующаяся протяженностью и объемом.

*Среда* – это вещество, заполняющее пространство, или окружение, совокупность природных условий, в которых протекает деятельность человеческого общества.

Если взять это за основу, то можно определить понятия «пространство КБ (киберпространство)», «среда КБ (киберсреда)» и «сфера КБ (киберсфера)» следующим образом (рис.6,а):

***Киберпространство*** *— это форма существования объектов КБ и субъектов КБ, характеризующаяся координатами взаимного расположения.*

[7]ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

[8]Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. URL: http://ozhegov.info/slovar/ (дата обращения: 24.12.2023).

***Киберсреда*** *– это заполнение киберпространства, в котором осуществляется взаимодействие объектов КБ и субъектов КБ.*

***Сфера кибербезопасности (Киберсфера)*** *– это совокупность киберпространства и киберсреды.*

Эти понятия будут относиться к категории «предмет (объект)».

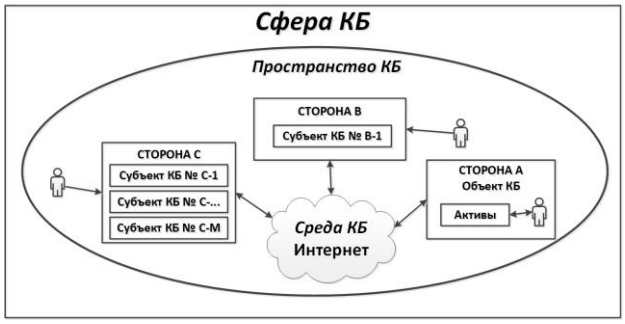


*Рис. 6,а. Структура сферы КБ*

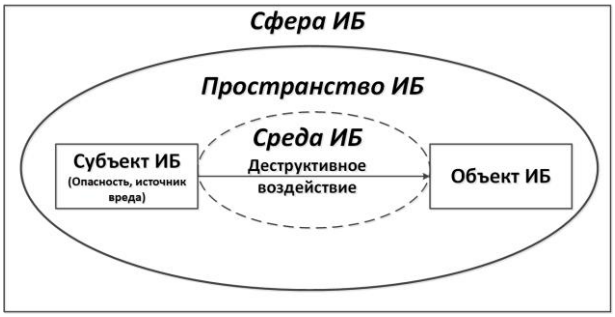


*Рис. 6,б. Структура сферы ИБ*

Аналогичные определения были даны и для области ИБ [2] (рис. 6,б). Отличительной особенностью сферы КБ от сферы ИБ является то, что киберпространство и киберсреда, как правило, будут виртуальными (особенности использования сетевых и интернет-технологий), а пространство ИБ и среда ИБ могут быть и реальными (физическими), и виртуальными.

Существенным является то, что в случае КБ нападающая и защищающаяся сторона потенциально располагают равными возможностями и взаимодействуют в одной сфере – Интернет [5].

Следует отметить, что различают киберпространство от пространства ИБ еще и тем, что введено понятие «заинтересованных сторон» (stakeholders)[2] – это организации или лица, обладающие своими объектами КБ, взаимодействующими друг с другом с использованием технологии интернет.

Стороны взаимодействия (типовой случай, рис. 6,а):

Сторона А – организации или лица, имеющие объекты КБ и потребляющие определенные услуги, необходимые для их функционирования (например, услуги провайдеров интернет).

Сторона В (провайдер) – это организация (лицо), предоставляющая свои услуги на основе эксплуатации определенного объекта КБ.

Сторона С – организации (лица), которые являются источниками деструктивного воздействия (опасностями) по направлению стороны А и, возможно, стороны В.

В соответствии со структурной схемой противоборства объекта и субъекта (рис. 4), сторона А будет обладать объектами КБ, сторона В объектами КБ и, возможно, субъектом КБ, а сторона С – субъектами КБ. Стороны А и В имеют общую заинтересованность сохранить свои активы. Стороны С имеет цель — это нанесение ущерба стороне А и (или) стороне В.

Особую роль во взаимодействии заинтересованных сторон играют их сотрудники. Причем для стороны А они должны рассматриваться как активы объектов КБ, на которые могут быть направлены деструктивные воздействия. Для сторон С и В сотрудники могут быть потенциальными нарушителями.

Таким образом, КБ должна рассматриваться как задача конфликтующих ветвей эволюции информационных технологий, что должно учитываться при создании ее методологических основ.

