Аналитическая статья
УДК 004.056; DOI: 10.61260/2218-13X-2023-3-84-94

ОБРАЩЕНИЕ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ В МЧС РОССИИ: ГАРМОНИЗАЦИЯ ТЕРМИНОЛОГИИ

✉Метельков Александр Николаевич;
Уткин Олег Валерьевич.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉metelkov5178@mail.ru

Аннотация. Целью статьи является исследование логической и сематической точности применения технических терминов в организационно-правовых и организационно-распорядительных документах МЧС России по защите служебной информации, упорядочение отдельных терминов сферы информационной безопасности. Формирование понятийного аппарата в области информационной безопасности выделено в качестве общеметологической проблемы информационной безопасности. Определение ведомственной терминологии и ее гармонизация с общими подходами позволяет повысить защищённость информации. Исследовано содержание цели защиты информации ограниченного распространения и предложено уточнить его в руководящем документе МЧС России. Рассматриваются понятия термина «носитель информации», обзорно раскрыты типы носителей. Актуальность исследования обусловлена тем, что ввиду интернационализации образования терминосистемы образовательной сферы русского и английского языков на сегодняшний день нуждаются в гармонизации. В результате сравнения с аналогичными документами других государственных органов и анализа содержания терминов выявлены несоответствия терминологии, применяемой в отдельных ведомственных документах по организации защиты информации конфиденциального характера. Установлены расхождения в целях защиты такой информации между нормами федерального законодательства и ведомственным порядком обращения со служебной информацией ограниченного распространения.

Ключевые слова: терминология, служебная информация, ограниченное распространение, доступ, защита

Для цитирования: Метельков А.Н., Уткин О.В. Обращение со служебной информацией в МЧС России: гармонизация терминологии // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 3. С. 84–94. DOI: 10.61260/2218-13X-2023-3-84-94.

Analytical article

HANDLING WITH OFFICE INFORMATION TO OF EMERCOM OF RUSSIA: HARMONIZATION OF TERMINOLOGY

✉Metelkov Alexander N.;
Utkin Oleg V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉metelkov5178@mail.ru

Abstract. The purpose of the article is to study the logical and sematic accuracy of the use of technical terms in the organizational, legal and organizational and administrative documents of EMERCOM of Russia for the protection of service information, streamlining individual terms in the field of information security. The formation of the conceptual apparatus in the field of information security is singled out as a general methodological problem of information security. The definition of departmental terminology and its harmonization with common approaches allows increasing the security of information. The content of the goal of protecting information of limited distribution is studied and it is proposed to clarify it in the

governing document of EMERCOM of Russia. Deals with the concepts of the term information carrier, the types of carriers are reviewed. The relevance of the study is due to the fact that, in view of the internationalization of education, the terminological system of the educational sphere of the russian and english languages today needs to be harmonized. As a result of comparison with similar documents of other state bodies and analysis of the content of terms, inconsistencies in the terminology used in individual departmental documents on the organization of the protection of confidential information were revealed. In order to protect such information, discrepancies have been established between the norms of federal legislation and the departmental procedure for handling proprietary information of limited distribution.

Keywords: terminology, proprietary information, limited distribution, access, protection

For citation: Metelkov A.N., Utkin O.V. Handling with office information to of EMERCOM of Russia: harmonization of terminology // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 3. P. C. 84–94. DOI: 10.61260/2218-13X-2023-3-84-94.

Введение

В числе актуальных вопросов находится разрешение правовой неопределенности понятия электронного носителя информации как источника информации [1, с. 5]. Стандарт ИСО 860: 2007 регламентирует терминологическую деятельность, различая гармонизацию понятий и гармонизацию терминов. Недостатки правовой и технической регламентации терминов, раскрывающих содержание обработки информации на электронных носителях, отражаются на правильности сбора оперативной информации. Терминологическая ясность позволяет на практике более точно реализовывать требования государственных регуляторов по защиты информации и обеспечению информационной безопасности.

