УДК: 004.056
doi: 10.26583/bit.2024.3.05

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

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация. В статье определены основные проблемы, связанные с противоречивостью и несогласованностью таких понятий, как «защита информации», «информационная безопасность», «безопасность информации», «кибербезопасность» и «киберустойчивость», что привело к отсутствию в настоящее время принятой профессиональным сообществом единой системы понятий рассматриваемой предметной области. Для преодоления этого недостатка предложено построить базовую систему понятий для предметной области «безопасность объектов в информационной сфере (ИСФ)», основанную на учете особенностей объектов (использующих информационные технологии и осуществляющих обработку информации), на использовании понятия «ИСФ» (как совокупности пространства таких объектов и среды их взаимодействия) и на понятии «актив» (часть объекта, представляющая определенную ценность), который может быть основным и вспомогательным. С учётом этих исходных данных выделенная предметная область сопоставлена с тремя отдельными системами понятий: «обеспечение безопасности информации объектов в ИСФ», «обеспечение устойчивости объектов в ИСФ» и «обеспечением информационно-психологической безопасности человека как актива объекта в ИСФ». Дано описание предложенных систем понятий, что можно отнести к развитию методологической базы обеспечения безопасности объектов. Эти системы понятий имеют минимальное пересечение друг с другом и соответствуют трем отдельным сферам практической и научной деятельности, которые требуют профессионалов с уникальными профессиональными компетенциями. Результаты работы также имеют практическую значимость для образовательной области при формировании у обучающихся современной, методически обоснованной понятийной базы.

Ключевые слова: понятие, термин, определение, защита информации, безопасность, устойчивость, кибербезопасность, объект, информационная сфера, актив, процесс, система.
Для цитирования: ТОЛСТОЙ, Александр И. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ В ИНФОРМАЦИОННОЙ СФЕРЕ. Безопасность информационных технологий, [S.l.], т. 31, № 3, с. 105–123, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1677. DOI: http://dx.doi.org/10.26583/bit.2024.3.05.

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

Ensuring the security of objects in the information sphere

Abstract. The article identifies the main problems associated with the inconsistency and incoordination of such concepts as “information protection”, “information security”, “security of information”, “cybersecurity” and “cyber resilience”, which has led to the absence of a unified system currently accepted by the professional community concepts of the subject area under consideration. To overcome this flaw, it is proposed to build a basic system of concepts for the “security of objects in the information sphere (ISF)” subject area, based on taking into account the characteristics of objects (which using information technologies and processing information), using the ISF concept (as a collection of space of such objects and the environment of their interaction) and on the asset concept (part of an object that has a certain value),

which can be main and auxiliary. Taking into account these initial data, the selected subject area is compared with three separate systems of concepts: “ensuring the security of information of objects in the ISF”, “ensuring the resilience of objects in the ISF” and “ensuring the information and psychological security of a person as an object’s asset in the ISF”. A description of the proposed systems of concepts is given, which can be attributed to the development of a methodological basis for ensuring the objects’ security. These conceptual systems have minimal overlap with each other and correspond to three separate areas of practical and scientific activity that require professionals with unique professional competencies. The results of the work have practical significance for the educational field in the formation of students' modern, methodologically sound conceptual base.

Keywords: concept, term, definition, information protection, security, resilience, cybersecurity, object, information sphere, asset, process, system.

For citation: TOLSTOY, Alexandr I. Ensuring the security of objects in the information sphere. IT Security (Russia), [S.l.], v. 31, no. 3, p. 105–123, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1677. DOI: http://dx.doi.org/10.26583/bit.2024.3.05.

Введение

Построение систематики понятий, относящихся к предметной области «безопасность», возможна только при обеспечении однозначности самого понятия термину, его представляющего. Речь идет о системе понятий в узком смысле слова [1]. Поэтому в дальнейшем будут рассмотрены только понятия, имеющие отношение к термину «безопасность объекта». Причем ограничимся рассмотрением тех объектов, которые относятся к информационной сфере (ИСФ).

Анализ определения понятия «информационная сфера», приведённого в Доктрине «Информационная безопасность РФ»[1], позволяет утверждать, что объект в ИСФ (далее Объект) может быть материальным предметом (например, техническая система), или нематериальный предмет (процесс, система), или человеком (носителем информации), или самой информацией.

К Объектам могут быть отнесены, например, государство[1], любая организация (ГОСТ Р 53114-2008[2]), банковская организация (СТО БР ИББС-1.0-2014[3]) или такие объекты, как информационная система, автоматизированная система, объект информатизации, киберфизическая система [2]. Все эти объекты обладают также общей особенностью, связанной с обработкой определенного вида информации с использованием информационных технологий.

Наиболее актуальной проблемой, относящейся и к научным исследованиям, и к практическим действиям, является обеспечение безопасности и устойчивости таких Объектов. При этом можно использовать методологию обеспечения информационной безопасности (ИБ) и обеспечения кибербезопасности (КБ), основы которой изложены в группе международных стандартов ISO/IEC 27000.

У части этих стандартов имеются аналоги в виде группы национальных стандартов ГОСТ Р ИСО/МЭК 27000. Если ориентироваться на определение понятия «ИБ» как *сохранение конфиденциальности, целостности и доступности информации*, приведенное в ГОСТ Р ИСО/МЭК 27000-2021[4], то можно утверждать, что основной целью ИБ Объекта

[1]Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 05.12.2016 № 646.

[2]ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

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

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

будет обеспечение сохранности данных (сведений, знаний), обрабатываемых Объектом. Проблема устойчивости Объекта, не называя ее, учитывается в рамках обеспечения непрерывности ИБ в связи с обеспечением непрерывности бизнес-процессов организации, частью которой является Объект (ГОСТ Р ИСО/МЭК 27001-2021[5]).

В настоящее время внимание профессиональной общественности все больше уделяется проблемам кибербезопасности (КБ), которые на международном уровне решаются с учетом существующей нормативной базы, приведенной в группе стандартов ISO/IEC 27000: 27032[6] (Руководство по КБ), 27103[7] (КБ и стандарты ISO и IEC) и 27110[8] (Руководство по обеспечению КБ). Данные стандарты не имеют аналогов в национальной системе стандартизации, что делает актуальным совершенствование нормативно-правового регулирования в области обеспечения ИБ и КБ [3].

Следует отметить тот факт, что в стандарте ISO/IEC 27103[7] определено, что большинство норм, приведенных в группе стандартов ISO/IEC 27000 и относящихся к обеспечению ИБ, могут быть применены и при обеспечении КБ. Таким образом можно полагать, что данная группа стандартов является общей нормативной базой, реализующей риск-ориентированный, процессный и системный подходы к обеспечению и ИБ, и КБ.

Актуальность и важность развития направления обеспечения КБ подчеркивает и тот факт, что в 2022 г. общее название группы стандартов ISO/IEC 27000 изменилось с «Информационные технологии. Методы обеспечения безопасности (Information technology. Security techniques)» на «Информационные технологии, кибербезопасность и защита персональных данных (Information technology, cybersecurity and privacy protection)».