Анализ приведенных выше ответов на поставленные вопросы, определяющие максимально полное соответствие между понятием и его термином, позволил сформировать следующую совокупность ключевых терминов (понятий), относящихся к понятию «КБ объекта»: «объект КБ» (1), «актив объекта КБ» (2), «опасность» (3), «сфера КБ» (4), «пространство КБ» (5), «среда КБ» (6), «ущерб» (7), «состояние защищенности активов объекта КБ» (8). При этом понятия с (1) по (7) относятся к категории «предмет (объект)», а понятие (8) – к категории «свойство».

## 4. Формирование структуры системы понятий «кибербезопасность объекта», относящиеся к категории «предмет (объект)» и «свойство»

Ключевые понятия (термины), определенные выше, были использованы для того, чтобы сформулировать определения основных понятий (терминов) области «КБ объекта, а также определить структуру системы таких понятий.

Перечень определений основных понятий(терминов):

***Кибербезопасность объекта (КБ объекта)*** *— это состояние защищенности активов объекта КБ от деструктивного воздействия опасностей на объект КБ в сфере КБ, при котором возможный ущерб активам объекта КБ не будет превышать допустимый уровень (Вариант 1).*

***Объект кибербезопасности (объект КБ)*** *– это предмет, который может быть материальным (использующим информацию, сетевые и интернет-технологии), нематериальным (как результат интеллектуальной деятельности человека) или человеком.*

***Актив объекта кибербезопасности (актив объекта КБ)*** *– это часть объекта, представляющая ценность для владельца объекта.*

***Состояние защищенности активов объекта ИБ*** *– внутреннее состояние объекта, при котором свойства его активов находятся в допустимых пределах.*

***Свойства актива*** *– это качественные (признаки) или количественные (величины) характеристики актива.*

***Опасность (объекту)*** *– это источник потенциального ущерба для актива объекта.*

***Ущерб (активу)*** *– это недопустимое изменение свойств (характеристик) актива.*

*Определение понятия* ***«сфера КБ»*** *было сформулировано в четвертом разделе.*

Структура системы понятий «КБ объекта ИБ» приведена на рис. 7.

В структуру понятий «КБ объекта» включены не только ключевые понятия (термины), но и понятия (термины), связанные с ключевыми:

***«Виды объектов КБ»:*** сам объект КБ (ОтКБ), человек (Ч) как основной объект, имеющий отношение к информации (сведениям), информационный объект (ИнО), обрабатывающий информацию и использующий сетевые и интернет-технологии (ИТ); киберфизическая система (КФС), которой в настоящее время уделяют большое значение [5].

***Киберфизическая система*** *– это цифровая система, связанная с физическим процессом, объединяющая устройства управления цифровым производством, роботами, «Умными» устройствами интернет вещей, цифровые системы мониторинга и контроля, а также другие решения* [5].


*Рис. 7. Структура системы понятий «кибербезопасность объекта»*

***«Виды активов объекта КБ»:*** человек (Ч), взаимодействующий с объектом КБ, основные активы (процессы, которые реализует объект КБ или основные процессы (бизнес-процессы) организации, к которым имеет отношение объект КБ, и, возможно, информация, обрабатываемая объектом КБ) и вспомогательные активы (процессы, системы и ресурсы, обеспечивающие функционирование объекта КБ).

***«Свойства КБ»,*** относящиеся к активам объекта КБ и в отличии от свойств ИБ (ГОСТ Р ИСО/МЭК 13335-1[8]) будем называть свойствами КБ, которые включают в себя. целостность (Ц), доступность (Д), киберустойчивость (КУ) и реже, конфиденциальность (К).

***Киберустойчивость объекта*** *– это способность (свойство) объекта КБ сохранять свои характеристики в заданных пределах при деструктивном воздействии опасностей на активы объекта в сфере КБ или восстанавливать эти характеристики в установленных пределах времени после такого воздействия.*

Данное определение понятия «Киберустойчивость объекта» не противоречит ранее предложенному определению понятия «Киберустойчивость системы» как свойство системы сохранять функционирование системы в заданном диапазоне входных и выходных характеристик в условиях целенаправленных внешних информационных воздействий [17, 18].

