Научная статья
УДК 004.56; DOI: 10.61260/2218-13X-2024-2-80-90

КОМПЛЕКСНАЯ ИНФОЛОГИЧЕСКАЯ МОДЕЛЬ ОБЪЕКТОВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

✉**Метельков Александр Николаевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***metelkov5178@mail.ru***

Аннотация. Проблема гармонизации подходов к определению объектов защиты информации приобретает все большую актуальность в связи с ростом информационных массивов, усложнением информационных технологий, технических и криптографических средств защиты информации, увеличивающимся числом компьютерных атак, в том числе на критическую информационную инфраструктуру. Исторически понятие объектов защиты в России связано с требованиями государственных регуляторов, поэтому оно имеет различные трактовки.

Целью исследования является разработка инфологической модели объектов защиты информации. Целеполаганием инфологического моделирования может быть обеспечение наиболее естественных для человека способов сбора и представления информации об объектах защиты для ее учета при создании систем защиты и хранения в базе данных. Автором на основе анализа требований основных регуляторов Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России и метода моделирования разработана инфологическая модель объектов защиты информации. Эта модель в наибольшей степени согласуется с концепцией объектно-ориентированного проектирования, которая является базовой для разработки сложных программных систем, освоения технологии проектирования баз данных объектов защиты информации, основанных на ER-модели. Модель «сущность-связь» (ER-модель) имеет несколько базовых понятий, из которых по заранее определенным правилам выстраиваются более сложные объекты.

Ключевые слова: инфологическая модель, информация, защита, объекты защиты, конфиденциальная информация

Для цитирования: Метельков А.Н. Комплексная инфологическая модель объектов защиты конфиденциальной информации // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 80–90. DOI: 10.61260/2218-13X-2024-2-80-90.

Scientific article

A COMPREHENSIVE INFOLOGICAL MODEL OF CONFIDENTIAL INFORMATION PROTECTION OBJECTS

✉**Metel'kov Alexander N.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***metelkov5178@mail.ru***

Abstract. The problem of harmonization of approaches to the definition of information security objects is becoming increasingly relevant due to the growth of information arrays, the complexity of information technologies, technical and cryptographic means of information protection, and the increasing number of computer attacks, including on critical information infrastructure. Historically, the concept of objects of protection in Russia is associated with the requirements of state regulators, so it has different interpretations.

The purpose of the study is to develop an infological model of information security objects. The goal of infological modeling may be to provide the most natural ways for a person to collect

and present information about objects of protection for its consideration when creating protection systems and storing in a database. The author based on the analysis of the requirements of the main regulators of the Federal service according to the technical and export control of Russia and the Federal security service of Russia and the modeling method, an infological model of information security objects has been developed. This model is most consistent with the concept of object-oriented design, which is the basis for the development of complex software systems, the development of technology for designing databases of information security objects based on the ER-model. The entity-relationship model (ER-model) has several basic concepts, from which more complex objects are built according to predefined rules.

Keywords: infological model, information, protection, protection objects, confidential information

For citation: Metel'kov A.N. A comprehensive infological model of confidential information protection objects // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 2. P. 80–90. DOI: 10.61260/2218-13X-2024-2-80-90.

Введение

Концепцией технологического развития на период до 2030 г. определены вызовы, принципы и цели технологического развития России. В приложении № 1 к Концепции приведен Предварительный перечень сквозных технологий (технологических направлений), включающий технологии обработки и передачи данных, искусственный интеллект, технологии хранения и анализа больших данных, технологии распределенных реестров, нейротехнологии, технологии виртуальной и дополненной реальностей, геоданные и геоинформационные технологии, технологии доверенного взаимодействия. Эти и другие технологии связаны с информацией, что предопределяет актуальность определения объектов защиты с целью обеспечения защиты данных путем обеспечения их конфиденциальности, целостности и доступности.

Построение инфологической модели объектов защиты

Для построения системы защиты информации нужно определиться с тем, что необходимо защищать, то есть с объектами защиты. Если нет четкого представления об объекте защиты, то и вся система защиты информации не будет устойчивой и безопасной.

