Аналитическая статья
УДК 004.056; DOI: 10.61260/2218-13X-2025-3-113-127

ОНТОЛОГИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ В МЧС РОССИИ

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

Аннотация. Целью статьи является углубление понимания мониторинга информационных ресурсов в контексте обеспечения информационной безопасности и защиты не только информации, но и конституционных прав человека и гражданина. В работе автором использован междисциплинарный подход, который объединяет правовые и технические взгляды на дефинирование терминов в сфере информационной безопасности и позволяет более выверенно подойти к единому пониманию правового и технического содержания понятия информационных ресурсов. В результате структурно-правового и сравнительно-правового анализа содержания термина «информационные ресурсы» в контексте мониторинга их защищённости автор приходит к выводу о необходимости их более четкого нормативного закрепления на уровне федерального закона. В результате исследования автором установлено, что расширенная формулировка в действующем российском законодательстве не способствует на практике единообразному толкованию состава рассматриваемого термина. В правовой модели информационных ресурсов предложено не включать субъекта (человека) как непосредственный элемент, входящий в структуру технических сетей и систем, а рассматривать его в виде компонента взаимодействующей социальной системы. Автор приходит к выводу о необходимости уточнения формулировки законодательного определения исследуемого термина применительно к информационным (автоматизированным) системам и другим технологическим системам, информационно-коммуникационным сетям, иным элементам технологической инфраструктуры.

Ключевые слова: информация, ресурсы, защищенность, информационные системы, право, правовое регулирование, персонал, мониторинг, безопасность, устойчивость

Для цитирования: Метельков А.Н. Онтология информационных ресурсов в МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 3. С. 113–127. DOI: 10.61260/2218-13X-2025-3-113-127.

Analytical article

ONTOLOGY OF INFORMATION RESOURCES IN EMERCOM OF RUSSIA

✉**Metel'kov Alexander N.**
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 deepen understanding of the content of monitoring information resources in the context of ensuring information security and protecting not only information, but also the protection of constitutional human and civil rights. The author uses an interdisciplinary approach that combines legal and technical views on the definition of terms in the field of information security and allows a more precise approach to a common understanding of the legal and technical content of the concept of information resources. As a result of a structural, legal and comparative legal analysis of the content of the term «information resources» in the context of monitoring their security, the author comes to the conclusion that they need to be more clearly regulated at the federal law level. As a result of the research, the author found that the expanded wording in the current Russian legislation does not contribute to a uniform interpretation in practice of the composition of the term in question.

It is proposed not to include a subject (person) in the legal model of information resources as a direct element included in the structure of technical networks and systems, and consider it as a social or complex sociotechnical system. The author comes to the conclusion that it is necessary to clarify the wording of the legislative definition of the term under study in relation to information (automated) systems and information and communication networks and other technological systems.

Keywords: information, resources, security, information systems, law, legal regulation, personnel, monitoring, safety, and sustainability

For citation: Metel'kov A.N. Ontology of information resources in EMERCOM of Russia // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 3. P. 113–127. DOI: 10.61260/2218-13X-2025-3-113-127.

Введение

Основой многих видов человеческой деятельности в информационном обществе являются информационные ресурсы (ИР). В условиях проведения недружественными России государствами целевых кибератак на государственные и иные ИР необходимым условием обеспечения их устойчивости и безопасности является мониторинг защищенности таких ресурсов. В целях мониторинга защищенности ИР важно определиться в объеме понятия, которое в законодательстве и документах технического регулирования имеет множественное отражение. Для реализации требований Указа Президента Российской Федерации о мониторинге защищенности ИР [1] необходимо уточнение актуального смысла этого понятия, понятие которое законодательно дано применительно только к конкретным видам объектов или отдельных отраслей права.

Проблема заключается в том, что само понятие ИР в научной и учебной литературе, стандартах, подзаконных нормативных правовых актах ИР описывается по-разному, имеет известную неопределенность и даже противоречивость, поэтому рассматриваемый термин можно назвать «размытым», неструктурированным. Следовательно, таким же «туманным» становится и понятие «защищенность ИР», если не описать его конкретное содержание.

Понятие информационных ресурсов

В России обеспечению информационной безопасности (ИБ) государство придает значение национального стратегического приоритета. Ранее безопасности отводилось второстепенное значение. Основными целями компьютерного проектирования были повышение производительности и снижение стоимости, энергопотребления и размера.

По мере увеличения числа подключенных к Интернету устройств, от персональных интеллектуальных встраиваемых систем до всеобъемлющих облачных серверов, отмечается устойчивая тенденция роста числа вредоносных атак на ИР. Поэтому важно сформировать понимание ИР как системного объекта защиты и объекта мониторинга защищенности.