Понятие «свойства КБ» непосредственно связано с ключевыми понятиями «состояние защищённости активов объекта КБ» и «ущерб». Современная методология обеспечения ИБ базируется на риск-ориентированном подходе[1] который позволяет связать понятие «состояние защищенности» с понятием «риск ИБ», которое базируется на понятии «опасность», как вероятности ее проявления и понятии «ущерб» при деструктивном воздействии опасности (рис. 7). При этом важным является определение величины и значимости риска ИБ. Значимость риска ИБ «допустимый» будет соответствовать состоянию защищенности активов объекта.

Аналогичным образом можно поступить при определении понятия (термина) «КБ объекта»:

***Кибербезопасность объекта (КБ объекта)*** *— это состояние защищенности активов объекта КБ от деструктивного воздействия опасностей на объект КБ в сфере*

*КБ, при котором риск нарушения свойств активов объекта КБ не будет превышать допустимый уровень. (Вариант 2).*

Существует множество определений понятия «риск»[6] и «риск ИБ» [19]. В данном случае можно остановиться на следующем определении понятия «риск КБ» [2]:

***Риск нанесения ущерба активу объекта КБ (риск КБ)*** *– это мера, учитывающая вероятностный характер нанесения ущерба активу объекта КБ и величину этого ущерба.*

Описанная выше структура понятий (рис. 7), относящихся к КБ объекта, обладает свойством иерархичности связей. Поэтому ее можно отнести к основам таксономии понятий в области КБ.

Следует отметить, что на практике повсеместно оперируют не понятием «опасность», а понятием «угроза ИБ», которое по отношению, например, к безопасности информации будет определяться как совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 50922-2006[9]). Это определение можно адаптировать к определению понятия «угроза КБ» [2]:

***Угроза кибербезопасности объекта (угроза КБ)*** *— это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения свойств активов объекта КБ.*

С учетом понятия «угроза КБ» и «риск КБ» можно предложить еще два варианта определения понятия «КБ объекта»:

***Кибербезопасность объекта (КБ объекта)*** *— это состояние защищенности активов объекта КБ от деструктивного воздействия угроз на объект КБ в сфере КБ, при котором возможный ущерб активам объекта КБ не будет превышать допустимый уровень (Вариант 3).*

***Кибербезопасность объекта (КБ объекта)*** *— это состояние защищенности активов объекта КБ от деструктивного воздействия угроз на объект КБ в сфере КБ, при котором риск нарушения свойств активов объекта КБ не будет превышать допустимый уровень. (Вариант 4).*

При построении систематики понятий в области ИБ [2] был признан факт, что по своей сути понятие «угроза ИБ» не может быть отнесена ни к одной из принятых категорий понятий (предмет, процесс, свойство), что усложняет выстраивание связей этого понятия с другими понятиями., что приводит к нарушению иерархичности системы понятий – важного принципа таксономии. Это утверждение также справедливо и для системы понятий в области КБ объекта.

Анализ структуры системы понятий «КБ объекта» (рис. 7) показывает, что для обеспечения ее таксономичности (рис. 1) можно совсем обойтись без понятия «угроза КБ», пользуясь только понятием «опасность». В настоящее время это сделать нельзя из-за распространенности использования термина (понятия) «угроза» в различных правовых и нормативных документах.

Необходимо отметить, вышеперечисленная совокупность терминов и определений, относящихся к понятию «кибербезопасность», не противоречит результатам анализа терминов и определений, существующих, например, в русскоязычных [2, 5, 16, 17] и в англоязычных [3] источниках.

[9]ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».

## 5. Формирование структуры системы понятий «кибербезопасность объекта», относящиеся к категории «процесс»

Современная методология, относящаяся к области ИБ, строится не только на риск-ориентированном подходе, но и на процессном и управленческом подходах (ГОСТ Р ИСО/МЭК 27000-2021[4]), чему соответствует своя понятийная база.

Понятия «КБ объекта» (Варианты 1, 2, 3 и 4), определения которых сформулированные выше, связаны с понятием «состояние защищенности актива объекта КБ». На практике важным является реализация набора взаимосвязанных или взаимодействующих мероприятий, которые направлены на обеспечение требуемого состояния защищенности активов объектов КБ. Сам набор мероприятий принято обозначать понятием «процесс»[5]. Поэтому важным является понятие «обеспечение КБ объекта», которое можно определить следующим образом:

***Обеспечение кибербезопасности объекта (ОКБ объекта)*** *– это реализация набора взаимосвязанных или взаимодействующих процессов* ***(процессов ОКБ объекта)****, которые направлены на обеспечение требуемого состояния защищенности активов объекта КБ.*

Определение понятия «ОКБ объекта» непосредственно связано с определениями «КБ объекта» и должны рассматриваться вместе, когда речь идет о решении проблем ОКБ различных объектов.