Устойчивость системы автором понимается, как способность системы восстанавливать свое состояние, из которого она была выведена под влиянием возмущающего воздействия. Восстановление понимается как процесс и событие, отражающее переход объекта защиты из неработоспособного состояния в работоспособное. Безопасность информационной системы можно определить как свойство, заключающееся в способности системы обеспечить конфиденциальность, целостность и доступность информации, то есть состояние защищенности информации в такой системе от несанкционированного доступа, утечки информации по техническим каналам и деструктивных силовых воздействий.

Построение теоретической основы защищаемой информации и других элементов объекта защиты будет способствовать установлению взаимосвязей между самими объектами защиты информации и актуальными угрозами информационной безопасности, для нейтрализации которых необходимо принять контрмеры с применением соответствующих методов и средств.

Объекты защиты рассматриваются в системе обеспечения безопасности, описываемой в виде различных моделей (например, Хартсона, Белла и Ла Падулы, Кена Биба, LWM, Лендвера и др. [1–4]). Например, в системе Клементса-Хоффмана, модель с полным перекрытием множества угроз описывается в виде пяти кортежного набора [5]:

$$S = \{O, T, M, V, B\},$$

где обозначены наборы: O – объектов защиты; T – угроз безопасности информации; M – средств защиты; V – уязвимостей – отображение T×O на набор упорядоченных пар $v_i = (t_i, o_j)$, представляющих собой пути проникновения в систему; B – набор барьеров – отображение V×M или T×O×M на набор упорядоченных троек $b=(t_i, o_j, m_k)$, представляющих собой точки (участки, узлы), в которых следует осуществить защиту в системе; S – состояние системы обеспечения безопасности.

Объект защиты информации представляет собой один из главных элементов системы защиты информации, под которым в ГОСТ Р 50922–2006 понимается «информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации [6]. Семантический анализ приводит к предположению, что обслуживающий персонал и пользователи в понятие объект защиты информации компьютерных систем не включены. В работе [7] в концептуальной схеме процесса обеспечения информационной безопасности объект защиты выделен в числе других семи сущностей. При этом авторами защищаемая информация, информационная система, в которой обрабатывается защищаемая информация, и объект защиты считаются самостоятельными однопорядковыми сущностями.

В научной литературе предлагаются разные подходы к пониманию классификации и моделей объектов защиты. Понятие «объект защиты» или «объект» нередко трактуется в широком смысле. Для сосредоточенных компьютерных систем или элементов распределенных систем понятие «объект» включает в себя не только информационные ресурсы, аппаратные, программные средства, но и обслуживающий персонал и пользователей, помещения, здания, и прилегающую к зданиям территорию [8, с. 15; 9, с. 25]. В качестве примера можно привести классификацию, где выделяются следующие объекты:

– информация;

– ресурсные объекты (аппаратное и программное обеспечение, процессы и процедуры обработки информации);

– физические объекты (территории, помещения, здания, техническое оборудование, средства и каналы связи);

– пользовательские объекты (пользователи информации, субъекты информации, собственники информации, обслуживающий персонал) [10].

Информационное взаимодействие предполагает использование людьми технических и программных средств для обработки и преобразования информации в соответствии с информационной технологией, представления ее в виде информационных ресурсов и передачи по каналам связи. Исходя из таких рассуждений, в качестве объектов защиты выделяют «компьютеры, данные, каналы, информационные технологии» [10, с. 15]. Задачей формирования такой классификации было выявление и обоснование информационной технологии как отдельного объекта защиты. Конявская С.В. полагает, что «данные» являются общим для всех выделяемых объектов защиты:

– каналов (каналов передачи данных);

– информационных технологий (технологии обработки данных);

– компьютеров (средство, место хранения данных и их обработки; содержит и инструменты, и хранилища, и даже каналы передачи). В контексте данной классификации предлагается компьютер (или СВТ) заменить на «носитель» (средство хранения данных), чтобы избежать нарушения правила единого основания, обязательного для классификации. Из таких умозаключений и допущений получилась обобщенная классификация объектов защиты, относящихся к предмету защиты – «данным». Такая классификация включает носители (хранение), технологии (обработка) и каналы (передача). В процессе критического анализа такой модели автору представляется, что понятие «компьютер (СВТ)» как материальный объект и «носитель» – это разные понятия, которые отчасти совпадают в отдельных функциях, но в теоретических рассуждениях признать их тождественными