Терминологическая ясность как метод совершенствования защиты служебной информации

Служебная информация ограниченного распространения – составное понятие, включающее два компонента несекретной информации [2]. В МЧС России к этому виду информации относится несекретная информация, касающаяся деятельности МЧС России, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в МЧС России несекретная информация, доступ к которой ограничен в соответствии с федеральными законами. В то же время в одном из нормативных правовых актов МЧС России для обеспечения защиты установлена тождественность конфиденциальной информации и служебной информации, содержащей сведения ограниченного распространения. Целесообразность такого методологического подхода, на взгляд авторов, вызывает сомнения в виду отсутствия легального определения термина «конфиденциальная информация» и может дезориентировать деятельность при выделении защищаемой несекретной информации, установления соотношения между служебной.

Общий порядок обращения с документами и другими материальными носителями ограниченного распространения (фото-, кино-, видео- и аудиопленки, машинные носители информации и др.) (п. 1.1) определен в Положении, утвержденном постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233. Вопросы организации защиты такой информации определены в Приложении № 4 к приказу МЧС России от 14 октября 2019 г. № 581 «О порядке обращения со служебной информацией ограниченного распространения в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий». Приложение не лишено существенных терминологических недостатков, которые не способствуют правильному пониманию некоторых аспектов защиты служебной информации. В Приложении № 4 (Организация защиты служебной информации

ограниченного распространения), как показывают результаты проведенного анализа и сравнения с положениями ч. 1 ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», цели защиты информации отражены фрагментарно, недостаточно полно и ясно. Во-первых, в Приложении № 4 говорится о соблюдении конфиденциальности информации ограниченного распространения, а в законе – об информации ограниченного доступа, то есть о возможности получения информации и ее использовании. В обязательных Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17), устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в том числе от блокирования доступа к ней при обработке указанной информации в государственных информационных системах. Блокирование доступа в ГОСТ Р 53114–2008 рассматривается как прекращение или затруднение доступа к информации законных пользователей. Информация ограниченного доступа охватывает как сведения, отнесенные к государственной тайне, так и сведения конфиденциального характера [3].

Следует подчеркнуть, что Перечень сведений конфиденциального характера определен в Указе Президента Российской Федерации от 6 марта 1997 г. № 188 [4]. Данный Перечень содержит семь групп такой информации, включая:

– персональные данные;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии федеральными законами;

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.

Требования к защите информации могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в п. 1 и 3 ч. 1 ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации».

Во-вторых, вряд ли положение Приложения № 4 об обеспечении полноты, целостности и достоверности служебной информации ограниченного распространения в системах подготовки, учета, хранения и обработки данных и документов по смыслу и объему соответствует законодательному положению об обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации. В стандарте ГОСТ Р 50922-20062.4.2 цель защиты информации – это заранее намеченный результат защиты информации (например, результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на нее). Неправомерным становится доступ, который осуществляется без разрешения ее законного владельца и в нарушение определенного законодательством порядка. «Владелец может установить ограничения доступа посредством правовых, организационных, технических мер» [5, с. 163]. В-третьих, целями защиты служебной информации в МЧС России определено предотвращение неправомерного (случайного) доступа неуполномоченных должностных лиц к служебной информации ограниченного распространения. В приведенное положение не вписывается такой смоделированный случай, который может иметь место в действительности. Например, сотрудники сторонней организации в ходе ремонта или аудита информационной безопасности, действуя строго по инструкции и внутренним документам, при выполнении предусмотренных программой ремонта или испытаний случайно ознакомились с содержанием неочищенных носителей, на которых была записана конфиденциальная информация. При этом действовали они правоверно и имели полномочия на ремонт или исследования. Сравнение рассматриваемых

положений с похожими нормами документов других государственных органов показывает, что в руководящих документах ряда министерств и ведомств (например, Минюста России, Следственного комитета России, Федерального агентства связи и др.) целями защиты является не только предотвращение неправомерного или случайного доступа к служебной информации, но и, что наиболее важно, предотвращение утечки, хищения служебной информации по техническим каналам, а также несанкционированного уничтожения, искажения, подделки, копирования, распространения, блокирования служебной информации в системах информатизации. Такой подход точнее отражает заранее намеченный результат защиты информации и реализацию законодательных норм.