Традиционно ИР воспринимались как представленный в виде отдельных «документов и/или их массивов системообразующий элемент человеческой деятельности» [2, с.45], который является источником сведений или средством для получения различными субъектами (лицами, организациями) знаний, накапливаемых в процессе жизнедеятельности государства и общества. Характерной особенностью информационного законодательства является «неопределенность, неустойчивость применения многих терминов» [2, с.59]. Возможно поэтому отсутствует легальное общеправовое определение ИР в российском законодательстве. Термин ИР имеет несколько определений. Нередко в подзаконных нормативных правовых актах и других руководящих документах он употребляется как в узком, так и в широком смысле этого слова.

В главе 136 (Межкультурные проблемы управления информационными ресурсами) второго издания Энциклопедии информационной науки и технологий (Encyclopedia

of Information Science and Technology) ИР определены как ресурсы, необходимые для производства информации, включая оборудование, программное обеспечение (ПО), техническую поддержку, пользователей, объекты, системы данных и сами данные. В главе 4 (Использование информационных ресурсов среди кандидатов на экзамен на государственную службу с особым акцентом на Тамил Наду, Индия) и главе 15 (Роль публичных библиотек в построении общества знаний) под ИР понимаются данные и информация, используемые организацией, в главе 7 (Подход к оценке готовности предприятия к цифровой трансформации) ИР рассматриваются как документы/массивы документов в информационной системе или за пределами организации (например, в сети Интернет). ИР рассматривают в широком и узком смысле. В научной литературе к ИР причисляют также информационные ситуации/отношения/процессы, цифровые модели, технологии геомониторинга, информационные системы (ИС), прикладные сервисы, киберфизические системы. Ученые, изучавшие ИР на протяжении ряда последних лет, использовали при их определении «в качестве родовых понятий такие слова, как информация, знание, данные, сведения, документ» [3, с. 88]. В разработанной Правительством Российской Федерации Концепции построения и развития аппаратно-программного комплекса «Безопасный город» понятие ИР означает «отдельные документы и отдельные массивы документов» [4].

Уязвимости ИР

Кибератаки обычно основаны на эксплуатации уязвимостей. Уязвимость представляет собой слабое место в ИС, которое может быть использовано киберпреступниками для получения несанкционированного доступа или выполнения несанкционированных действий в компьютерной системе. Уязвимости могут существовать в различных формах, от ошибок ПО до ошибок пользователей и персонала, обеспечивающего нормальное функционирование ИС и телекоммуникационных сетей. Каждый тип требует особого подхода для смягчения.

В случае использования эксплойтов, нацеленных на уязвимости конструкции оборудования, традиционное антивирусное ПО не может справиться с растущей частотой этих атак. Например, уменьшение масштаба технологии ячеек DRAM способствует появлению уязвимости за счет влияния электромагнитного взаимодействия соседних ячеек. В атаках Rowhammer используется механизм разрушительного воздействия на данные в соседних строках при чтении той же строки в DRAM. Поскольку Rowhammer использует слабость компьютерного оборудования, программный патч не может полностью исправить проблему. Аналогично, не существует эффективного программного смягчения атаки Spectre, использующей уязвимости микроархитектуры для утечки защищенных данных через побочные каналы. Следует заметить, что утечки информации по побочным каналам навсегда учитываются при организации защиты информации. Например, в МЧС России при организации защиты служебной информации ограниченного распространения, в отличие от большинства государственных органов, цели предотвращения утечки, хищения служебной информации по техническим каналам, на взгляд автора, необоснованно не ставятся [5].

Уязвимости сетевого и системного оборудования сопровождают развитие информационных технологий и технических средств. В целом, полное исправление уязвимостей на уровне оборудования потребует его перепроектирования. Авторами статьи [6] продемонстрировано, что атаки путем мониторинга отклонений в микроархитектурных событиях (таких как, например, промахи кэша, когда процессор пытается получить доступ к данным, которых уже нет в кэше; неверные предсказания ветвлений от существующих счетчиков производительности центрального процессора; атаки на уровне оборудования, такие как Rowhammer и Spectre) могут быть эффективно обнаружены во время выполнения с допустимой точностью и разумными издержками производительности с использованием различных классификаторов технологии машинного обучения.

В прошлом злоумышленники использовали программные атаки, нацеленные на уязвимости ПО, или аппаратные атаки, нацеленные на уязвимости оборудования.