возможно лишь с большой долей условности. Под термином «носитель компьютерной информации» понимается «материальный объект, предназначенный для хранения компьютерной информации» [11]. В официальных документах регулятора термин «вычислительная машина (компьютер)» определяется как «СВТ, выполняющее некоторые функции без участия человека и функционирующее по заданной программе» [11]. В Кембриджском словаре под термином «компьютер (computer)» понимается электронная машина, которая используется для хранения, систематизации и поиска слов, цифр и изображений, для выполнения вычислений и для управления другими машинами [12]. Хранение является только одним из элементов жизненного цикла информации. Традиционность и узость представлений С.В. Конявской выражается в том, что автор разделяет сведения и данные (такой подход был характерен для 1970–1980-х гг. в ряде стран), сужает объем понятия «технологии», а СВТ – заведомо «нагружает» информацией, хранящейся в них. С такой трактовкой в настоящее время трудно согласиться. В устоявшихся представлениях «информация – сведения (сообщения, данные) независимо от формы их представления» [13], а СВТ как раз не содержат пользовательской (защищаемой) информации. В Концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, утвержденной решением Гостехкомиссии при Президенте Российской Федерации от 30 марта 1992 г., и ГОСТ Р 57429–2017 средство вычислительной техники (computer) определяется как «совокупность технических устройств и программ, обеспечивающих их функционирование, способных функционировать самостоятельно или в составе других систем» [14]. Рассматриваемая Концепция защиты предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от несанкционированного доступа к информации (НСД): направление, связанное с СВТ, и направление, связанное с автоматизированными системами (АС). Их отличие заключается в том, что СВТ разрабатываются как элементы, из которых строятся функционально ориентированные АС, и поэтому СВТ, не решая прикладных задач, не содержат защищаемой пользовательской информации. Кроме того, при создании АС возникают несвойственные для СВТ характеристики систем (например, полномочия пользователей, модель нарушителя, информационные технологии). В связи с этим, в случае СВТ, можно говорить лишь о защищенности СВТ от НСД к информации, для обработки, хранения и передачи которой оно предназначено, то есть о потенциальной защищенности [15, с. 52]. Информационные технологии, на взгляд автора, ошибочно сужать лишь до одной обработки. Они объединяют кроме обработки процессы, методы поиска, сбора, хранения, предоставления, распространения информации и способы осуществления таких процессов и методов. Информационные технологии – это совокупность методов, программно-технических и технологических средств. В состав информационных технологий входят методы передачи информации (например, канал связи, компьютерная сеть), поэтому нередко в научной литературе используется понятие информационно-коммуникационных технологий. Автором не разделяется точка зрения о том, что отдельно данные как самостоятельный объект защиты не имеют смысла, поскольку их защита оказывается возможной только при хранении, обработке или передаче. Иных состояний у данных, по взглядам С.В. Конявской, не существует.

Автором проанализированы и сопоставлены объекты защиты на примере нормативных правовых актов четырех государственных органов, которые представлены в таблице. Анализ объектов защиты приводит к следующим двум выводам, связанным с использованием понятий в сфере обеспечения информационной безопасности и защиты информации.

Во-первых, в нормативных правовых актах ряда государственных органов используется нечеткое понятие «программные средства», хотя в сфере технической защиты конфиденциальной информации в государственных информационных системах в качестве одного из основных объектов защиты Федеральной службой по техническому и экспортному

контролю России (ФСТЭК) указано общесистемное, прикладное, специальное программное обеспечение (ПО). Государственными и национальными стандартами Российской Федерации разъясняются определения, являющиеся аналогами термина «программа для ЭВМ», в частности, «программное средство». Термин «программа для ЭВМ» описывается в Гражданском кодексе Российской Федерации (ст. 1261). Согласно ГОСТ Р ИСО/МЭК 12207–2010 под программным продуктом понимается совокупность компьютерных программ, процедур и, возможно, связанных с ними документации и данных.

В Руководстве Р 50.1.056–2005 «Техническая защита информации. Основные термины и определения» под термином «защищаемые программные средства» понимаются программные средства, используемые в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности. Анализ терминов «программное обеспечение» и «программные средства» показывает их различие в объеме понятий. Программное средство определено в ГОСТ Р 51904–2002 как «ПО и связанные с ним документы, вновь созданные, модифицированные или сгруппированные для удовлетворения требований контракта» (п. 3.48), а ПО как «совокупность компьютерных программ и программных документов, необходимых для эксплуатации этих программ» (п. 3.47). В государственном стандарте ГОСТ 28806–90 программное средство (ПС; en software) определено иначе как объект, состоящий из программ, процедур, правил, а также, если предусмотрено, сопутствующими им документацией и данными, относящимися к функционированию системы обработки информации.