Применение в рамках ОКБ объекта процессного подхода предполагает необходимость проведения идентификации процессов ОКБ и процессов управления ими, определения мер, реализующих эти процессы, а также определения необходимых для этого ресурсов так, как это осуществляется для области ИБ[5]. Меры ОКБ – это практические приемы или другие действия, относящиеся к конкретному процессу ОКБ.

На рис. 8 представлена структура систем понятий категории «процессы» области КБ объекта, относящихся к процессному и управленческому подходам. При этом каждому процессу сопоставлены меры, его реализующие и необходимые для этого ресурсы.

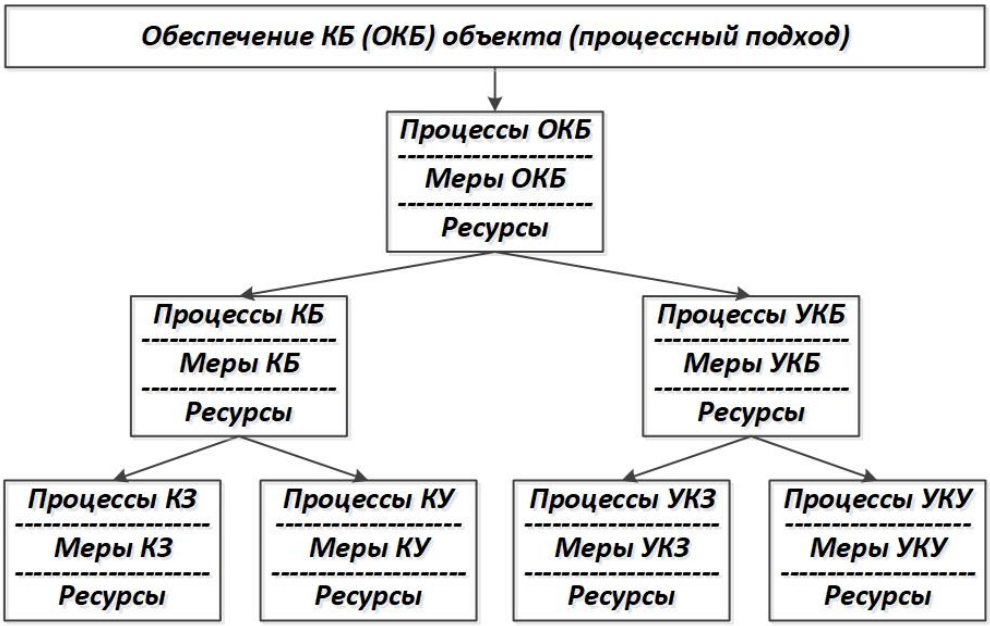


*Рис. 8. Структура системы понятий области КБ объекта, имеющих категорию «процессы»*

Реализация любого процесса для достижения необходимого результата требует определенных действий по его управлению. Поэтому среди всех возможных процессов ОКБ объекта представляется целесообразным выделить группу процессов кибербезопасности (процессы КБ) и группу процессов управления КБ (процессы УКБ).

***Процессы кибербезопасности объекта КБ (процессы КБ)*** *– это набор взаимосвязанных или взаимодействующих процессов, реализация которых направлена на обеспечение определенного состояния защищенности активов объекта КБ.*

***Процессы управления кибербезопасностью объекта ИБ (процессы УКБ)*** *– это набор процессов управления, предназначенные для обеспечения необходимого качества конкретного процесс КБ объекта при его планировании, реализации, контроле и совершенствовании.*

Под качеством процесса будем понимать результативность и эффективность его реализации.

Такое решение соответствует современной методологии обеспечения ИБ[4], и аналогичен, например, подходу, реализованном в стандарте ГОСТ Р 57580.1-2017[10]: процессы защиты информации и процессы организации и управления защитой информации.