Программные атаки используют недостатки или дефекты в программном коде. Они позволяют злоумышленникам использовать операционную систему (ОС) или приложения в системе для получения некоторых привилегий. Аппаратные атаки направлены на недостатки, присущие аппаратным компонентам системы. Аппаратные атаки дают возможность нарушителям напрямую использовать взаимодействие с электронными компонентами системы, не полагаясь на уязвимость ПО и независимость от ОС. Помимо традиционных аппаратных атак, таких как атаки сбоя или атаки по сторонним каналам, злоумышленники берут на вооружение способы использования аппаратных уязвимостей с помощью программного кода. Такой класс атак называют программными атаками, нацеленными на аппаратные уязвимости (SATHV). Нарушители ИБ для добывания информации из системы используют SATHV в системе, например такие как: предсказание ветвлений, выполнение вне очереди (OoO), динамическое масштабирование напряжения и частоты (DVFS), прямой доступ к памяти (DMA) и кэш-памяти. Поскольку SATHV нацелен на уязвимости оборудования, их трудно нейтрализовать. Устранение таких уязвимостей часто требует перепроектирования микроархитектуры или отдельных макрокомпонентов оборудования. Для защиты от программных атак, нацеленных на уязвимости ПО, применяются классические инструменты, такие как антивирусные инструменты, которые не могут обнаружить и защитить систему от атак, нацеленных на уязвимости оборудования. Это происходит потому, что SATHV нацелены на уязвимости оборудования, которые не видны программному приложению. Они могут выполняться удаленно и не обнаруживаться, ведут себя как обычные программные приложения и не оставляют следов в файлах системного журнала. Для решения проблемы SATHV исследователи предложили онлайн-механизмы обнаружения на основе счетчиков производительности оборудования (HPC), то есть интегрированных в большинство современных архитектур регистров специального назначения, хранящих информацию о специфичных для оборудования событиях (ошибки предсказания переходов, промахи кэша, доступы к памяти, операции загрузки и сохранения) и используемых для анализа производительности, настройки и отладки. Количество доступных счетчиков и событий зависит от платформы. Однако механизмы обнаружения специфичны для некоторых SATHV и не могут обнаружить все возможные SATHV, применимые в системе. По мере увеличения количества доступных векторов атак злоумышленники могут обойти механизмы обнаружения, используя варианты атак, не рассматриваемые моделью обнаружения. Такими примерами являются SATHV, использующие стратегии вытеснения, или уклончивый SATHV. Уклончивый SATHV пытается избежать обнаружения, вставляя инструкции nop или sleep во время атаки. Необходимо учитывать нарушителей, пытающихся скрыть свою вредоносную активность. Если механизмы обнаружения принимают во внимание только небольшой набор SATHV, система не защищена от оставшихся атак. Необходимо разработать механизм, который сможет с высокой точностью обнаруживать большую часть SATHV на целевой платформе, а не только ограниченное подмножество. Это сложная задача, поскольку количество HPC ограничено, а доступные события различаются в зависимости от технологической платформы. Поиск событий HPC, коррелирующих для всех атак, сложен.

Ключевым аспектом защитных архитектур является аппаратное шифрование, гарантирующее, что ключи шифрования хранятся и обрабатываются в безопасной аппаратной среде. Полное шифрование диска (FDE) и файловое шифрование (FBE) – широко используемые методы обеспечения аппаратной безопасности, защищающие пользовательских данных в состоянии покоя. Шифрование гарантирует безопасность конфиденциальных данных даже при получении злоумышленником физического доступа к устройству, так как он не сможет расшифровать данные без соответствующих аппаратно защищенных ключей. Аппаратное шифрование может значительно снизить риск утечки данных даже при попытках злоумышленников обойти программные средства безопасности.

Интегрируя несколько аппаратных компонентов в целостную архитектуру безопасности для смягчения сложных векторов атак (атаки по сторонним каналам, эксплойты повреждения памяти, несанкционированный доступ к системным ресурсам), эти системы создают многоуровневую защиту, более эффективную и надежную, чем обычные программные подходы. Например, для добывания конфиденциальной информации атаки по сторонним каналам часто нацелены на физические свойства устройства (энергопотребление, электромагнитное излучение). Аппаратное шифрование и технологии TEE могут скрыть эти физические сигналы, что затрудняет злоумышленникам извлечение полезной информации с помощью анализа сторонних каналов. Аналогичным образом, сложнее эксплуатировать нередко используемые в программных атаках уязвимости повреждения памяти, когда применяются средства защиты на уровне оборудования, например, такие как изоляция памяти и безопасное управление памятью.

Уязвимости ПО в отличие от аппаратных уязвимостей обычно связаны с недостатками в приложениях или самой ОС и, как правило, их легче устранить с помощью обновлений или исправлений безопасности. Уязвимости аппаратных средств используют слабые места в физических компонентах устройства, таких как процессоры, память или модули связи. Эти атаки часто имеют более широкое воздействие, поскольку они могут обойти несколько уровней защиты ПО, делая традиционные меры безопасности неэффективными. В результате поверхность атаки, открытая уязвимостями оборудования, значительно больше и ее сложнее защитить по сравнению с уязвимостями ПО.