Автор при описании названий объектов защиты полагает необходимым придерживаться позиции ФСТЭК России, изложенной в Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17 (в ред. от 28 мая 2019 г.).

Таблица

Сравнительная таблица объектов защиты

«Порядок отнесения служебной информации к разряду ограниченного распространения…», утв. приказом Следственного комитета России от 23 декабря 2014 г. № 109 п. 26	Приложение № 4 к приказу Минюста Российской Федерации от 7 октября 2010 г. № 250 п. 3.	Приложение № 4 к приказу Минтранс России от 31 марта 2023 г. № 101 п. 2.	Приложение № 4 к приказу МЧС России от 14 октября 2019 г. № 581 п. 3
Защите подлежат			
Информационные ресурсы, содержащие сведения, отнесенные к служебной информации, в информационных системах и банках данных, а также в виде носителей на магнитной, оптической и бумажной основе;	Информационные ресурсы, содержащие сведения, отнесенные к служебной информации, в информационных системах и банках данных, а также в виде носителей на магнитной, оптической основе и бумажных носителях;	Информационные ресурсы, содержащие сведения, отнесенные к служебной информации ограниченного распространения, в информационных системах и банках данных, а также в виде носителей на магнитной, оптической основе и на бумажных носителях;	Информационные ресурсы, содержащие сведения, отнесенные к служебной информации ограниченного распространения; носители информации, содержащие служебную информацию ограниченного распространения, имеющиеся

ПС (операционные системы, системы управления банками данных и другое ПО), используемые в работе со служебной информацией	ПС (операционные системы, системы управления банками данных и другое ПО), используемые в работе со служебной информацией	ПС (операционные системы, системы управления банками данных и другое ПО), используемые в работе со служебной информацией	в распоряжении МЧС России, территориальных органов МЧС России и организаций, находящихся в его ведении; ПС, используемые для обработки служебной информации ограниченного распространения

Во-вторых, в одном случае (Следственный комитет Российской Федерации, Минюст России, Минтранс России) при раскрытии объекта защиты отмечено, что защите подлежат программные средства, используемых в работе со служебной информацией, а в другом (МЧС России) – суженный набор программных средств, используемы только для обработки служебной информации ограниченного распространения. Очевидно, что термины «служебная информация» и «служебная информация ограниченного распространения» по объему не совпадают. К служебной информации ограниченного распространения, как известно, не могут быть отнесены: сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов; решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке; сведения об исполнении бюджета и использовании других государственных ресурсов; документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан и др. Защита информации представляет собой принятие мер, направленных не только на соблюдение конфиденциальности информации, но ограниченного доступа на реализацию права на доступ к информации, на обеспечение защиты информации от уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении всей служебной информации.

Объект защиты информации, как правило, является сложным иерархическим объектом. Моделирование упрощает изучение сложных объектов и систем, особенно если их непосредственное исследование затруднено или невозможно [16]. Под моделью обычно понимают материальный или мысленно представляемый объект, который в процессе познания замещает объект – оригинал, сохраняя некоторые важные его черты. Каждый изучаемый процесс можно описать различными моделями, при этом ни одна модель не может сделать это абсолютно полно и всесторонне [17]. Фибан В., например, рассматривает модель «в качестве посредствующего звена между идеализированным объектом познания и изучаемым материальным объектом» [18]. Сопоставление модели с познаваемым объектом позволяет усовершенствовать ее. Во взаимодействии исследуемого объекта, его модели и идеализированного объекта происходит развитие научного познания.

Модель – это упрощенное представление реального объекта, системы или процесса, которое позволяет анализировать и понимать его свойства и взаимодействия. Объекты защиты информации в информационной системе, согласно требованиям ФСТЭК России, можно представить в виде различных групп (рис. 1).

Рис. 1. **Объекты защиты информации в информационной системе**

Инфологическая модель объектов защиты информации представляет собой обобщенное неформальное описание объектов защиты информации, выполненное с использованием естественного языка, таблиц и других средств, понятных лицам, осуществляющим меры защиты информации в информационных системах и информационно-телекоммуникационных сетях (рис. 2). Иными словами, инфологическая модель объектов защиты информации – обобщенное, схематичное описание предметной области.