Реализация процессов КБ и процессов УКБ направлена на обеспечение необходимого уровня риска нанесения ущерба активам объекта КБ. При этом процессы КБ напрямую формируют уровень риска, а процессы управления КБ оказывают косвенное влияние на это формирование.

Учитывая особенности целей ОКБ объекта КБ, его активов, угроз КБ, ущерба, возникающего при возможной реализации угроз КБ, а также современной тенденции перевода рассмотрения проблемы обеспечения КБ объекта КБ в плоскость обеспечения его киберустойчивости [5] предлагается разделить группу процессов КБ на две части (рис. 8): процессы киберустойчивости (КУ), когда активами объекта КБ являются или его основные процессы и связанные с ними основные процессы организации или сам объект КБ; процессы киберзащиты (КЗ), когда учитываются остальные активы (в том числе и информационные активы). Аналогичным образом группа процессов УКБ разделяется на две части: процессы управления КУ и процессы управления КЗ.

***Процессы управления киберберустойчивостью объекта ИБ (процессы УКУ)*** *– это набор процессов управления, предназначенные для обеспечения необходимого качества конкретного процесс КУ объекта при его планировании, реализации, контроле и совершенствовании.*

***Процессы управления киберзащитой объекта ИБ (процессы УКЗ)*** *– это набор процессов управления, предназначенные для обеспечения необходимого качества конкретного процесс КЗ объекта при его планировании, реализации, контроле и совершенствовании.*

В настоящей работе предлагается совокупность мер ОКБ разделить на четыре группы, связанные с конкретными группами процессов обеспечения КБ (рис. 8): меры КЗ (процессы КЗ), меры КУ (процессы КУ), меры УКЗ (процессы УКЗ) и меры УКУ (процессы УКУ). Причем меры КЗ и меры КУ чаще бывают техническим, а меры УКЗ и УКУ – организационными.

Анализ структуры системы понятий, приведенной на рис. 8, показывает, что эта структура строго иерархична. Таким образом, можно признать систематику понятий КБ объекта при рассмотрении понятий категории «процесс» таксономией.

[10]ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

## 6. Формирование структуры системы понятий «кибербезопасность объекта», относящиеся к категории «предмет (система)»

Современная методология, относящаяся к области ИБ, строится не только на риск-ориентированном, процессном и управленческом подходах, но и на системном подходе[5], чему соответствует своя понятийная база.

Разделение процессов ОКБ и связанных с ними мер ОКБ на группы (процессный и управленческий подходы) позволяет сформировать совокупность систем, относящихся к ОКБ. Структура системы понятий, относящихся к системе ОКБ представлена на рис. 9.

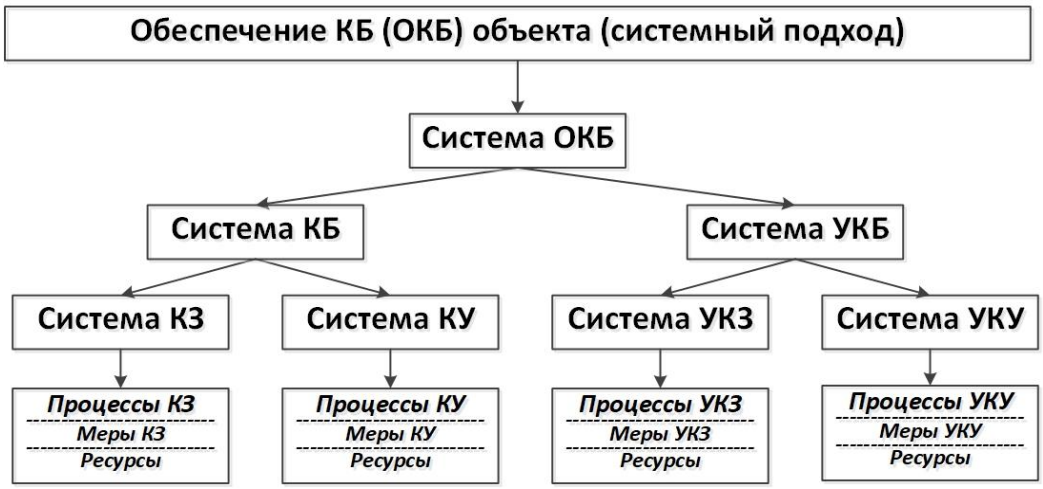


*Рис. 9. Структура системы понятий области КБ объекта, имеющих категорию «предмет (система)»*