В стандарте ISO/IEC 27032[6] дано определение понятия «кибербезопасность» (приводится в свободном переводе на русский язык), как *сохранение конфиденциальности, целостности и доступности информации в киберпространстве.*

Этот стандарт впервые вводит термин «киберпространство», определяемый как *сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и услуг в интернете посредством технологических устройств и подключенных к нему сетей*». При этом в группе стандартов ISO/IEC 27000 не используется в отношении области ИБ термин, аналогичный терминам киберпространство и киберсреда, а в нормативных документах РФ при определении понятия «ИБ» используется понятие «информационная сфера». Отсюда возникает необходимость уточнения понятийной базы, относящейся к области обеспечения безопасности Объектов в части использования понятий «сфера», «пространство» и «среда» [4].

Отсутствие единой понятийной базы в области КБ объясняет, например, попытки применить определение термина КБ, взятого из международного стандарта ISO/IEC 27032[6], не имеющего аналога на национальном уровне, при исследовании угроз нарушения КБ для организаций инфраструктуры финансовых рынков [5]. Особенностью этого определения является утверждение, что область КБ является частью области ИБ.

Сравнение помянутых выше определений понятий «ИБ» и «КБ» показывает, что и в случае КБ основным объектом защиты является информация. Отличие заключается в особенностях киберпространства.

[5]ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
[6]ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.
[7]ISO/IEC TR 27103:2018 Information technology – Security techniques – Cybersecurity and ISO and IEC standards.
[8]ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines.

Второе отличие относится к основной цели КБ [2, 6] – это обеспечить стабильность (устойчивость) функционирования Объекта и Организации, к которой он относится. В данном случае киберустойчивость можно определить, как *способность предвидеть и адаптироваться к изменениям в среде, а также выдерживать, сдерживать и быстро восстанавливаться после киберинцидентов* [7].

Таким образом, при решении проблем обеспечения КБ Объекта в первую очередь следует обращать внимание на его устойчивость, а не на сохранность информации.

В настоящее время можно говорить о возникновении противоречия в случаях обеспечения ИБ и КБ Объекта: с одной стороны, единая методологическая база (группа стандартов ISO/IEC 27000), а с другой – различие целей обеспечения ИБ и КБ. По сути, возникла коллизия между направлениями исследований при рассмотрении последствий, возникающих при противодействии Объекта возможным деструктивным воздействиям на него.

Все это внесло определенную путаницу в понятийную базу области ИБ. Например, утверждается, что понятие «ИБ в автоматизированных системах» с точки зрения методологии является абсурдом [8]. Для таких объектов необходимо говорить только о защите информации (корректнее – информационных ресурсов) обрабатываемой / циркулирующей / содержащейся в этой системе. Высказывается мнение о необходимости разработки новой методологии ИБ [8].

В данной статье предпринята попытка разрешения выше отмеченных проблем и противоречий на основе использования системного подхода при формировании систематики понятий в рассматриваемой предметной области [1, 4] с учетом особенностей объектов в ИСФ.

1. Объекты в информационной сфере

Обеспечение безопасности любого объекта может быть рассмотрена как противоборство двух сущностей (рис. 1): субъекта, реализующего деструктивное воздействие на объект (Объект Б), и самого объекта (рис. 1). При этом важным является определение особенностей этих сущностей и имеющей к ним отношение информационной сферы.

В схеме противоборства (рис. 1) при определенных условиях следствием деструктивного воздействия Субъекта Б на Объект Б будет ущерб, нанесенный Объекту Б. Поэтому он может быть определен как «опасность» (*потенциальный источник возникновения ущерба*, ГОСТ Р 51898[9]) или источник угрозы, представляющий собой *совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности объекта* (адаптировано из ГОСТ Р 50922[10]). Типовые источники деструктивного воздействия могут иметь антропогенный, природный, техногенный, социальный или нормативно-правовой характер (ГОСТ Р ИСО/МЭК 27005-2010[11]).

[9]ГОСТ Р 51898-2002 (переиздан в 2018 г.) Аспекты безопасности. Правила включения в стандарты.
[10]ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
[11]ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности.

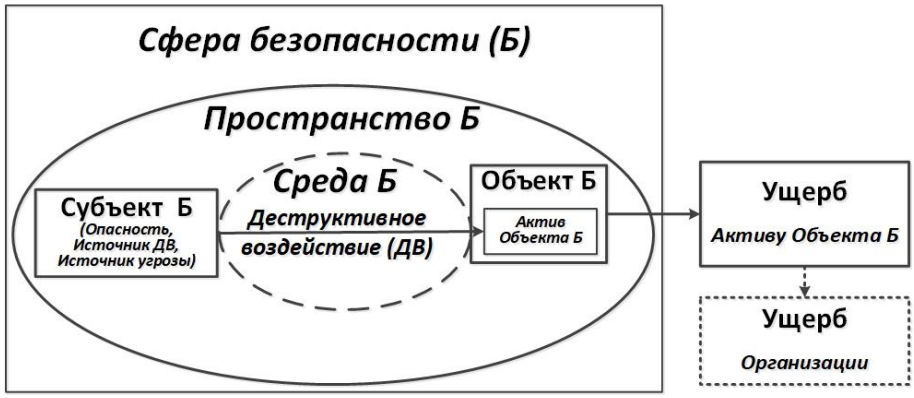

Рис. 1. Схема противоборства объекта и субъекта

При этом можно уверено утверждать, что безопасность объекта – это ситуация, когда по отношению к Объекту отсутствует опасность как источник деструктивного воздействия[9] [9] или источник угрозы.

При противоборстве важным является определение совокупности источников деструктивного воздействия (Опасностей) и Объектов с описанием их особенностей включая взаимное расположение, а также описание особенностей области их взаимодействия. Такой подход позволяет преодолеть выделенное выше противоречие в определении понятий «информационная сфера», «киберпространство» и «киберсреда», если воспользоваться принятым понятием «сфера», которое связывают с определенной областью, окружением, средой и обстановкой (Философская энциклопедия[12]) для определения следующих понятий [1]:

Сфера безопасности (сфера Б) *– это совокупность пространства безопасности и среды безопасности.*

Пространство безопасности (пространство Б) *– это совокупность объекта безопасности (Объекта Б) и субъекта безопасности (источника деструктивного воздействия на активы объекта безопасности - Субъекта Б) с описанием их свойств и определением взаимного расположения.*

Среда безопасности (среда Б) *– это область взаимодействия объекта безопасности (Объекта Б) и субъекта безопасности (источника деструктивного воздействия на активы объекта безопасности - Субъекта Б) с описанием ее свойств.*

Данные определения не учитывают конкретный вид безопасности. Поэтому они обладают универсальностью. Если объект имеет отношение к обработке информации с необходимостью обеспечить ее безопасность, то он будет объектом в информационной сфере (Объект в контексте данной работы или Объект БИ и соответствующий ему Субъект БИ), а унифицированные определения, приведенные выше, можно преобразовать в определения понятий «**сфера безопасности информации (сфера БИ)**» (информационная сфера), «***пространство безопасности информации*** (пространство БИ (информационное пространство) и «***среда безопасности информации (среда БИ)***» (информационная среда) [1]. Аналогичным образом при переходе от унифицированных понятий Объект Б и Субъект Б к объекту и субъекту, относящихся к кибербезопасности (Объект КБ и Субъект КБ) можно преобразовать унифицированные определения понятий, приведенные выше, в определения понятий «***сфера кибербезопасности (сфера КБ)***» (киберсфера),

[12]Философская энциклопедия. Режим доступа к ресурсу: URL: https://terme.ru/termin/sfera.html (дата обращения: 04.04.2024).