Средства электронно-вычислительной техники (ЭВТ) включают в себя средства сбора, обработки, регистрации, отображения информации и передачи данных. Они обеспечивают хранение, переработку и документирование информации [6]. В качестве видов внутренней памяти специалисты выделяют оперативную, постоянную, полупостоянную, кэш-память и видеопамять [7, с. 260]. Основным элементом средств ЭВТ являются электронно-вычислительные машины, которые обеспечивают накопление, хранение и автоматическую обработку данных, циркулирующих в автоматизированных системах (АС). Техническую основу АС также составляют средства оргтехники, средства обеспечения и контрольно-диагностические средства, обеспечивающие нормальное функционирование технических средств в требуемых режимах. К средствам оргтехники относятся аппараты факсимильной связи, электронные печатающие устройства, устройства размножения, проекционные установки, редакционно-издательское и другое оборудование обработки документов. Для защиты информации важным является рассмотрение вопроса защиты носителей, содержащих служебную информацию ограниченного распространения. Поэтому вопрос о защите носителей информации имеет практическое значение. Рассмотрим его подробнее с учетом анализа ведомственной терминологии. В государственных информационных системах, в том числе МЧС России, применяются различные типы сертифицированных носителей информации, которые как и информация, и информационный процесс являются объектом защиты информации.

Широкое распространение получили съемные и несъёмные носители на магнитной, оптической и бумажной основе. Носители данных имеют разную емкость и скорость. К ним относятся кэш-память, динамическая оперативная память (DRAM) или основная память; магнитная лента и магнитный диск; оптические диски, такие как CD, DVD и Blu-Ray диски; флэш-память и различные итерации встроенной памяти. Происходит быстрая эволюция аппаратных технологий хранения данных, включая NVM с байтовой адресацией (Intel Optane DCPMM), твердотельные накопители со сверхнизкой задержкой (Intel Optane SSD, Samsung ZSSD), твердотельные накопители NVMe с более быстрыми соединениями PCIe (Gen 4 и Gen 5), и расширение постоянной памяти на основе CXL [8, с. 589].

К современным устройствам хранения относят твердотельные накопители на основе флэш-памяти (Solid State Drives), память на основе фазового перехода (PCM) и 3D Xpoint [9], а также магниторезистивную память MRAM (Magnetoresistive Random Access Memory). Эти устройства имеют ряд преимуществ по сравнению с классическими жесткими дисками, например, более низкое энергопотребление и более быстрое чтение и запись. Эти устройства имеют ряд преимуществ по сравнению с классическими жесткими дисками, например, более низкое энергопотребление и более быстрое чтение и запись. К основным типам носителей информации, используемых сегодня, относятся: жесткие диски (HDD), твердотельные накопители, оптические хранения и ленты. Жесткие диски широко используются для хранения в персональных компьютерах, серверах и корпоративных хранилищах систем, а твердотельные накопители уже достигают производительности и паритета цены с диском [10, с. 237]. Оптическое хранение данных популярно в потребительских товарах, таких как компьютерные игры и фильмы, а также используется в системах архивирования данных большой емкости.

Что такое носитель информации? В компьютерах носитель данных – это обычно физическое устройство, которое получает и сохраняет электронные данные для приложений и пользователей и делает данные доступными для поиска. В эпоху цифровой трансформации и стремительного развития информационных технологий носители информации также быстро видоизменяются. Носитель данных может находиться внутри компьютера или другого устройства или быть подключенным к системе извне (съемный носитель информации, сменный носитель информации), напрямую или по сети. Любой носитель, такой как диск или лента, на котором могут храниться машиночитаемые данные. Ранние формы носителей информации включали компьютерную бумажную ленту с пробитыми в ней отверстиями. Каждая дыра соответствовала одному биту данных. Перфокарты также широко использовались на заре хранения данных и когда-то хранили большую часть мировой цифровой информации. Бумажная лента и перфокарты были вытеснены магнитной лентой, которая со временем уступила место магнитным гибким дискам. Жесткие диски (HDD) и твердотельные накопители (SSD) в настоящее время являются основными формами хранения. Наиболее доступными твердотельными накопителями являются одноуровневая ячейка (SLC), многоуровневая ячейка (MLC), трехуровневая ячейка (TLC). Носители, используемые в компьютерном хранилище, получают сообщения в виде данных с помощью программных команд от хост-системы. Тип носителя, необходимого для хранения данных, зависит от ценности данных для решения практических задач, применимых нормативных требований, требований к производительности и доступности и других факторов.