***Система киберзащиты объекта КБ (система КЗ, СКЗ)*** *– это совокупность связанных процессов и мер киберзащиты, а также необходимых для этого ресурсов:* ***СКЗ = Процессы КЗ + Меры КЗ + Ресурсы****.*

***Система киберустойчивости объекта КБ (система КУ, СКУ)*** *– это совокупность связанных процессов и мер киберустойчивости, а также необходимых для этого ресурсов:* ***СКУ = Процессы КУ + Меры КУ + Ресурсы****.*

***Система управления киберзащитой объекта КБ (система УКЗ, СУКЗ)*** *– это совокупность связанных процессов и мер УКЗ, предназначенных для обеспечения необходимого качества конкретного процесса КЗ объекта при его планировании, реализации, контроле и совершенствовании, а также необходимых для этого ресурсов:* ***СУКЗ = Процессы УКЗ + Меры УКЗ + Ресурсы.***

***Система управления киберустойчивостью объекта КБ (система УКУ, СУКУ)*** *– это совокупность связанных процессов и мер УКУ, предназначенных для обеспечения необходимого качества конкретного процесса КУ объекта при его планировании, реализации, контроле и совершенствовании, а также необходимых для этого ресурсов:* ***СУКУ = Процессы УКУ + Меры УКУ + Ресурсы.***

***Система кибербезопасности (система КБ, СКБ)*** *состоит из системы киберзащиты (СКЗ) и системы киберустойчивости (СКУ):* ***СКБ = СКЗ + СКУ****.*

***Система управления кибербезопасностью (система УКБ, СУКБ)*** *состоит из системы управления киберзащитой (СУКЗ) и системы управления киберустойчивостью (СКУ):* ***СКБ = СКЗ + СКУ****.*

***Система обеспечения кибербезопасности (СОКБ)*** *состоит из системы кибербезопасности (СКБ) и системы управления кибербезопасностью (СУКБ):* ***СОКБ = СКБ + СУКБ.***

Такое решение полностью соответствует современной методологии обеспечения ИБ, описанной в группе стандартов ГОСТ Р ИСО/МЭК 27000, и аналогичен, например, подходам, реализованным в:

1) стандарте Банка России СТО БР ИББС-1.0-2014[11]: процессы ИБ, система ИБ (СИБ), процессы менеджмента, система менеджмента ИБ (СМИБ).

2) стандарте ГОСТ Р 57580.1-2017[10]: процессы ЗИ и система ЗИ (СЗИ), процессы и система организации и управления ЗИ (СОиУЗИ).

Анализ структуры системы понятий, приведенной на рис. 9, показывает, что эта структура строго иерархична. Таким образом, можно признать систематику понятий КБ объекта при рассмотрении понятий категории «предмет (система)».

В данной работе были сделаны попытки объединения структур систем понятий, представленных на рис. 8 и рис. 9, рис. 7 и рис. 8, рис. 7 и рис. 9, а также рис. 7, рис.8 и рис. 9, которые не привели к построению строго иерархичных систем.

Необходимо также отметить, что рассмотренные в данном разделе понятия следует отнести к категории «предмет (объект)» искусственного происхождения, как к результату интеллектуальной деятельности человека, подобно сделанному в отношении системы менеджмента ИБ (СМИБ) в стандарте ГОСТ Р ИСО/МЭК 27001-2021[12]: в котором рассмотрены требования к созданию, внедрению, поддержке и постоянному улучшению СМИБ.

## Заключение

В работе на базе принятой ранее систематики понятий предложена классификация понятий, имеющая отношение к кибербезопасности (КБ) объектов и обладающая на данный момент максимальной однозначностью соответствия терминов, обозначающими эти понятия, и понятиями.

При построении классификации была предпринята попытка применить основы теории таксономии (систематики), результаты которой позволили сделать вывод, что рассмотренные структуры систем понятия будут иерархичными (основной принцип таксономии) при определенных условиях (например, при использовании только понятий, которые относятся к категориям предмета (объекта), процесса и предмета(системы)).

Первую из перечисленных структур можно считать таксономией условно. Это можно объяснить, например, тем фактом, что в структуру системы понятий «КБ объекта» вынуждено было включено понятие «угроза КБ», признанное в настоящее время, но находящееся вне существующих категорий понятий. Исключение этого понятия могло бы существенно повысить уровень иерархичности системы понятий.