«***пространство кибербезопасности (пространство КБ)***» (киберпространство) и «***среда кибербезопасности (среда КБ)***» (киберсреда) [4], заменив Объект Б и Субъект Б на Объект КБ и Субъект КБ. При этом, если на физическом уровне Сфера БИ (информационная сфера) может быть любой, то Сфера КБ (киберсфера) будет исключительно виртуальной из-за использования сетевых и интернет-технологий.

Если говорится об обеспечении безопасности Объекта, то прежде всего обращают внимание на ту его часть, которая признается наиболее ценной для владельца Объекта и которую принято (ГОСТ Р ИСО/МЭК 27000-2021[4]) называть активом Объекта. Причем ценность актива будет определяться исходя из влияния актива на реализацию процессов самого объекта (рис. 1). При этом возможны принципиально отличающиеся два варианта Объектов: организация в целом (Организация) и Объект как часть Организации.

Для первого варианта в Организации можно выделить актив, непосредственно имеющий отношение к реализации основного процесса Организации, формирующего ее бюджет (бизнес-процесс). В большинстве случаев реализацию бизнес-процесса можно связать с оказанием определенных услуг партнёрам или клиентам. Примером может быть деятельность банковской организации.

При деструктивном воздействии на активы Организации может быть нанесен ущерб ее активам и связанному с ними бизнес-процессу. Ущерб обычно для актива связывают с нарушением его свойств конфиденциальности (К), доступности (Д) и целостности (Ц), а у бизнес-процесса с нарушением его Д и Ц (ГОСТ Р ИСО/МЭК 27000-2021[4]). Причем значимость ущерба для бизнес-процесса может быть определена на экономическом, финансовом, технологическом или репутационном уровнях.

Примером второго варианта, когда Объект является частью Организации, может быть банковская организация, использующая автоматизированную банковскую систему (АБС) для автоматизации банковского технологического процесса, участвующего в поддержке бизнес-процесса банка, связанного с оказанием банковской услуги. Для АБС принципиально важным является обеспечение ее безопасности. К таким объектам других организаций можно отнести информационные системы, автоматизированные системы управления технологическим процессом (АСУТП), объекты информатизации. Общими особенностями таких Объектов являются обработка информации и использование для этого современных информационных технологий (ИТ), а также реализацию процессов обработки информации, которую можно интерпретировать как внутренне-организационный ИТ-сервис.

В Объекте как части организации необходимо выделить актив, имеющий непосредственное отношение к реализации процесса Объекта (ИТ-сервис), связанного с бизнес-процессом Организации. При деструктивном воздействии опасности на актив Объекта может быть нанесен ущерб его активу и связанному с ним ИТ-сервису Объекта и бизнес-процессу (услуги) Организации (рис. 1). Ущерб для актива связывают с нарушением его свойств К (только для информационного актива), Д и Ц, для Объекта – с нарушением Д и Ц процесса оказания ИТ-сервиса, а для бизнес-процесса – с нарушением Д и Ц.

При описании особенностей Объекта важным является классификация его активов, которую можно осуществить в соответствии с рекомендациями ГОСТ Р ИСО/МЭК 27005-2010[11]. К активам Объекта могут быть отнесены: процессы Объекта и, если он является частью Организации, связанные с ними бизнес-процессы Организации; информация; аппаратное обеспечение (АО); программное обеспечение (ПО); сеть (телекоммуникационные устройства, используемые для соединения нескольких физически удаленных частей Объекта); персонал (состоит из всех групп сотрудников, участвующих в работе Объекта); место функционирования Объекта (включает в себя все площадки,

имеющие отношение к области применения Объекта); вспомогательные сервисы, необходимые для функционирования оборудования Объекта (связь, коммуникации); организация (инфраструктурные части организации, к которым относятся сотрудники организации, осуществляющие определенную деятельность под руководством этих частей).

Данным активам присущи уязвимости, которые могут быть использованы источниками деструктивного воздействия, нацеленными на нанесение ущерба активам Объекта. Этот ущерб непосредственно связан с изменением определенных свойств (характеристик, параметров) активов. Его величина может быть определена на основе использования конкретных метрик свойств активов и оценена исходя из допустимости или недопустимости возникновения определенного уровня ущерба активам Объекта, самому Объекту и Организации, к которой он относится. Заранее владелец объекта должен определить максимальный уровень допустимого ущерба [1]. Если деструктивное воздействие на актив организации или Объект приведет к уровню ущерба, меньшему, чем максимально допустимый уровень, то этим деструктивным воздействием можно пренебречь. В этом случае можно считать, что Организация или Объект будет обладать внутренним состоянием защищенности.

Кроме этого, признано целесообразным среди активов Объекта выделить основной актив и вспомогательные активы (остальные из перечисленного выше списка)[11]. В данном случае возможны три варианта, когда основным активом Объекта является: 1) информация; 2) процесс Объекта или бизнес-процесс Организации; 3) человек, относящийся к персоналу организации в том числе имеющий отношение к функционированию Объекта.

Учитывая особенности Объекта и его активов, а также цели создания условий, которые обеспечат внутреннее состояние защищенности или устойчивости Объекта можно определить следующие основные варианты обеспечения безопасности Объекта: 1) обеспечение безопасности информации, относящейся к Объекту; 2) обеспечение устойчивости Объекта; 3) обеспечение безопасности человека как актива Объекта; 4) комплексное обеспечение безопасности Объекта. Данные направления будут рассмотрены отдельно.

2. Обеспечение безопасности информации, относящейся к объектам в информационной сфере

Информация как актив Объекта в соответствии с Федеральным законом №149-ФЗ[13] представляет собой *сведения (сообщения, данные) независимо от формы их представления*. Объект в информационной сфере – это объект, функционирование которого связано с обработкой информации (данных) с использованием современных информационных технологий (ИТ). Термин ИТ определяется как *процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов*[13].

Основным активом Объекта является информация, представленная в форме данных или сигнала различного происхождения (электрического, магнитного, электромагнитного). Остальные активы объекта можно рассматривать как вспомогательные или как активы, относящиеся к среде обработки информационного актива (РС БР ИББС-2.2-2009[14]). Структура активов Объекта представлена на рис. 2.

[13]Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
[14]Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечения ИБ организаций банковской системы РФ. Методика оценки рисков нарушения ИБ».