С учетом требований государственных регуляторов ФСБ России и ФСТЭК России предлагается построить инфологическую модель объектов защиты информации. Инфологическая модель должна включать формализованное описание объектов защиты, которое будет понятно даже не специалистам в сфере информационной безопасности.

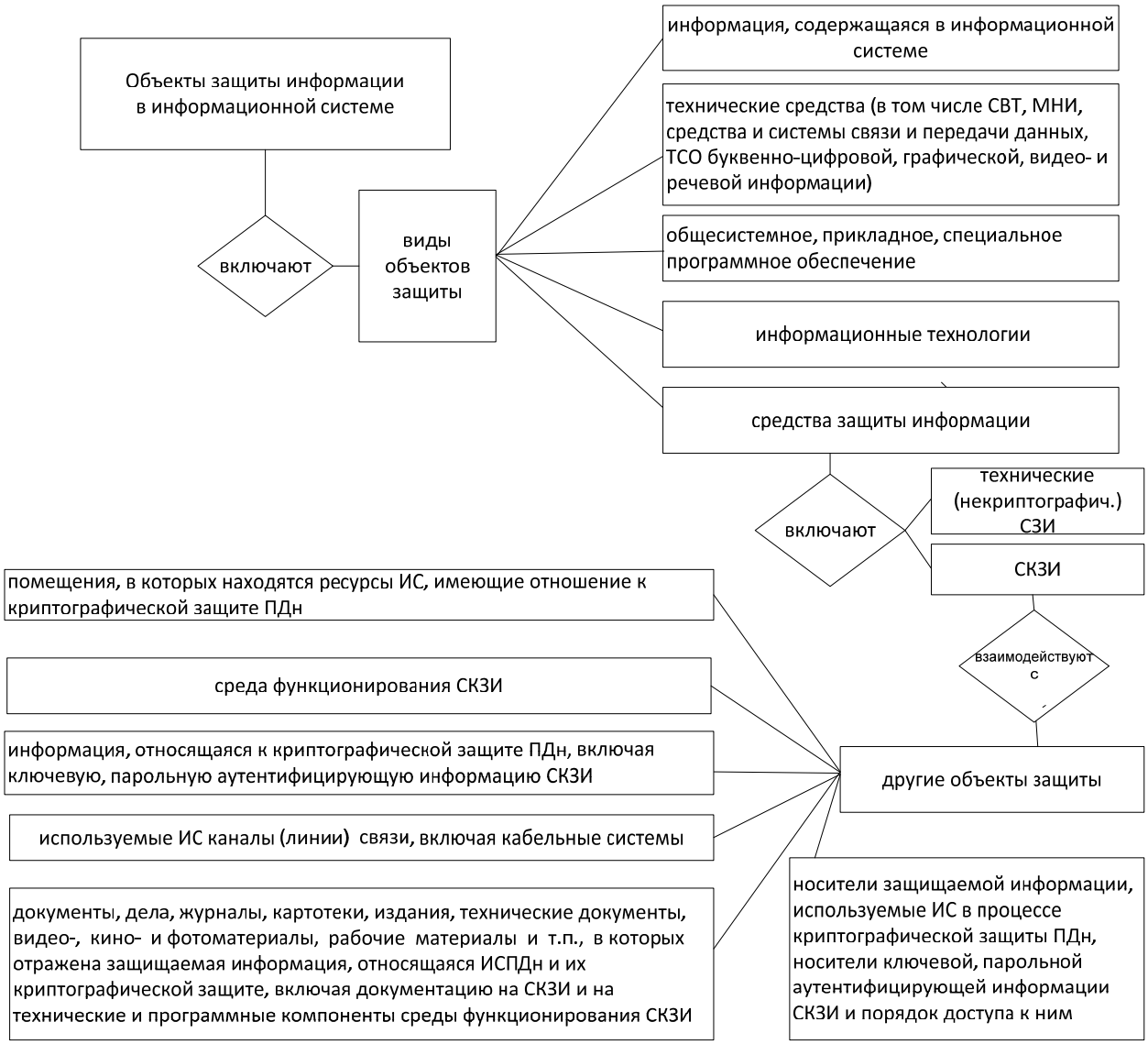

Рис. 2. **Комплексная инфологическая модель объектов защиты информации (используемые аббревиатуры: СВТ – средства вычислительной техники; МНИ – машинные носители информации; ТСО – технические средства отображения; СЗИ – средства защиты информации; СКЗИ – средства криптографической защиты; ПДн – персональные данные; ИСПДн – информационная система персональных данных)**