Понятие носитель информации не имеет легального определения. Носителем информации может быть любой материальный объект, в том числе физическое поле, в котором информация отображается в виде символов, образов, явлений или, например, технических решений и процессов. С созданием электронно-вычислительных машин появилась компьютерная информация. Сегодня широкое распространение получили электронные носители информации. К электронным носителям данных относятся, например, USB-накопители, чип-карты, твердотельные жесткие диски, флэш-память смартфонов и планшетных персональных компьютеров, карты памяти цифровых фотоаппаратов. Эти носители данных также подпадают под действие стандарта ISO/IEC 21964 (DIN 66399), в котором носитель информации определен как объект или элемент, содержащий данные. Это означает, что персональные данные на этих носителях должны быть уничтожены в соответствии с правилами защиты данных. Содержание термина проявляется в некоторых федеральных законах, из текста которых следует, что к видам носителей информации относятся материалы фото- и киносъемки, аудио- и видеозаписи, бумажные и машинные носители. Расширенное определение носителя информации содержится в п. 2.5.3 ГОСТ Р 50922–2006. В стандарте носитель защищаемой информации определяется весьма широко как физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [11]. Схожее определение содержалось в выписке из Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 15 февраля 2008 г. Носитель информации, согласно этой модели, – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин. Согласно ГОСТ Р 7.0.8–2013 носитель документированной информации – это «материальный объект, предназначенный для закрепления, хранения (и воспроизведения) речевой, звуковой или изобразительной информации» [12].

Термин «носитель данных» может относиться к устройству хранения в целом или к отдельному компоненту, которые используются вместе с другой системой или является ее частью. Например, внутренние жесткие диски и твердотельные накопители в компьютерах обычно называются носителями данных, как и компакт-диски, но сам дисковод компакт-

дисков рассматривается как устройство хранения или система, а не как носитель данных. Носители, используемые в компьютерном хранилище, получают сообщения в виде данных с помощью программных команд от хост-системы. Тип носителя, необходимого для хранения данных, зависит от ценности данных для реализации технологического процесса, применимых нормативных требований, требований к производительности и доступности, других факторов.

Носитель данных может быть внутренним для вычислительного устройства, такого как твердотельный накопитель компьютера, или съемным устройством, таким как внешний жесткий диск или флэш-накопитель с универсальной последовательной шиной (USB). Существуют также другие типы носителей информации, включая магнитную ленту, компакт-диски (CD) и карты энергонезависимой памяти (NVM).

Хранилище организации часто классифицируется как первичное и вторичное. Первоначально основное хранилище относилось к данным, которые хранятся в памяти для быстрого извлечения процессором компьютера, а вторичное хранилище относилось к данным, хранящимся на энергонезависимых устройствах, таких как твердотельные накопители и жесткие диски.

В последнее время первичное хранилище стало обозначать любой тип памяти, который поддерживает повседневные рабочие нагрузки организации. Например, жесткие диски, твердотельные накопители или устройства памяти класса хранения (SCM), которые хранят данные для критически важных приложений, считаются основным хранилищем. Напротив, вторичное хранилище может относиться практически ко всему, включая оптические диски или ленточные системы, поддерживающие долгосрочное хранение данных.

В многоуровневых хранилищах используются автоматизированные программные политики для перемещения данных между различными типами хранилищ, такими как жесткие диски, твердотельные накопители и облачные платформы.

Термин «носитель данных» может относиться к устройству хранения в целом или к отдельному компоненту, который используется вместе с другой системой или является ее частью. Например, внутренние жесткие диски и твердотельные накопители в компьютерах обычно называются носителями данных, как и компакт-диски, но сам дисковод компакт-дисков рассматривается как устройство хранения или система, а не как носитель данных. Точно так же массив представляет собой полную систему хранения, состоящую из отдельных носителей данных. Массив часто отделен от сервера приложений и подключен к отдельному серверу, доступ к которому осуществляется через сеть. Массив может состоять из жестких дисков или твердотельных накопителей или может быть настроен в гибридной конфигурации, которая объединяет жесткие диски и твердотельные накопители в интегрированную систему, при этом жесткие диски обеспечивают уровень емкости, поддерживающий более быстрые твердотельные накопители.