Учитывая особенности рассматриваемых объектов, обработка основного актива (ИА; например, данных) происходит в среде, к которой можно отнести активы среды обработки информационного актива (АСОИА), имеющей слоистую структуру, состоящую, например, из помещения, в котором находится объект (АСОИА-1), аппаратного обеспечения (АСОИА-2) и программного обеспечения (АСОИА-3). Причем эти слои (зоны) последовательно встроены друг в друга (рис. 2), а ИА (данные) находится в центре структуры.

При существовании источников угроз безопасности информации (опасностей) в ИСФ они могут находиться вне объекта (во внешней среде) и/или внутри отдельной зоны. Деструктивное воздействие опасности на ИА возможно при условии преодоления соответствующих границ (рубежей) между отдельными слоями. Успех такого воздействия будет зависеть от существования уязвимостей у АСОИА. Поэтому безопасность информации, относящейся к объектам в ИСФ, будет зависеть от результативности использования различных мер защиты на границах отдельных слоев АСОИА (обеспечение рубежной и эшелонированной защиты).

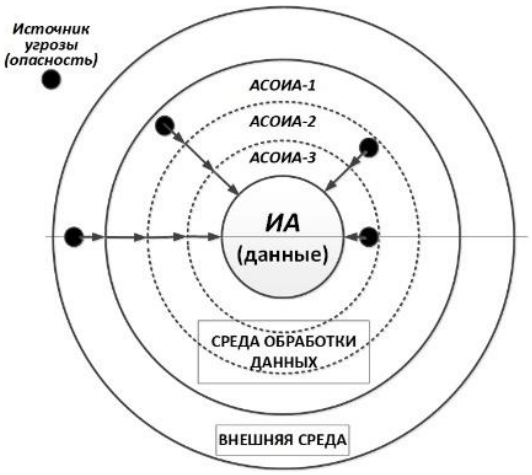

Рис. 2. Структура активов объекта в информационной сфере

Существует принятое на уровне национального стандарта ГОСТ Р 50922-2006[10] определение термина «безопасность информации (данных)» – это *состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.* Это определение не учитывает наличие Объекта, к которому относится информация (данные), и его особенности (наличие не только ИА, но и АСОИА со своими уязвимостями, а также характеристики возможных угроз безопасности информации.

В данной статье предлагается определение понятия «безопасность информации», учитывающее отмеченные выше факторы:

Безопасность информации (данных), относящейся (относящихся) к объекту в информационной сфере (БИ) *– это состояние защищенности активов объекта от угроз в информационной сфере при котором обеспечены у информации (данных) ее (их) конфиденциальность, доступность и целостность.*

Достичь требуемое состояние защищенности активов объекта (это значит обеспечить конфиденциальность, доступность и целостность информации (данных)) возможно при выполнении совокупности связанных действий или процессов. В этом случае представляется целесообразным ввести понятия «процесс обеспечения безопасности

информации» и понятие «обеспечение безопасности информации», имеющие следующие определения:

Процесс обеспечения безопасности информации (данных), относящейся (относящихся) к объектам в информационной сфере (Процесс ОБИ) *– это ряд мероприятий (действий), направленных на обеспечение безопасности информации (данных).*

Обеспечение безопасности информации (данных), относящейся (относящихся) к объекту в информационной сфере (ОБИ) *– это реализация совокупности взаимосвязанных и взаимодействующих процессов, направленных на обеспечение состояния защищенности активов объекта при котором обеспечены у информации (данных) ее (их) конфиденциальность, доступность и целостность.*

Используемый в данном случае процессный и системный подходы[4] предполагают разделение совокупности процессов ОБИ на две группы (процессы защиты информации (ПЗИ) и процессы управления защитой информации, а также их объединение в соответствующие системы (адаптированы из [1]):

Процессы ОБИ = Процессы ЗИ + Процессы УЗИ; СОБИ = СЗИ + СУЗИ.

Процесс защиты информации (данных), относящейся к объекту в информационной сфере (Процесс ЗИ) *– это ряд мероприятий (действий), направленных на обеспечение состояния защищенности активов объекта при котором обеспечены у информации (данных) ее (их) конфиденциальность, доступность и целостность.*

Процесс управления защитой информации (данных), относящейся к объекту в информационной сфере (Процесс УЗИ) *– это ряд мероприятий (действий), направленных на достижение полноты и качества обеспечения безопасности информации, и предназначенные для планирования, реализации, контроля и совершенствования процесса защиты информации.*

Система обеспечение безопасности информации (данных), относящейся (относящихся) к объектам в информационной сфере (СОБИ) *– это совокупность процессов обеспечения безопасности информации и мер, реализующих эти процессы, а также необходимых для этого ресурсов.*

Система защиты информации (данных), относящейся (относящихся) к объекту в информационной сфере (СЗИ) *– это совокупность процессов защиты информации и мер, реализующих эти процессы, а также необходимых для этого ресурсов.*

Система управления защитой информации (данных), относящейся (относящихся) к объектам в информационной сфере (СУЗИ) – это совокупность процессов управления защитой информации и мер, реализующих эти процессы, а также необходимых для этого ресурсов.

Следует обратить внимание на то, что такое разделение процессов и систем, относящихся к обеспечению безопасности информации, позволяет связать реализацию процессов ЗИ с непосредственным управлением рисками нарушения безопасности информации, а процессы управления защитой информации – с обеспечением качества (необходимой результативности) реализации процессов ЗИ.

Таким образом, рассмотренный в данной статье подход к обеспечению безопасности информации реализует процессный, системный и риск-ориентированный подходы, что согласуется с методологией обеспечения ИБ (группы стандартов ISO/IEC 27000 и ГОСТ Р ИСО/МЭК 27000).

3. Обеспечение устойчивости объектов в информационной сфере

В данном случае основным активом Объекта является процесс, реализуемый Объектом и/или бизнес-процесс Организации, частью которой является такой Объект. При этом перед владельцем Объекта (Организации) возникает принципиальная цель обеспечить определенное качество процесса, при котором реализация процесса Объекта и/или бизнес-процесса Организации осуществляется с сохранением определенных свойств этих процессов.

В настоящее время признаны следующие варианты обеспечения определенного качества процесса как основного актива Объекта и связанного с ним бизнес-процесса Организации:

1. Обеспечение непрерывности бизнеса (НБ). Под этим понимается стратегическая и тактическая способность Организации планировать свою работу в случае инцидента и нарушения ее деятельности, направленная на обеспечение непрерывности деловых операций на установленном приемлемом уровне[15].

2. Обеспечение готовности информационно-коммуникационных технологий (ИКТ) к обеспечению непрерывности бизнеса (ГИКТкОНБ), как способности организации поддерживать свои операции бизнеса путем предупреждения, обнаружения, реагирования на нарушения и восстановления услуг ИКТ[16]. В данном случае Объектом является часть Организации, использующая для обработки информации информационно-коммуникационные технологии. Причем обеспечение готовности Объекта качественно реализовывать процессы обработки информации непосредственно связывается с обеспечением непрерывности бизнес-процессов Организации.