Заключение

Определение объектов защиты информации имеет не только теоретическое, но и практическое значение. Более ясное и конкретное выделение объектов защиты позволяет гармонизировать ведомственные подходы, экономить различные ресурсы (материальные, финансовые, людские, временные и др.) при разработке и внедрении организационных и технических мер защиты информации.

Данные об изучаемом объекте защиты информации, полученные благодаря модели, используются для дальнейшей разработки идеализированного объекта познания, что, в свою очередь, приводит к модификации модели. Модели используются для представления сложных явлений и помогают лучше понять их сущность.

Построение инфологической модели позволяет наглядно и более полно представить все объекты защиты и их основные взаимосвязи, что служит методологическим подходом

к выделению объектов защиты в информационных системах и информационно-телекоммуникационной структуре. Современные угрозы безопасности информации требуют не только обеспечения конфиденциальности сведений, но и не в меньшей степени целостности и доступности данных, что, в частности, в МЧС России требует защиты всего объема служебной информации.

Статья подготовлена в рамках выполнения в 2024 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России по тематике «Гармония».

Список источников

1. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.

2. Девянин П.Н. Обзорные лекции по моделям безопасности компьютерных систем // ПДМ. Приложение. 2009. № 2. С. 151–190.

3. Bell D.E., LaPadula L.J. Secure computer system: Unified exposition and multics interpretation. MITRE CORP BEDFORD MA, 1976.

4. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in operating systems // Commun. ACM. 1976. № 19. С. 461–471.

5. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса-Хоффмана: научное издание // Вестн. Брянск. гос. техн. ун-та. 2008. № 1. С. 61–66.

6. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008.

7. Концептуальная схема обеспечения информационной безопасности в типовом объекте защиты / Г.А. Попов [и др.] // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2017. № 4. С. 45–53.

8. Завгородний В.И. Комплексная защита информации в компьютерных системах: учеб. пособие. М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. 264 с.

9. Сухостат В.В., Васильева И.Н. Основы информационной безопасности: учеб. пособие. СПб.: Изд-во СПбГЭУ, 2019. 103 с.

10. Конявская С.В. К вопросу о классификации объектов защиты информации к вопросу о классификации объектов защиты информации // Безопасность информационных технологий. 2013. Т. 20. № 3. С. 14–18.

11. Компьютерная экспертиза. Термины и определения: Стандарт СТО.ФСБ.КК 1-2018 (утв. Директором ФСБ России 12 нояб. 2018 г. № 33) // ФСБ России. URL: http://www.fsb.ru/fsb/npd/more.htm%21id%3D10437602%40fsbNpa.html (дата обращения: 05.04.2024).

12. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/computer (дата обращения: 27.12.2023).

13. Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 12 дек. 2023 г.) // Собр. законодательства Рос. Федерации. 2006. № 31 (Ч. I). Ст. 3448.

14. Концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утв. решением Государственной технической комиссии при Президенте Рос. Федерации от 30 марта 1992 г.). URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2 (дата обращения: 28.12.2023).

15. Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем. 1998. 158 с.

16. Исенко А.И. Понятия модели и моделирования в человеческой деятельности // Концепт. 2015. № 4. С. 31–35.

17. Звонарев С.В. Основы математического моделирования: учеб. пособие. Екатеринбург: Изд-во Урал. ун-та, 2019. 112 с.

18. Фибан В. Моделирование в биологии / отв. ред. Г. Гёрц, М.Э. Омельяновский // Эксперимент. Модель. Теория: сб. статей М.; Берлин: Наука, 1982. 333 с.

References

1. Gajdamakin N.A. Razgranichenie dostupa k informacii v komp'yuternyh sistemah. Ekaterinburg: Izd-vo Ural. un-ta, 2003. 328 s.

2. Devyanin P.N. Obzornye lekcii po modelyam bezopasnosti komp'yuternyh sistem // PDM. Prilozhenie. 2009. № 2. S. 151–190.