Рассмотренный в работе подход позволил сформировать группу терминов, непосредственно связанных с понятиями из предлагаемой классификации. Эту совокупность можно рассматривать как терминосистему, относящуюся к области КБ объекта.

Предложенные термины и их определения не противоречат аналогичным, используемым на практике, но отличаются системностью в отношении самих терминов

[11]Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение ИБ организаций банковской системы РФ. Общие положения».

[12]ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

(определений) и системностью в отношении соответствующих понятий, а также имеют универсальный характер применения, что позволяет их использование для практически любых объектов КБ, имеющих отношение к информации (например, информационные и автоматизированные системы, системы информатизации, социотехнические системы, киберфизические системы и информация как объект).

Результаты работы имеют практическую значимость для образовательной области. Формирование у обучающихся современной, методически обоснованной понятийной базы – одна из задач, которая решается образовательными учреждениями при подготовки современных профессионалов в области кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Информационная безопасность. Глоссарий. А. Черемушкин; под ред. С. Пазизина. М.: Медиа группа «АВАНГАРД, 2018. – 372 с.
2. Толстой Александр И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, [S.l], т. 30, № 1, с. 130–148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10. – EDN: JTYQNV.
3. Definition of Cybersecurity – Gaps and overlaps in standardization. European Union Agency For Network And Information Security, v1.0, December 2015. ISBN 978-92-9204-155-7. DOI: 10.2824/4069.
4. Добродеев А.Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века. Вопросы кибербезопасности. 2021, № 4(44). С. 61–72.
5. Зегжда Д.П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак. СПб.: ПОЛИТЕХ-ПРЕСС, 2022. – 490 с.
6. Что такое кибербезопасность? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (дата обращения: 25.12.2023).
7. Милославская, Наталья Г.; Толстая, Светлана А. Угрозы нарушения кибербезопасности для организаций инфраструктуры финансовых рынков. Безопасность информационных технологий, [S.l.], т. 23, № 1, p. 115–126, 2016. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/39 (дата обращения: 25.12.2023). – EDN: WMWDGJ.
8. Сухомлин В.А. и др. Модель цифровых навыков кибербезопасности 2020. Современные информационные технологии и ИТ-образование, [S.l.], т. 16, № 3, p. 695–710, 2020. ISSN 2411-1473. DOI 10.25559/SITITO.16.202003.695-710. – EDN: MKXOUE.
9. Сухомлин В.А. Каррикулум дисциплины «Кибербезопасность»: научное издание. В.А. Сухомлин, С.В. Лебедь, О.С. Белякова, А.С. Климина, М.С. Полянская. М.: Фонд «Лига интернет-медиа». 2022. – 402 с.
10. Советский энциклопедический словарь. М.: Советская энциклопедия, 1990.
11. Шаталкин А.И. Таксономия. Основания, принципы и правила. М.: Товарищество научных изданий КМК. 2012. – 600 с.
12. Черешкин Д.С., Тищенко Д.В. Принципы таксономии угроз безопасности информационных систем. URL: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/principy-taksonomii-ugroz-bezopasnosti-informacionnyh-sistem (дата обращения: 21.11.2023).
13. Духнич Ю. Таксономия в системе управления знаниями. URL: http://www.smart-edu.com/taksonomiya-v-sisteme-upravleniya-znaniyami.html (дата обращения: 24.12.2023).
14. Атаманов Г.А. Топология безопасности. 2010. URL: http://gatamanov.blogspot.ru/ (дата обращения: 25.12.2023).
15. Чувелева Н.Н. Классификация видов безопасности. Образовательный портал «Справочник». 2020. URL: https://spravochnick.ru/pravo_i_yurisprudenciya/klassifikaciya_vidov_bezopasnosti/ (дата обращения: 24.12.2023).
16. Энциклопедия кибернетики» под ред. В.М. Глушкова, т. 1., Киев. 1974. –440 с.
17. Гавдан Григорий П. и др. Устойчивость технологических процессов в авспекте безопасности критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 30, № 2, с. 38–52, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.2.02.
18. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. М.: Горячая линия – Телеком, 2023. – 560 с.
19. Милославская Н.Г., Толстой А.И. Управление рисками информационной безопасности. Учебное пособие для вузов. 3-е изд., перераб. и доп. М.: Горячая линия – Телеком. 2022. – 224 с.