3. Обеспечение функциональной устойчивости (ФУ) системы (Объекта, Организации). Под функциональной устойчивостью системы понимается ее свойство, характеризующее способность выполнять заданный перечень функций и задач системы в течение требуемого времени, в условиях воздействия на систему различных факторов [10, 11]. Причем система должна работать на гарантированное выполнение требуемого перечня функций и задач, своего предназначения, а также обеспечения отсутствия возникновения в системе конфликтов, обусловленных потребностями вышестоящей системы и невозможности выполнить эти потребности.

Решение проблемы обеспечения ФУ приобретает чрезвычайное значение для современных сложных технических систем (например, отнесенных к объектам критической информационной инфраструктуры), которые часто функционируют в условиях неопределенности их состояния и воздействующих на них факторов, которые могут приводить к снижению ФУ системы. Нарушение функционирования таких систем может привести к невозможности выполнения организацией, в интересах которых функционирует сложная техническая система, требуемого перечня функций и задач. Такие системы становятся критичными. На критичность влияет также развитие систем, появление у них и их элементов новых функций.

4.Обеспечение операционной надежности (ОН). В данном случае операционной надёжностью называют возможность отдельного технологического процесса или организации в целом непрерывно выполнять свою работу в условиях сбоев и иного негативного влияния (внешнего или внутреннего) [12]. Иными словами, это способность сохранять рабочие функции несмотря на какие-либо препятствия.

[15]ГОСТ Р ИСО 22301-2014 «Системы менеджмента непрерывности бизнеса. Общие требования».
[16]ГОСТ Р ИСО 27031-2012 «Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».

Данный подход получил свое развитие в финансовой сфере в отношении к некредитным финансовым организациям в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)[17] и в отношении к кредитным организациям в целях оказания банковских услуг[18]. На практике обеспечение ОН в той или иной мере реализуется в каждой финансовой организации. Нормативные документы Банка России[17, 18] только расширяют перечень требований к обработке и защите данных, а также добавляют меры к управлению ОН.

Анализ выделенных выше четырех направлений позволяет определить общие особенности деятельности, связанные с обеспечением необходимого уровня качества процессов как основных активов Объекта.

Во-первых, в рамках рассматриваемой в данной статье предметной области эти направления имеют отношение к действиям, направленным на Объект (как части Организации), функционирующий в ИСФ и использующий современные информационные технологии.

Во-вторых, Объекты имеют типовую структуру, в которой можно выделить определенные активы, среди которых к основным активам отнесены процессы, реализуемые Объектом и связанные с ними бизнес-процессы Организации.

В-третьих, действия, направленные на обеспечение НБ, ГИКТкОНБ, ФУ или ОН Объекта, связаны с формированием такого его состояния, при котором он будет способен противодействовать деструктивному воздействию опасностей в ИСФ на его активы путем сохранения свойств этих активов в заданных пределах или, если эти пределы будут нарушены, путем восстановления этих свойств в допустимый для этого интервал времени.

В-четвертых, методологическую основу обеспечения такого состояния у Объекта по всем четырем направлениям составляют процессный, системный, и риск-ориентированный подходы (ГОСТ Р ИСО/МЭК 27000-2021[4], ГОСТ Р 57580.1-2017[19])

Анализ выделенной выше третьей особенности позволяет не только сделать вывод, что понятия НБ, ГИКТкОНБ, ФУ и ОН являются частным случаем понятия «устойчивость», раскрытом в известном Толковом словаре[20] и используемом, например, в [6, 13], но и сформулировать определение понятия, которое представляет следующий термин:

Устойчивость объекта в информационной сфере *– это состояние (способность) объекта, при котором он сможет противодействовать деструктивному воздействию опасностей в информационной сфере на его активы путем сохранения свойств устойчивости этих активов в заданных пределах или, если эти пределы будут нарушены, восстанавливать эти свойства в допустимый для этого интервал времени.*

Важным понятием, входящим в вышеприведенное определение, является «свойства устойчивости актива», которые можно определить как качественные признаки (характеристики, показатели) и их количественные величины (адаптировано из [1]). Для

[17]Положение Банка России от 15.11.2021 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)».

[18]Положение Банка России от 12.01.2022 № 787-П “Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг”.

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

[20]Даль В. Толковый словарь живого великорусского языка: в 4 т. Т. 4. В. Даль. М.: Универс, 1994. – 1082 с.

определения устойчивости Объекта необходимо определить пороговые значения количественных величин качественных признаков.

В качестве примера приведем определение свойства устойчивости основного актива – процесса ИТ-сервиса, реализуемого Объектом: доступность процесса и его целостность.

В данном случае доступность процесса – это свойство быть готовым к реализации ИТ-сервиса по запросу клиента (авторизованного субъекта). Пороговым значением количественной величины этого свойства будет максимальное время ожидания начала реализации процесса.

Целостность процесса может быть определена как свойство сохранения правильности и полноты актива. Для реализации ИТ-сервиса важным является его производительность – достигнутый необходимый клиенту результат реализации процесса за определенный интервал времени. Пороговым значением количественной величины этого свойства будет максимальный допустимый интервал времени, в пределах которого ИТ-сервис будет реализован полностью.

Для того, чтобы обеспечить требуемое состояние объекта, которое характеризует его устойчивость, необходимо выполнить ряд связанных действий (процессов). В данном случае целесообразно определить следующие понятия (термины):

Процесс обеспечения устойчивости объекта в информационной сфере (Процесс ОУ) *– это ряд мероприятий (действий), направленных на обеспечение его устойчивости.*

Обеспечение устойчивости объекта в информационной сфере (ОУ) *– это реализация совокупности взаимосвязанных и взаимодействующих процессов, которые направлены на обеспечение такого состояния (способности) объекта, при котором он будет способен противодействовать деструктивному воздействию опасностей в информационной сфере на его активы путем сохранения свойств устойчивости этих активов в заданных пределах или, если эти пределы будут нарушены, восстанавливать эти свойства в допустимый для этого интервал времени.*

Используемый в данном случае процессный подход[10] предполагает разделение совокупности процессов обеспечения устойчивости на две группы: процессы обеспечения необходимых свойств устойчивости актива объекта (Процессы У) и процессы управления устойчивостью – Процессы УУ (адаптированы из [1, 4]):

Процессы ОУ = Процессы У + Процессы УУ.

Процесс устойчивости объекта в информационной сфере (Процесс У) *– это ряд мероприятий (действий), непосредственно направленных на обеспечение свойств устойчивости актива объекта;*

Процесс управления устойчивостью объекта в информационной сфере (Процесс УУ) *– это ряд мероприятий (действий), направленных на достижения полноты и качества обеспечения свойств устойчивости актива объекта, предназначенные для планирования, реализации, контроля и совершенствования процесса устойчивости объекта.*

Учитывая характер, процессов, относящихся к обеспечению устойчивости Объекта можно утверждать, что при решении практических задач обеспечения устойчивости, необходимо ориентироваться на системный подход, связанный объединением процессов ОУ, У и УУ в соответствующие системы ОУ, ПУ и УПУ (адаптировано из [1, 4]):

Система ОУ = Система ПУ + Система УПУ.