Учитывая рост числа атак на основе оборудования и растущую зависимость от мобильных устройств в средах с высокими рисками, крайне важно сосредоточиться на этих типах уязвимостей. Исследователи сравнительно недавно начали признавать важность безопасности оборудования. Однако безопасность оборудования еще остается фрагментированной, а категоризация и понимание этих уязвимостей находятся на ранних стадиях.

В то время как некоторые атаки используют уязвимости ПО (такие как переполнение буфера или ошибки двойного освобождения), другие программные атаки используют уязвимости оборудования для формирования каналов утечки конфиденциальной информации. Такие посягательства включают микроархитектурные атаки, использующие синхронизацию кэша, историю предсказания ветвлений, буферы целевых ветвлений или открытые строки DRAM. Программные методы также используются в атаках, направленных на сбои в работе аппаратных средств посредством внесения изменений в физическую память или внутренние значения центрального процессора.

При проведении мониторинга информационных ресурсов объективно возникает и конституционно-правовая проблема обеспечения прав человека и гражданина – субъекта ИР (например, персонала) в части обеспечения государством конституционных прав человека, соблюдения условий их ограничения. Теоретический и практический интерес, исходя из конституционных положений, представляет осмысление правового понимания ИР в контексте мониторинга их защищенности. Более широкое понятие «мониторинг ИБ» организации определяется как «постоянное наблюдение за процессом обеспечения ИБ в организации с целью установить его соответствие требованиям» [7] по ИБ. Согласно ГОСТ Р ИСО/МЭК 27002–2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (п. 10.10), мониторинг нацелен на обнаружение неавторизованных действий, связанных с обработкой информации. Мониторинг систем проводится с целью проверки эффективности применяемых мер и средств контроля и управления, а также подтверждения следования выбранной модели политики доступа. В условиях проведения изощренных целевых кибератак необходимость контроля систем и сетей, а также регистрация событий ИБ не вызывает возражений. Для обеспечения уверенности в относительно полном выявлении проблем ИС ведутся журналы эксплуатации и регистрируются инциденты ИБ и неисправности. Организация должна выполнять все действующие правовые требования, применимые к ее деятельности, связанной с мониторингом и регистрацией.

Информационные ресурсы как объект мониторинга защищенности

В самом широком понимании в качестве ИР выступают сведения, системы и сети, а также персонал. Например, Национальный институт стандартов и технологий США в документе NIST SP 800-59 определяет ИР как информацию и связанные с ней ресурсы: персонал, оборудование, фонды и информационные технологии.

В документе стратегического планирования [8] информационное пространство определено как совокупность ИР, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их ИС и необходимой информационной инфраструктуры.

В четвертом издании Энциклопедии информационной науки и технологий (2017 г.) ИР описываются как элемент инфраструктуры, позволяющий осуществлять транзакции определенных выбранных значимых и релевантных данных, предоставлять контент и информационные услуги, которые могут использоваться непосредственно пользователем. ИР означают коллекцию ценной информации, полученной в результате человеческой деятельности, включая печатные, непечатные и электронные материалы. В более широком смысле она также включает соответствующее оборудование, персонал и капитал.

В одобренном Правительством Российской Федерации проекте соглашения об обмене информацией о чрезвычайных ситуациях (ст. 4), представленном МЧС России, введен термин «национальные информационно-коммуникационные ресурсы»[9].

Связь между ИБ организации и ИР (активами) организации представлена на рис. 1.