Носители информации бывают разных форм: жесткие диски, флэш-память, твердотельные накопители или устройства памяти класса хранения (SCM), которые хранят данные для критически важных приложений, считаются основными типами первичной (оперативной) памяти. Классификация носителей информации представлена на рисунке. В качестве иной физической основы могут, например, использоваться фотографические носители. В некоторых жестких дисках используется односкатная магнитная запись (SMR) в качестве альтернативы обычной магнитной записи.

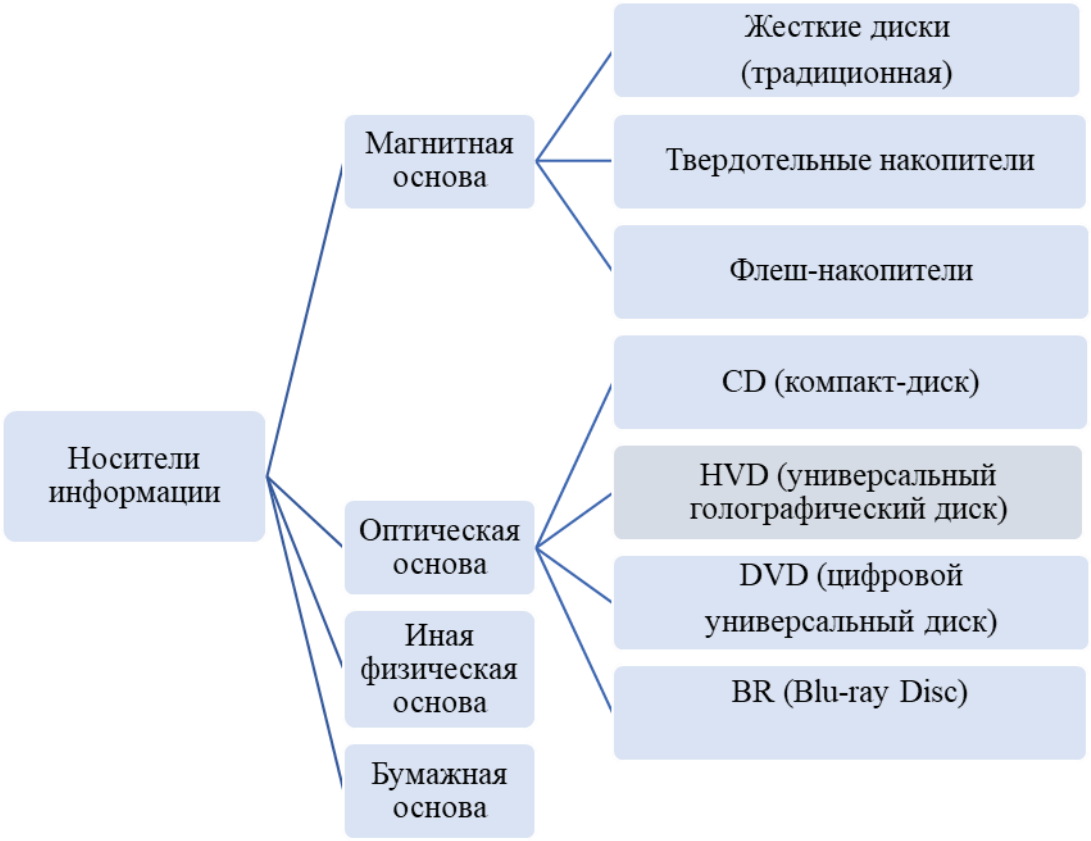

Рис. **Классификация носителей информации**

Ведущими производителями дисков на базе SMR являются Seagate, Western Digital и Toshiba. Метод SMR обеспечивает большую плотность записи, позволяя записывать данные на частично перекрывающиеся дорожки на диске. Диски SMR оптимально работают с постоянно записываемыми данными, такими как архивирование и резервное копирование на диск, но это может негативно сказаться на производительности для других типов рабочих нагрузок.