Система обеспечения устойчивости объекта в информационной сфере (Система ОУ) *– это совокупность процессов обеспечения устойчивости объекта и мер, реализующих эти процессы, а также необходимых для этого ресурсов;*

Система процессов устойчивости объекта в информационной сфере (Система ПУ) *– это совокупность процессов устойчивости объекта в информационной сфере и мер, реализующих эти процессы, а также необходимых для этого ресурсов;*

Система управления процессами устойчивостью объекта в информационной сфере (Система УПУ) *– это совокупность процессов управления процессами устойчивости объекта и мер, реализующих эти процессы, а также необходимых для этого ресурсов.*

Такое разделение процессов и систем, относящихся к обеспечению устойчивости Объекта, позволяет связать непосредственное обеспечение свойств устойчивости актива Объекта с управлением рисками нарушения устойчивости объекта, а процессы управления устойчивостью – с обеспечения качества (необходимой результативности) обеспечения устойчивости объекта в ИСФ.

Если сравнивать обеспечение устойчивости Объекта и обеспечение БИ у таких Объектов, то, несмотря на похожесть, можно выделить существенное различие, связанное с необходимостью адаптировать процессы управления устойчивостью к возможным изменениям условий реализации процессов Объекта и коррекции пороговых значений количественных величин свойств основного актива Объекта (процесса) и соответствующего пересмотра применения мер обеспечения его устойчивости. Такое положение поддерживает, например, существующее мнение о принципиальном различии направления, связанного с обеспечением киберустойчивости объектов и обеспечением информационной безопасности [2].

Необходимо отметить роль информационных активов Объекта при обеспечении его устойчивости в ИСФ. Информационные активы (ИА) Объекта, если нет отдельных требований по обеспечению БИ, должны рассматриваться как вспомогательные активы. В случае наличия деструктивного воздействия на ИА Объекта необходимо связать ущерб, нанесенный ИА с возможным в данном случае ущербом основному активу – процессу Объекта и далее с ущербом бизнес-процессу Организации. Если будет обнаружено нарушение устойчивости Объекта (или Организации), то необходимо предпринять шаги по обеспечению БИ, которые могли бы привести к обеспечению требуемой устойчивости Объекта. Это говорит о связи рассмотренного подхода к обеспечению устойчивости Объекта с подходом к обеспечению безопасности информации, относящейся к этому Объекту.

Аналогичная проблема может появиться в случае, когда возникает чрезвычайная ситуация, которая приводит к нарушению непрерывности обеспечения БИ на Объекте. Меры, которые должны быть реализованы для восстановления обеспечения БИ, должны быть применены в контексте с обеспечением устойчивости Объекта. В данном случае можно руководствоваться соответствующими рекомендациями по обеспечению непрерывности информационной безопасности (ГОСТ Р ИСО/МЭК 27001-2021[4]).

4. Обеспечение безопасности объекта в информационной сфере, если основным его активом является человек

Последствия деструктивного воздействия опасности на актив Объекта (рис. 1) определяются характером этого воздействия и особенностью актива Объекта, который в большинстве случаях является социотехнической системой [14, 15], состоящей из технической подсистемы, подсистемы персонала и внешней среды [15].

Техническая подсистема (ТПС) представляет собой совокупность программного обеспечения, аппаратных устройств, методов, конфигураций и процедур, применяемых пользователями системы для преобразования входных данных в выходные.

Социальная подсистема (СПС) включает в свой состав людей и организации, которые взаимодействуют с технической подсистемой. При этом неизбежно проявляются их уникальные социальные признаки.

Объект как объединение ТПС, СПС и обрабатываемой информации (данных), предполагает включение в перечень активов персонал (людей, взаимодействующих с ТПС и информацией).

Особенностью этого актива (человека) является принадлежность ему информации, представленной в первичной ее форме в виде определенных сведений. Причем совокупность этих сведений формирует уровень его знаний, оказывает влияние на формирование его убеждений, позиций по решению определенных задач, на поведение на работе и в быту, а также может оказывать влияние на его психику и в некоторых случаях на его здоровье. Все перечисленное здесь можно отнести к свойствам человека, которые могут оказать критическое влияние на выполнение им своих должностных обязанностей, от которых зависит результативность обеспечения безопасности информации, обрабатываемой Объектом, и результативность обеспечения устойчивости Объекта.

Возникает вопрос о виде деструктивного воздействия на этот актив (человека). Если исключить физические действия, то остается негативное информационное воздействие на уровень сведений, которыми обладает человек. Формой такого воздействия является манипуляция, которая может повлиять на поведение человека через психику, изменяя компоненты сознания [15], что может привести, например, к его целенаправленным действиям, связанным с нарушениями БИ, обрабатываемой в автоматизированной системе [16] или к нарушению устойчивости Объекта и Организации, частью которой является Объект.

При обеспечении безопасности Объекта и выделении в качестве его основного актива человека, актуальным является описание свойств этого актива, связанных с поведением человека в отношении Объекта, и определение их пороговых значений, вне которых можно ожидать при деструктивном воздействии опасностей на активы Объекта нанесение недопустимого ущерба активам Объекта, Объекту в целом и, как следствие, всей Организации.

Таким образом решение проблемы обеспечения безопасности Объекта, если основным его активом является человек, прежде всего связано с проведением исследования поведения человека при информационно-психологическом воздействии на него, что должно базироваться на таких предметных областях, как психология и физиология человека, а также социология. При этом необходимо учитывать факторы, которые определяются особенностями человека как актива Объекта для выработки решений, связанных с обеспечением безопасности Объекта. Это направление можно назвать обеспечением информационно-психологической безопасности человека как актива объекта в ИСФ. Специфика исследований и принимаемых при этом решений позволяет отнести это направление к отдельной предметной области, что предполагает наличие отдельного направления подготовки профессионалов. Актуальность решения этой проблемы была обоснована еще в 2005 г. в [17] в разделе 4.13. «Проблемы подготовки специалистов в сфере обеспечения информационно-психологической безопасности»

5. Комплексное обеспечение безопасности объекта в информационной сфере

Особенностью рассмотренных выше вариантов обеспечения безопасности (устойчивости) является то, что: они могут быть реализованы по отдельности или совместно. При этом необходимо отметить, что у них есть общая основа – это объект в

ИСФ, который может не быть (чаще так и считают на практике) или быть социотехническим.

Если среди активов Объекта нет человека, то возможно решение следующих задач (рис. 3):

А1. Обеспечение безопасности информации, относящейся к Объекту (информация – основной актив Объекта).

А2. Обеспечение устойчивости Объекта (процесс, реализуемый Объектом – основной актив Объекта) при отсутствии отдельных требований к обеспечению БИ (информация – вспомогательный актив Объекта).

А3. Обеспечение устойчивости Объекта, являющегося частью Организации в контексте обеспечения устойчивости Организации (процесс, реализуемый Объектом, и бизнес-процесс Организации – основные активы) при отсутствии отдельных требований к обеспечению БИ (информация – вспомогательный актив Объекта).