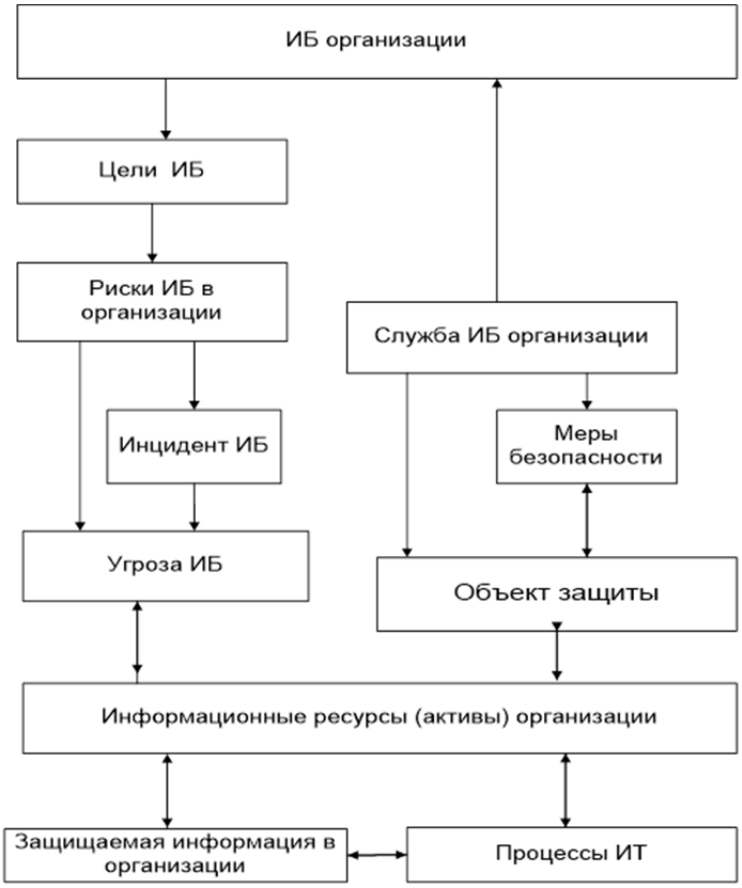

Рис. 1. **Связь между ИБ и ИР организации**

В ГОСТ Р 57486–2017 Услуги населению. Требования к информационному обеспечению (п.п. 3.1) под ИР (информацией) понимается «совокупность данных (сообщения, сведения) независимо от формы их представления, используемых для формирования объективных знаний об объекте» [10]. В числе десяти групп ИР названы

нормативные правовые акты и нормативные документы, а также документы по стандартизации. В ГОСТ Р 53114–2008 (п.п. 3.1.6, примечание) ИР организации отождествляются с информацией (активом) и отличаются от людских ресурсов [7]. Они непосредственно связаны с угрозами ИБ, защищаемой информацией в организации, процессами ИТ и объектом защиты.

Анализ взаимодействия терминов показывает, что ИР и защищаемая информация в организации соотносятся как частное и общее. На основе изображенной на рис. 1 схемы можно выделить следующие связи элементов: ИБ организации – цели ИБ – риски ИБ в организации – инцидент ИБ – ИР (активы) организации– защищаемая информация в организации – процессы ИТ – объект защиты – меры безопасности – служба ИБ организации – ИБ организация. В ГОСТ Р 53114–2008 выделяются людские, вычислительные, информационные, телекоммуникационные ресурсы [7].

Очевидно, что разброс содержания ИР и размытость термина негативно отражается на реализации практических мероприятий по обеспечению ИБ и защите информации. В отдельных монографических исследованиях с названием «Информационные ресурсы в планировании и функционировании образовательных систем»[11] и «Стратегия информационных ресурсов в контексте социологической парадигмы»[12] термин ИР вообще не раскрывается, а из содержания работ невозможно понять, что же авторами понимается под этим термином.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) к группам ИР и компонентов систем и сетей, которые могут являться объектами воздействия, относит восемь составляющих, включая информацию, программные и программно-аппаратные средства, машинные носители информации, телекоммуникационное оборудование, средства защиты информации, «пользователей систем и сетей (интерфейсы взаимодействия с ними) и обеспечивающие системы» [13]. Регулятор разделяет союзом «и» собственно ИР и компоненты систем и сетей. Следовательно, если ИР и компоненты систем и сетей рассматриваются как самостоятельные объекты исследования, то логично исключить ИС из ИР, так как в их состав кроме информации входят технические средства и информационные технологии.

В российском законодательстве и официальных документах государственных регуляторов термин ИР применяется весьма противоречиво. В нормативных правовых актах можно встретить определение, в котором ИС включают ИР, и, наоборот, в ИР включают ИС. Одним из государственных регуляторов ИР рассматриваются весьма широко. В частности, в приказе Федеральной службы безопасности Российской Федерации от 11 мая 2023 г. № 213 «Об утверждении порядка осуществления мониторинга защищенности ИР» такое наблюдение осуществляется в отношении ИР, к которым отнесены ИС (в том числе сайты в сети Интернет); информационно-телекоммуникационные сети, автоматизированные системы управления (АСУ). Аналогичное по составляющим понятие используется в Регламенте Национального координационного центра по компьютерным инцидентам от 2 сентября 2024 г. Исходя из актуальных угроз безопасности с технико-технологической точки зрения, такой подход конструктивен и оправдан по объему мониторинговых элементов. В противном случае, если осуществлять мониторинг только чисто информационной составляющей, то теряется весь смысл мониторинга, так как в осуществлении компьютерных атак важно учитывать все составляющие, включая сети и АСУ. Противоположный рассмотренному подход отражен в постановлении Правительства Российской Федерации № 57 (рис. 2), в котором понятие «информационная система» в числе других элементов включает ИР и базы данных [14], в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, ИР и ИС рассматриваются как однопорядковые элементы (рис. 3).