3. Bell D.E., LaPadula L.J. Secure computer system: Unified exposition and multics interpretation. MITRE CORP BEDFORD MA, 1976.

4. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in operating systems // Commun. ACM. 1976. № 19. S. 461–471.

5. Averchenkov V.I., Rytov M.Yu., Gajnulin T.R. Optimizaciya vybora sostava sredstv inzhenerno-tekhnicheskoj zashchity informacii na osnove modeli Klementsa-Hoffmana: nauchnoe izdanie // Vestn. Bryansk. gos. tekhn. un-ta. 2008. № 1. S. 61–66.

6. GOST R 50922–2006. Zashchita informacii. Osnovnye terminy i opredeleniya. M.: Standartinform, 2008.

7. Konceptual'naya skhema obespecheniya informacionnoj bezopasnosti v tipovom ob"ekte zashchity / G.A. Popov [i dr.] // Vestnik AGTU. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika. 2017. № 4. S. 45–53.

8. Zavgorodnij V.I. Kompleksnaya zashchita informacii v komp'yuternyh sistemah: ucheb. posobie. M.: Logos; PBOYUL N.A. Egorov, 2001. 264 s.

9. Suhostat V.V., Vasil'eva I.N. Osnovy informacionnoj bezopasnosti: ucheb. posobie. SPb.: Izd-vo SPbGEU, 2019. 103 s.

10. Konyavskaya S.V. K voprosu o klassifikacii ob"ektov zashchity informacii k voprosu o klassifikacii ob"ektov zashchity informacii // Bezopasnost' informacionnyh tekhnologij. 2013. T. 20. № 3. S. 14–18.

11. Komp'yuternaya ekspertiza. Terminy i opredeleniya: Standart STO.FSB.KK 1-2018 (utv. Direktorom FSB Rossii 12 noyab. 2018 g. № 33) // FSB Rossii. URL: http://www.fsb.ru/fsb/npd/more.htm%21id%3D10437602%40fsbNpa.html (data obrashcheniya: 05.04.2024).

12. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/computer (data obrashcheniya: 27.12.2023).

13. Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii: Feder. zakon ot 27 iyulya 2006 g. № 149-FZ (v red. ot 12 dek. 2023 g.) // Sobr. zakonodatel'stva Ros. Federacii. 2006. № 31 (Ch. I). St. 3448.

14. Koncepcii zashchity sredstv vychislitel'noj tekhniki i avtomatizirovannyh sistem ot nesankcionirovannogo dostupa k informacii (utv. resheniem Gosudarstvennoj tekhnicheskoj komissii pri Prezidente Ros. Federacii ot 30 marta 1992 g.). URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2 (data obrashcheniya: 28.12.2023).

15. Kotuhov M.M., Markov A.S. Zakonodatel'no-pravovoe i organizacionno-tekhnicheskoe obespechenie informacionnoj bezopasnosti avtomatizirovannyh sistem. 1998. 158 s.

16. Isenko A.I. Ponyatiya modeli i modelirovaniya v chelovecheskoj deyatel'nosti // Koncept. 2015. № 4. S. 31–35.

17. Zvonarev S.V. Osnovy matematicheskogo modelirovaniya: ucheb. posobie. Ekaterinburg: Izd-vo Ural. un-ta, 2019. 112 s.

18. Fiban V. Modelirovanie v biologii / otv. red. G. Gyorc, M.E. Omel'yanovskij // Eksperiment. Model'. Teoriya: sb. Statej. M.; Berlin: Nauka, 1982. 333 s.

Информация о статье:
Статья поступила в редакцию: 08.02.2024; одобрена после рецензирования: 22.04.2024;
принята к публикации: 06.05.2024
Information about the article:
The article was submitted to the editorial office: 08.02.2024; approved after review: 22.04.2024;
accepted for publication: 06.05.2024

Сведения об авторах:
Метельков Александр Николаевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат юридических наук, e-mail: metelkov5178@mail.ru, https://orcid.org/0000-0002-6113-8981, SPIN-код: 5990-6833

Information about the authors:
Metelkov Alexander N., associate professor of the department of applied mathematics and information technologies, Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of law, e-mail: metelkov5178@mail.ru, https: //orcid.org/0000-0002-6113-8981, SPIN: 5990-6833