А4. Обеспечение устойчивости Объекта (процесс, реализуемый Объектом – основной актив Объекта) при наличии отдельных требований к обеспечению БИ (информация – основной актив Объекта).

А5. Обеспечение устойчивости Объекта, являющегося частью Организации в контексте обеспечения устойчивости Организации (процесс, реализуемый Объектом, и бизнес-процесс Организации – основные активы) при наличии отдельных требований к обеспечению БИ (информация – основной актив Объекта).

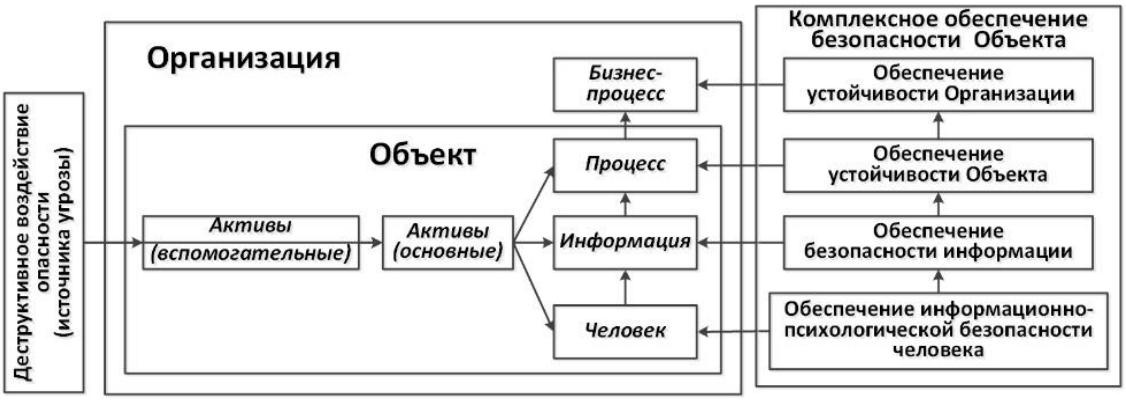

Рис. 3. Комплексное обеспечение безопасности объекта в информационной сфере

Если к основным или вспомогательным активам Объекта относится человек, то возможно решение следующих задач (рис. 3):

Б1. Обеспечение информационно-психологической безопасности (ИПБ) человека с учетом его свойств как основного актива Объекта.

Б2. Обеспечение безопасности информации, относящейся к Объекту с учетом обеспечения ИПБ человека как актива Объекта.

Б3. Обеспечение устойчивости Объекта (процесс, реализуемый Объектом – основной актив Объекта) при наличии отдельных требований к обеспечению БИ (информация – основной актив Объекта) с учетом обеспечения ИПБ человека как актива Объекта.

Б4. Обеспечение устойчивости Объекта, являющегося частью Организации в контексте обеспечения устойчивости Организации (процесс, реализуемый Объектом, и бизнес-процесс Организации – основные активы) при наличии отдельных требований к

обеспечению БИ (информация – основной актив Объекта) с учетом обеспечения ИПБ человека как актива Объекта.

Названные выше задачи могут быть рассмотрены как цели обеспечения безопасности (устойчивости) объекта в информационной сфере. Причем задачу (цель) будем считать комплексной, если к основным активам будут относиться информация и процессы без учета (варианты А4, А5) и с учетом (варианты Б3, Б4) человека в качестве актива Объекта.

Заключение

В данной статье определены основные проблемы, связанные с противоречивостью и несогласованностью таких понятий, как «защита информации», «информационная безопасность», «безопасность информации», «кибербезопасность» и «киберустойчивость», что привело к отсутствию в настоящее время принятой профессиональным сообществом единой системы понятий рассматриваемой предметной области.

Для преодоления этого недостатка предложено построить базовую систему понятий для предметной области «безопасность объектов в информационной сфере», основанную на учете особенностей объектов (использующих информационные технологии и осуществляющих обработку информации), на использовании понятия «информационная сфера» (как совокупность пространства таких объектов и среды их взаимодействия) и на понятии «актив» (части объекта, представляющей определенную ценность), который может быть основным и вспомогательным.

С учетом этих исходных данных выделенная предметная область обоснованно связана со следующими тремя отдельными системами понятий: «обеспечение безопасности информации объектов в информационной сфере», «обеспечение устойчивости объектов в информационной сфере» и «обеспечением информационно-психологической безопасности человека как актива объекта в информационной сфере».

Такое разделение оправдано тем, что эти три системы понятий будут иметь минимальное пересечение друг с другом. Следствием будет утверждение: сформулированы три отдельных направления подготовки профессионалов и три отдельных сферы их практической и научной деятельности, требующей наличия уникальных профессиональных компетенций.

Таким образом результаты работы также 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 ИБ. При этом необходимо сделать два важных замечания.

1. Определенные в работе названия трех систем понятий не содержат термин (понятие) «информационная безопасность», массовое использование которого началось с появлением документа высокого государственного уровня «Доктрина информационной безопасности РФ» и совпало с внедрением стандартов группы ГОСТ Р ИСО/МЭК 27000.

В целом складывается впечатление, что была допущена ошибка при переводе, редактировании и согласовании национальных стандартов этой группы, идентичных группе международных стандартов ISO/IEC 27000. Полагая, что термин «information security» можно перевести, как «информационная безопасность» (а не «безопасность информации», что было бы правильным), далее была выстроена терминосистема, основанная на этом понятии. Это оказало существенное влияние на формирование методологической базы обеспечения ИБ на государственном уровне (например, для ИБ организации[2]) или на корпоративном уровне (обеспечение ИБ организаций банковской системы РФ[3]), а также на

формирование укрупненного направления подготовки в системе высшего образования 10.00.00 «Информационная безопасность». Все это внесло определенную путаницу в понятийную базу области ИБ. Предложение трех отдельных систем понятий, сделанное в данной статье, направлено на исправление отмеченной выше ошибки.

2. Учитывая особенность названия третьей системы понятий, связанной с информационно-психологическим воздействием на человека, можно предложить вариант названия этой предметной области. Для этого отметим, что в настоящее время принято, если говорят о радиационной безопасности, то под эти понимают безопасность объектов от воздействия радиации; о пожарной безопасности – безопасность объектов от воздействия пожара и т.д. По этим образцам безопасность человека от воздействия информации можно назвать информационной безопасностью человека. Таким образом понятие и термин «информационная безопасность» предлагается оставить только для данной предметной области и исключить его использование с привязкой к любому объекту, кроме человека. В данном случае название третьей системы понятий (направления деятельности) может быть «обеспечением информационной безопасности социотехнических объектов в информационной сфере», которая будет связана с реализацией процессов, направленных на противодействие нанесению ущерба по трем направлениям: 1) человеку; 2) человеку и безопасности информации; 3) человеку и устойчивости объекта; 4) человеку, безопасности информации и устойчивости объекта. Профессионалам, которые должны принимать участие в этом, необходимо обладать не только профессиональными компетенциями в области обеспечения безопасности объектов в информационной сфере, но и специальными профессиональными компетенциями в области противодействия информационно-психологическому воздействию на человека, влияющего на его поведение. К сожалению, в настоящее время формирование таких компетенций не поддержано на уровне существующих направлений подготовки в системе профессионального образования России. Остается надеяться на то, что она будет решена в рамках идущей в настоящее время реформы профессионального образования.