Рис. 2. **ИР в составе информационной системы**

Рис. 3. **Структура информационного пространства**

По всей видимости, вполне понятное и отчасти справедливое в современных условиях стремление регулятора охватить контролем более широкий спектр объектов защиты привело к недостаточно корректному определению ИР. Отнесение АСУ, как разновидности автоматизированных систем (АС), к ИР приводит к противоречивой ситуации. В устоявшемся определении АС, признанном научным большинством и доминирующим в стандартах, является включение в его состав персонала (например, ГОСТ 34.003–90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения (п. 1.1); ГОСТ Р 59853–2021 Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения (п. 2.2); ГОСТ 34.602–2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы; ГОСТ 24.104–2023 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие

требования). Однако следует отметить, что определение АСУ, данное в ст. 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», как комплекса программных и программно-аппаратных средств, не предусматривает наличие человека как элемента этой системы [15]. Строго говоря, это определение касается исключительно объектов критической инфраструктуры. Следуя логике регулятора, персонал при стандартном понимании АС оказывается вовлеченным в структуру самого понятия ИР, что расширяет сферу деятельности по защите информации при условии соблюдения конституционных прав и свобод гражданина и человека в процессе мониторинга ИР. Мониторинг (англ. monitoring – контроль, слежение) – осуществляемая на постоянной основе «специальная форма наблюдения (слежения) за текущим изменением тех или иных процессов или объектов в пространстве и во времени» [16, с. 278]; «система постоянного наблюдения за явлениями и процессами, проходящими в окружающей среде и обществе …» [17, с. 278]. Под мониторингом ресурсов сети понимается «целенаправленное автоматизированное или автоматическое прямое или косвенное дистанционное «наблюдение» за состоянием ресурсов сети» [18, с. 82].

Полиморфизм отмечается в строении концептуальных, правовых и иных моделей ИР в МЧС России. В официальных документах МЧС России ИР определяются весьма противоречиво: как информация, как информационные системы и даже автоматизированные системы, которые, как известно, включают обслуживающий их персонал. В ведомственных нормативных правовых актах можно встретить определение, в котором информационные системы включают ИР, и, наоборот, определение, в котором ИР включают информационные системы. В Методическом документе ФСТЭК России ИР дефинируются традиционно узко как «информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях» [18]. Концептуальная модель состава ИР представлена на рис. 4. В процессе деятельности организаций и учреждений МЧС России формируются ИР, включающие общедоступную информацию, персональные данные, охраняемые результаты интеллектуальной деятельности, информацию ограниченного доступа и сведения, составляющие государственную или служебную тайну. Концептуально объект защиты рассматривается узко. Таким объектом являются ИР подразделений МЧС России (библиотеки, архивы и фонды; банки, базы и файлы данных; отдельные документы на традиционных носителях), содержащие зафиксированные на материальном носителе сведения, используемые в процессе сбора, обработки, накопления, хранения, распространения, взаимодействия в рамках исполнения возложенных на МЧС России функций и оказания государственных услуг.

Рис. 4. **Концептуальная модель состава ИР МЧС России**

Одновременно в МЧС России существуют модели понятия ИР, в состав которых входят различные элементы (рис. 5).

а)

б)

в)

Рис. 5. **Некоторые структурные модели понятия ИР в МЧС России**

В тоже время в постановлении Правительства Российской Федерации [14], наоборот, по отношению к модели в) ИР являются лишь частью ИС и не включают базы данных, которые представлены самостоятельным структурным элементом (рис. 6).

Рис. 6. **Схематичное представление ИР в автоматизированной информационно-управляющей системе РСЧС**

В учебном пособии [19, с. 10] в таблице 1, 1.5 ИР как социотехнический объект организационной системы описывается через структуры (вид, форма и построение текста документа, символа и знака; последовательность изложения; целостность, полнота), программы (смысловое соответствие, конфиденциальность, направленность, актуальность, новизна), ресурсы (объем, качество, релевантность, достоверность и др.), системные основы (уровень обобщения информации; роль и место в когнитивном, аксиологическим, мотивационном и других аспектах изучения), связи (логические связи с другими объектами, принадлежность, направленность: причина-следствие; посылки-выводы; аргументы-факты и др.). Анализ содержания показывает, что кроме самой информации, ее различных качеств и характеристик, включая ее форму существования в виде программ, никаких иных материальных объектов (компонентов систем и сетей) понятие ИР не содержит. По сути, аналогичное по содержанию определение ИР предложено в ГОСТ Р 43.0.2–2006 Информационное обеспечение техники и операторской деятельности. Термины и определения, п. 2.11 и ГОСТ Р 52448–2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения, п.5.1. В современных условиях установленный регулятором порядок мониторинга ИР является необходимым и оправданным в регулировании общественных отношений в сфере обеспечения устойчивости и безопасности ИР, однако он требует закрепления единообразного закрепления в базовом законе об информации, информационных технологиях и защите информации. Такой подход к мониторингу социальной сети ее владельцем установлен в статье 10.6. Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций в целях обеспечения формирования реестра социальных сетей организует мониторинг ИР.