REFERENCES:
[1] Cheremushkin A. V. Information security. Glossary. Ed. S. Pazizina. M.: Media group "AVANGARD". 2018. – 372 p. (In Russian).
[2] Tolstoy Alexander I. Systematics of concepts in the field of information security. IT Security (Russia), [S.1], v. 30, no. 1, p. 130–148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10 (in Russian). – EDN: JTYQNV.
[3] Definition of Cybersecurity – Gaps and overlaps in standardization. European Union Agency For Network And Information Security, v1.0, December 2015. ISBN 978-92-9204-155-7. DOI: 10.2824/4069.
[4] Dobrodeev A.Yu. Cybersecurity in the Russian Federation. A fashionable term or a priority technological direction for ensuring national and international security of the XXI century. Cybersecurity Issues. 2021, no. 4(44), p. 61–72 (in Russian).
[5] Zegzhda D.P. Theoretical foundations of cyber resilience and the practice of predictive protection against cyber attacks. St. Petersburg: POLYTECH-PRESS, 2022. – 490 p. (in Russian).
[6] What is cyber security? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (accessed: 24.12.2023) (in Russian).
[7] Miloslavskaya, Natalia G.; Tolstaya, Svetlana A. Cyber Threats for Organizations of Financial Market Infrastructures. IT Security (Russia), [S.l.], v. 23, no. 1, p. 115–126, 2016. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/39 (accessed: 24.12.2023) (in Russian). – EDN: WMWDGJ.
[8] Sukhomlin, Vladimir Alexandrovich et al. Cybersecurity digital skills model 2020. Modern information technologies and IT education, [S.l.], v. 16, no. 3, p. 695–710, 2020. ISSN 2411-1473. DOI 10.25559/SITITO.16.202003.695-710. – EDN: MKXOUE.
[9] Sukhomlin V.A. Curriculum of the discipline "Cybersecurity": scientific publication. V.A. Sukhomlin, S.V. Lebed, O.S. Belyakova, A.S. Klimina, M.S. Polyanskaya. Moscow: League of Internet Media Foundation. 2022. – 402 p. (in Russian).
[10] Soviet encyclopedic dictionary. M.: Soviet Encyclopedia, 1990 (in Russian).
[11] Shatalkin A.I. Taxonomy. Foundations, principles and rules. M.: Association of scientific publications KMK. 2012. – 600 p. (in Russian).
[12] Chereshkin D.S., Tishchenko D.V. Principles of taxonomy of security threats to information systems. URL: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/principy-taksonomii-ugroz-bezopasnosti-informacionnyh-sistem (accessed: 21.11.2023) (in Russian).
[13] Dukhnich Yu. Taxonomy in the knowledge management system. URL: http://www.smart-edu.com/taksonomiya-v-sisteme-upravleniya-znaniyami.html (accessed: 24.12.2023) (in Russian).
[14] Atamanov G.A. Security Topology. 2010. URL: http://gatamanov.blogspot.ru/ (accessed: 25.12.2023) (in Russian).
[15] Chuveleva N.N. Classification of security types. Educational portal "Spravochnik". 2020. URL: https://spravochnick.ru/pravo_i_yurisprudenciya/klassifikaciya_vidov_bezopasnosti/ (accessed: 24.12.2023) (in Russian).
[16] Encyclopedia of Cybernetics, ed. V.M. Glushkov, v. 1., Kyiv. 1974 – 440 p. (in Russian).
[17] Gavdan Grigory P. et al. Sustainability of technological processes in the aspect of security of critical information infrastructure. IT Security (Russia), [S.l.], v. 30, no. 2, p. 38–52, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.2.02 (in Russian).
[18] Cybersecurity of the digital industry. Theory and practice of functional resistance to cyberattacks. Edited by Professor of the Russian Academy of Sciences, Doctor of Technical Sciences D.P. Zegzhda. M.: Hotline – Telecom, 2023. – 560 p. (in Russian).
[19] Miloslavskaya N.G., Tolstoy A.I. Information security risk management. Textbook for universities. 3rd ed., revised. and additional. M.: Hotline – Telecom. 2022. – 224 p. (in Russian).

*Поступила в редакцию – 01 февраля 2024 г. Окончательный вариант – 10 марта 2024 г.*
*Received – February 01, 2024. The final version – March 10, 2024.*