Жесткие диски представляют собой альтернативу большой емкости магнитным носителям информации, таким как ленты или гибкие диски и по-прежнему являются одним из основных носителей для устройств хранения резервных копий, активных архивов и долгосрочного хранения. Жесткие диски содержат металлические пластины, покрытые магнитным слоем. Пластины обычно непрерывно вращаются, когда компьютер включен, сохраняя данные в разных секторах магнитного диска. Дисковое устройство резервного копирования может также включать интерфейсы для репликации копий данных, таких как клоны и моментальные снимки, на третичные устройства или в гибридное облако. Недостатком жестких дисков является зависимость от движущихся внутренних механизмов, таких как приводы, двигатели и шпиндели, которые могут выйти из строя и повредить диск. Тем не менее жесткие диски остаются популярными в корпоративных дисковых массивах из-за их увеличивающейся емкости и возможности перезаписи данных на диск. В 2017 г. Western Digital Corp. представила HDD на 14 ТБ, что сделало его самым большим на рынке на тот момент. В 2019 г. компания Seagate Technology выпустила жесткий диск емкостью 16 ТБ, а в 2023 г. Western Digital был представлен самый быстрый HDD в мире ёмкостью 20 Тбайт и скоростью 582 Мбайт/с, достигнутой за счёт использования двух независимых блоков головок. Различают внутренние и внешние жесткие диски (HDD), внутренние и внешние твердотельные накопители (SSD), сетевые устройства хранения данных (NAS). Вторичная память может относиться практически ко всему, включая оптические диски или

ленточные системы, поддерживающие долгосрочное хранение данных. Сюда относят флеш-накопители и SSD-диски. SSD-диск – это полупроводниковый электронный носитель, который также называют твердотельным накопителем, построенный на микросхемах памяти. Особенностью SSD-диска является невозможность восстановления удалённой информации какими-либо специальными утилитами. Флеш-память один из наиболее популярных электронных носителей, который имеет полупроводниковую технологию и программируемую память. Востребованность флеш-памяти объясняется ее небольшими размерами, невысокой ценой, механической прочностью, приемлемым объемом, скоростью работы и низким потреблением энергии. Флэш-память не зависит от движущихся механических частей. Данные записываются на микрочипы, что значительно ускоряет операции хранения по сравнению с традиционными дисками. Однако необходимость стирания и перезаписывания данных целыми блоками оказывает определенное влияние на надежность устройства. Существует два основных типа флэш-накопителей: NAND и NOR. Названия определяются соответствующими логическими элементами, которые определяют фундаментальную архитектуру, лежащую в основе цифровых схем. Флэш-память NAND записывается и читается блоками, тогда как флэш-память NOR считывает и записывает байты независимо друг от друга. Оба типа применяются в самых разных устройствах. Флэш-память NOR, как правило, используется во встроенных системах, а также в планшетах и смартфонах. В некоторых случаях NOR служит заменой оперативной памяти (RAM) или дисков с постоянной памятью (ROM).

Карты памяти представляют собой компактное электронное запоминающее устройство, используемое для хранения цифровой информации. Современные карты памяти изготавливаются на основе флеш-памяти и других технологий. Карты памяти применяются в электронных устройствах, включая цифровые фотоаппараты, сотовые телефоны, ноутбуки, портативные цифровые аудиопроигрыватели.

Носители данных могут быть организованы несколькими способами в зависимости от требований рабочей нагрузки. Некоторые известные конфигурации включают в себя: резервный массив независимых дисков (RAID), сетевое хранилище (NAS) и сеть хранения данных (SAN). Эти конфигурации не являются взаимоисключающими. Например, SAN часто объединяет хранилище в конфигурации RAID. Избыточный массив независимых дисков (RAID: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 и др.) относится к технологии, предназначенной для настройки дисков. Используя эту технологию, пользователь может хранить данные в нескольких местах на устройстве. RAID содержит множество дисков в виде массива, что повышает общую производительность, устойчивость к ошибкам и увеличивает емкость хранилища с помощью методов зеркального отображения или чередования. RAID работает путем размещения данных на нескольких дисках и балансировки операций ввода-вывода (I/O) между этими дисками. RAID может улучшить производительность, отказоустойчивость или и то, и другое, в зависимости от конфигурации RAID. Если RAID настроен на отказоустойчивость, данные защищены в случае отказа диска. Использование нескольких дисков также увеличивает среднее время наработки на отказ (MTBF).