Заключение

Проведенный анализ онтологии ИР МЧС России показывает многозначность, а следовательно, и неопределённость содержания таких ресурсов. Отмечается и заметное расхождение различных интерпретаций ИР в официальных документах МЧС России с принятыми концептуальными подходами. В результате исследования автор приходит к следующим выводам:

1. Структурно-правовой и семантический анализ термина «информационные ресурсы» показывает, что в правовых актах МЧС России он используется противоречиво, что существенно затрудняет понимание мониторинга защищенности ИР МЧС России и его практическую реализацию.

2. Содержание понятия ИР нестабильно. Существует потребность его более четкого нормативного закрепления в базовом федеральном законе в направлении обеспечения преемственности фундаментальной научной мысли, сложившейся в представлениях ученых, с учетом конституционных прав и свобод человека, которые могут затрагиваться в процессе мониторинга защищенности ИР.

3. В методологическом плане для удобства построения моделей технических систем при конструировании модели определения термина ИР необходимо включать только такие элементы, которые в своем составе не содержат субъекта как компонента социотехнической системы.

4. Объективно необходимое и оправданное расширение объектов мониторинга защищенности за счет включения в их число ИС, АСУ и информационно-телекоммуникационных систем на данном этапе развития информационных технологий и появления сопутствующих им новых угроз безопасности нуждается в выработке нового термина, объединяющего эти элементы под собственным названием, либо путем перечисления составляющих элементов. При этом нежелательно идти по пути «втискивания» их в традиционное понятие ИР.

Статья подготовлена в рамках выполнения в 2025 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России НИР «Кибермониторинг».

Список источников

1. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 1 мая 2022 г. № 250. Доступ из инф.-правового портала «Гарант».

2. Информационно-правовая политика в современной России: словарь-справочник / под ред. А.В. Малько, О.Л. Солдаткиной. М.: Проспект, 2021. 240 с.

3. Берестова Т.Ф. Теоретическое информационное ресурсоведение. Челябинск: ЧГИК, 2019. 336 с.

4. Распоряжение Правительства Российской Федерации от 03.12.2014 г. № 2446-р (в ред. от 5 апреля 2019 г.) «Концепция построения и развития аппаратно-программного комплекса «Безопасный город» URL: http://government.ru/docs/all/93978/ (дата обращения: 02.03.2025).

5. Официальный портал правовой информации России. Приказ Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий 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». URL: http://publication.pravo.gov.ru/Document/View/0001202001220002?ysclid=mcilc7gy5a492935721 (дата обращения: 30.06.2025).

6. MaDMAN: Detection of Software Attacks Targeting Hardware Vulnerabilities / N.F. Polychronou [et al.] // 24th Euromicro Conference on Digital System Design. Palermo, 2021. P. 355–362.

7. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М.: Стандартинформ, 2009. 16 с.

8. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203. Доступ из инф.-правового портала «Гарант».

9. ГОСТ Р 57486–2017. Услуги населению. Требования к информационному обеспечению. Доступ из инф.-правового портала «Гарант».

10. О подписании Соглашения об обмене информацией о чрезвычайных ситуациях природного и техногенного характера, об информационном взаимодействии при ликвидации их последствий и оказании помощи пострадавшему населению: постановление Правительства Рос. Федерации от 29 августа 2003 г. № 536. Доступ из инф.-правового портала «Гарант».

11. Нагаева И.А. Возможности применения информационных ресурсов в образовании // Проблемы и перспективы развития образования в России. 2012. № 15. С. 83–88.

12. Стратегия исследования информационных ресурсов в контексте социологической парадигмы: монография / под ред. А.В. Ковалевой. Барнаул: изд-во Алт. ун-та, 2020. 139 с.

13. Методический документ от 5 февраля 2021 г. ФСТЭК России. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 29.06.2025).

14. О государственной информационной системе «Автоматизированная информационно-управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций»: постановление Правительства от 24 января 2024 г. № 57. Доступ из инф.-правового портала «Гарант».

15. О безопасности критической информационной инфраструктуры Российской Федерации: Федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 31. Ч. I. Ст. 4736.

16. Симчера Я.В. Мониторинг. Большая российская энциклопедия – электронная версия. URL: https://old.bigenc.ru/economics/text/2227291?ysclid=mauo07hgxc85639940 (дата обращения: 19.05.2025).

17. Мониторинг // Гражданская защита: энциклопедия в 4-х т. Т. II. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2015. 623 с.

18. Цветков А.А. Задачи обработки данных мониторинга ресурсов распределенной вычислительной сети // Вестник евразийской науки. 2014. № 4. С. 81–90.