СПИСОК ЛИТЕРАТУРЫ:

1. 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.
2. Зегжда Д.П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак. СПб.: ПОЛИТЕХ-ПРЕСС, 2022. – 490 с.
3. Малюк Анатолий А., Морозов Андрей В. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 21–36, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.02.
4. Толстой Александр И. Таксономия понятий в области кибербезопасности. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 158–175, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.10.
5. Милославская Наталья Г.; Толстая Светлана А. Угрозы нарушения кибербезопасности для организаций инфраструктуры финансовых рынков. Безопасность информационных технологий, [S.l.], т. 23, № 1, с. 115–126, 2016. ISSN 2074-7136. – EDN: WMWDGJ.
6. Гавдан Григорий П. и др. Устойчивость технологических процессов в аспекте 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.
7. 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.
8. Атаманов Г.А. О необходимости новой методологии информационной безопасности. URL: https://gatamanov.blogspot.com/2023/10/blog-post.html (дата обращения: 04.04.2024).

9. Опасность: суть термина, виды, классификация, признаки и дерево причин опасностей. URL: https://fireman.club/statyi-polzovateley/opasnost-sut-termina-vidyi-priznaki/ (дата обращения: 04.04.2024).
10. Остроумов О.А. Проблема обеспечения функциональной устойчивости систем критически важных объектов. Электросвязь. 2022, № 1, с. 14–18. DOI: 10.34832/ELSV.2022.26.1.005. – EDN: VGCBOP.
11. Лепешкин О.М., Остроумов О.А. Методология обеспечения функциональной устойчивости сложной технической системы. Труды Шестнадцатой международной конференция «Управление развитием крупномасштабных систем» (MLSD'2023). Россия, 26-28 сентября 2023 г. М.: ИПУ РАН, с. 197–201. DOI: 10.25728/mlsd.2023.
12. Чекудаев К.В. Операционная надёжность. Новые положения ЦБ РФ №779-П и №787-П. URL: https://rtmtech.ru/articles/operational-reliability/ (дата обращения: 04.04.2024).
13. Шотыло Д.М. Сущность и содержание устойчивости производственной системы. ЭКОНОМИНФО. 2006, № 6. URL: https://cyberleninka.ru/article/n/suschnost-i-soderzhanie-ustoychivosti-proizvodstvennoy-sistemy/viewer (дата обращения: 04.04.2024).
14. Кравченко Сергей. И. Безопасность социотехнических систем. НБИ технологии. 2018, т. 12, № 2, с. 20–24. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3.
15. Остапенко Г.А. Информационные операции и атаки в социотехнических системах: учеб. пособие для вузов. Г.А. Остапенко, Е.А. Мешкова; под общ. ред. В.Г. Кулакова. М.: Горячая линия-Телеком, 2016. – 208 с.
16. Дружилов С.А. Негативные воздействия современной информационной среды на человека: психологические аспекты. Психологические исследования. 2018, т. 11, № 59, с. 11. URL: http://psystudy.ru (дата обращения: 04.04.2024).
17. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Многотомная серия. Научный руководитель К.В. Фролов. Книга «Информационная безопасность, М: МГФ «Знание», ГЭИТИ, 2005. – 512 с.

REFERENCES:

[1] Tolstoy Alexandr I. Systematics of concepts in the field of information security. IT Security (Russia), [S.l.], v. 30, no. 1, p. 130-148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10 (in Russian).
[2] 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).
[3] Malyuk Anatoly A.; Morozov Andrey V. The formation of the digital economy and the problems of improving legal regulation in the field of information security. IT Security (Russia), [S.l.], v. 26, no. 4, p. 21–36, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.02 (in Russian).
[4] Tolstoy Alexander I. Cybersecurity concepts' taxonomy. IT Security (Russia), [S.l.], v. 31, no. 1, p. 158–175, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.10 (in Russian).
[5] 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 (in Russian). – EDN: WMWDGJ.
[6] 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).
[7] 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).
[8] Atamanov G.A. On the need for a new information security methodology. URL: https://gatamanov.blogspot.com/2023/10/blog-post.html (accessed: 04.04.2024).
[9] Danger: the essence of the term, types, classification, signs and tree of causes of hazards. URL: https://fireman.club/statyi-polzovateley/opasnost-sut-termina-vidyi-priznaki/ (accessed: 04.04.2024) (in Russian).
[10] Ostroumov O.A. The problem of ensuring the functional stability of systems of critical objects. Electrosvyaz. 2022, no. 1, p. 14–18. DOI: 10.34832/ELSV.2022.26.1.005 (in Russian). – EDN: VGCBOP.
[11] Lepeshkin O.M., Ostroumov O.A. Methodology for ensuring the functional stability of a complex technical system. Proceedings of the Sixteenth International Conference "Managing the Development of Large-Scale Systems" (MLSD'2023). Russia, September 26-28, 2023. M.: IPU RAS, p. 197–201. DOI: 10.25728/mlsd.2023 (in Russian).
[12] Chekudaev K.V. Operational reliability. New provisions of the Central Bank of the Russian Federation No. 779-P and No. 787-P. URL: https://rtmtech.ru/articles/operational-reliability/ (accessed: 04.04.2024) (in Russian).

[13] Shotylo D.M. The essence and content of the sustainability of the production system. EKONOMINFO. 2006, no. 6. URL: https://cyberleninka.ru/article/n/suschnost-i-soderzhanie-ustoychivosti-proizvodstvennoy-sistemy/viewer (accessed: 04.04.2024) (in Russian).
[14] Kravchenko Sergey I. The security of socio-technical systems. NBI technologies. 2018, v. 12, no. 2, p. 20–24. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3 (in Russian).
[15] Ostapenko G.A. Information operations and attacks in sociotechnical systems: textbook. manual for universities. G.A. Ostapenko, E.A. Meshkova; under general ed. V.G. Kulakova. M.: Hot Line-Telecom, 2016. – 208 p. (in Russian).
[16] Druzhilov S.A. Negative impacts of the modern information environment on humans: psychological aspects. Psychological Research. 2018, v. 11, no. 59, p. 11. URL: http://psystudy.ru (accessed: 04.04.2024) (in Russian).
[17] Security of Russia. Legal, socio-economic and scientific-technical aspects. Multi-volume series. Scientific supervisor K.V. Frolov. Book “Information Security, M: IGF “Knowledge”, GEITI, 2005. – 512 p. (in Russian).

Поступила в редакцию – 27 мая 2024 г. Окончательный вариант – 26 июля 2024 г.
Received – May 27, 2024. The final version – Jule 26, 2024.