В российском федеральном законодательстве по защите информации и персональных данных применяются два термина по отношению к носителям информации: материальные носители информации и машинные носители персональных данных [13]. В нормативных правовых актах МЧС России для описания средств хранения информации используются различные термины: бумажные носители, средства вычислительной техники, перезаписываемые машинные носители информации, машинные носители информации, носители информации. При этом под электронным видом хранения информации понимается ее хранение в информационных системах персональных данных, на средствах вычислительной техники, а также на съемных магнитных, оптических и других цифровых носителях.

В Приложении № 4 (МЧС России) п. 8 процесс размножения (тиражирования) связан с носителями информации, содержащими служебную информацию ограниченного

распространения, а не с документами. В п. 2. Приложения № 3, утвержденным приказом МЧС России от 14 октября 2019 г. № 581, под термином «носитель информации» понимаются подлинники (копии) документов, баз данных и машинных носителей информации. В ряде аналогичных документов других органов исполнительной власти речь идет о размножении, тиражировании документов с ограничительной пометкой «ДСП», что более корректно и точно отражает содержание работ. Некорректно звучит и требование «копии носителей информации, содержащих служебную информацию ограниченного распространения, подлежат регистрации в учетных формах» (Приложение № 4), если, например, в качестве носителя информации рассматривать машинный носитель.

Заключение

Анализ некоторых технических терминов, отражающих отдельные аспекты обращения со служебной информацией ограниченного распространения в МЧС России, показывает их недостаточную проработанность и корректность использования в контексте формирования ведомственных требований и положений о защите информации с использованием автоматизированных информационных систем.

Гармонизация терминологии на основе обобщения опыта организации защиты информации в других государственных органах позволит повысить эффективность защиты информации за счет более прицельного применения защитных мер.

Статья подготовлена в рамках выполнения в 2023 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР № 123030100009-7 от 1 марта 2023 г.

Список источников

1. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. М., 2020. 216 с.

2. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности: постановление Правительства Рос. Федерации от 3 нояб. 1994 г. № 1233 (в ред. постановления Правительства Рос. Федерации от 6 авг. 2020 г. № 1186) // Собр. законодательства Рос. Федерации. 2005. № 30. Ст. 3165.

3. Метельков А.Н. Конфиденциальная и служебная информация в МЧС России: модели описания информационных процессов // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2021. № 2. С. 92–99. EDN AABQQU.

4. Об утверждении перечня сведений конфиденциального характера: Указ Президента Рос. Федерации от 6 марта 1997 г. № 188 (в ред. Указа Президента Рос. Федерации от 13 июля 2015 г. № 357) // Собр. законодательства Рос. Федерации.1997. № 10. Ст. 1127.

5. Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации // Вестник Уральского юридического института МВД России. 2020. № 2. С. 162–167.

6. Об утверждении Руководства по технической эксплуатации и учету средств вычислительной и оргтехники в системе МЧС России: приказ МЧС России от 27 окт. 2009 г. № 613. URL: https://base.garant.ru/70113592/ (дата обращения: 03.06.2023).

7. Лисиенкова Л.Н., Комарова Л.Ю. Обзор современных устройств хранения данных // Известия ТулГУ. Технические науки. 2020. № 7. С. 259–265. DOI: 10.24411/2071-6168-2020-00097.

8. Prism: Optimizing Key-Value Store for Modern Heterogeneous Storage Devices ASPLOS ’23, March 25–29 / Yongju Song [et al.]. Vancouver, BC, Canada. 2023:588-602.

9. Carniel A.C., Aguiar C.D. d., Spatial Index Structures for Modern Storage Devices: A Survey, IEEE Transactions on Knowledge and Data Engineering, 2023:1-20. DOI: 10.1109/TKDE.2023.3242207.

10. Sumalatha Sriramoju. A Comprehensive Review on Data Storage. International Journal of Scientific Research in Science and Technology (IJSRST). Vol. 6. Iss. 5. P. 236–241.

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

12. ГОСТ Р 7.0.8–2013. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. М.: Стандартинформ, 2019.

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

References

1. Balashova A.A. Elektronnye nositeli informacii i ih ispol'zovanie v ugolovno-processual'nom dokazyvanii: dis. ... kand. yurid. nauk. M., 2020. 216 s.

2. Ob utverzhdenii Polozheniya o poryadke obrashcheniya so sluzhebnoj informaciej ogranichennogo rasprostraneniya v federal'nyh organah ispolnitel'noj vlasti, upolnomochennom organe upravleniya ispol'zovaniem atomnoj energii i upolnomochennom organe po kosmicheskoj deyatel'nosti: postanovlenie Pravitel'stva Ros. Federacii ot 3 noyab. 1994 g. № 1233 (v red. postanovleniya Pravitel'stva Ros. Federacii ot 6 avg. 2020 g. № 1186) // Sobr. zakonodatel'stva Ros. Federacii. 2005. № 30. St. 3165.

3. Metel'kov A.N. Konfidencial'naya i sluzhebnaya informaciya v MCHS Rossii: modeli opisaniya informacionnyh processov // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2021. № 2. S. 92–99. EDN AABQQU.

4. Ob utverzhdenii perechnya svedenij konfidencial'nogo haraktera: Ukaz Prezidenta Ros. Federacii ot 6 marta 1997 g. № 188 (v red. Ukaza Prezidenta Ros. Federacii ot 13 iyulya 2015 g. № 357) // Sobr. zakonodatel'stva Ros. Federacii.1997. № 10. St. 1127.

5. Harlamova A.A. Nepravomernyj dostup k komp'yuternoj informacii: tolkovanie priznakov i nekotorye problemy kvalifikacii // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. 2020. № 2. S. 162–167.

6. Ob utverzhdenii Rukovodstva po tekhnicheskoj ekspluatacii i uchetu sredstv vychislitel'noj i orgtekhniki v sisteme MCHS Rossii: prikaz MCHS Rossii ot 27 okt. 2009 g. № 613. URL: https://base.garant.ru/70113592/ (data obrashcheniya: 03.06.2023).

7. Lisienkova L.N., Komarova L.Yu. Obzor sovremennyh ustrojstv hraneniya dannyh // Izvestiya TulGU. Tekhnicheskie nauki. 2020. № 7. S. 259–265. DOI: 10.24411/2071-6168-2020-00097.

8. Prism: Optimizing Key-Value Store for Modern Heterogeneous Storage Devices ASPLOS ’23, March 25–29 / Yongju Song [et al.]. Vancouver, BC, Canada. 2023:588-602.

9. Carniel A.C., Aguiar C.D. d., Spatial Index Structures for Modern Storage Devices: A Survey, IEEE Transactions on Knowledge and Data Engineering, 2023:1-20. DOI: 10.1109/TKDE.2023.3242207.

10. Sumalatha Sriramoju. A Comprehensive Review on Data Storage. International Journal of Scientific Research in Science and Technology (IJSRST). Vol. 6. Iss. 5. P. 236–241.

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

12. GOST R 7.0.8–2013. Sistema standartov po informacii, bibliotechnomu i izdatel'skomu delu. Deloproizvodstvo i arhivnoe delo. M.: Standartinform, 2019.

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

Информация о статье:
Статья поступила в редакцию: 03.06.2023; одобрена после рецензирования: 07.07.2023;
принята к публикации: 10.07.2023
Information about the article:
The article was submitted to the editorial office: 03.06.2023; approved after review: 07.07.2023;
accepted for publication: 10.07.2023

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
Уткин Олег Валерьевич, старший преподаватель кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), e-mail: utkin_oleg@mail.ru, SPIN-код: 7991-7504

Information about 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
Utkin Oleg V., senior lecturer, department of applied mathematics and information technologies, Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky pr., 149), e-mail: utkin_oleg@mail.ru, SPIN: 7991-7504