19. Дербин Е.А., Царегородцев А.В. Информационное противоборство: концептуальные основы обеспечения информационной безопасности. М.: ИНФРА-М, 2024. 267 с.

References

1. O dopolnitel'nyh merah po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 1 maya 2022 g. № 250. Dostup iz inf.-pravovogo portala «Garant».

2. Informacionno-pravovaya politika v sovremennoj Rossii: slovar'-spravochnik / pod red. A.V. Mal'ko, O.L. Soldatkinoj. M.: Prospekt, 2021. 240 s.

3. Berestova T.F. Teoreticheskoe informacionnoe resursovedenie. Chelyabinsk: ChGIK, 2019. 336 s.

4. Rasporyazhenie Pravitel'stva Rossijskoj Federacii ot 03.12.2014 g. № 2446-r (v red. ot 5maprelya 2019 g.) «Koncepciya postroeniya i razvitiya apparatno-programmnogo kompleksa «Bezopasnyj gorod» URL:http://government.ru/docs/all/93978/ (data obrashcheniya 02.03.2025).

5. Oficial'nyj portal pravovoj informacii Rossii. Prikaz Ministerstva Rossijskoj Federacii po delam grazhdanskoj oborony, chrezvychajnym situaciyam i likvidacii posledstvij stihijnyh bedstvij ot 14 oktyabrya 2019 g. № 581 «O poryadke obrashcheniya so sluzhebnoj informaciej ogranichennogo rasprostraneniya v Ministerstve Rossijskoj Federacii po delam grazhdanskoj oborony, chrezvychajnym situaciyam i likvidacii posledstvij stihijnyh bedstvij». URL: http://publication.pravo.gov.ru/Document/View/0001202001220002?ysclid=mcilc7gy5a492935721 (data obrashcheniya: 30.06.2025).

6. MaDMAN: Detection of Software Attacks Targeting Hardware Vulnerabilities / N.F. Polychronou [et al.] // 24th Euromicro Conference on Digital System Design. Palermo, 2021. P. 355–362.

7. GOST R 53114–2008. Zashchita informacii. Obespechenie informacionnoj bezopasnosti v organizacii. Osnovnye terminy i opredeleniya. M.: Standartinform, 2009. 16 s.

8. O Strategii razvitiya informacionnogo obshchestva v Rossijskoj Federacii na 2017–2030 gody: Ukaz Prezidenta Ros. Federacii ot 9 maya 2017 g. № 203. Dostup iz inf.-pravovogo portala «Garant».

9. GOST R 57486–2017. Uslugi naseleniyu. Trebovaniya k informacionnomu obespecheniyu. Dostup iz inf.-pravovogo portala «Garant».

10. O podpisanii Soglasheniya ob obmene informaciej o chrezvychajnyh situaciyah prirodnogo i tekhnogennogo haraktera, ob informacionnom vzaimodejstvii pri likvidacii ih posledstvij i okazanii pomoshchi postradavshemu naseleniyu: postanovlenie Pravitel'stva Ros. Federacii ot 29 avgusta 2003 g. № 536. Dostup iz inf.-pravovogo portala «Garant».

11. Nagaeva I.A. Vozmozhnosti primeneniya informacionnyh resursov v obrazovanii // Problemy i perspektivy razvitiya obrazovaniya v Rossii. 2012. № 15. S. 83–88.

12. Strategiya issledovaniya informacionnyh resursov v kontekste sociologicheskoj paradigmy: monografiya / pod red. A.V. Kovalevoj. Barnaul: izd-vo Alt. un-ta, 2020. 139 s.

13. Metodicheskij dokument ot 5 fevralya 2021 g. FSTEK Rossii. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (data obrashcheniya: 29.06.2025).

14. O gosudarstvennoj informacionnoj sisteme «Avtomatizirovannaya informacionno-upravlyayushchaya sistema edinoj gosudarstvennoj sistemy preduprezhdeniya i likvidacii chrezvychajnyh situacij»: postanovlenie Pravitel'stva ot 24 yanvarya 2024 g. № 57. Dostup iz inf.-pravovogo portala «Garant».

15. O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Feder. zakon Ros. Federacii ot 26 iyulya 2017 g. № 187-FZ // Sobr. zakonodatel'stva Ros. Federacii. 2017. № 31. Ch. I. St. 4736.

16. Simchera Ya.V. Monitoring. Bol'shaya rossijskaya enciklopediya – elektronnaya versiya. URL: https://old.bigenc.ru/economics/text/2227291?ysclid=mauo07hgxc85639940 (data obrashcheniya: 19.05.2025).

17. Monitoring // Grazhdanskaya zashchita: enciklopediya v 4-h t. T. II. M.: FGBU VNII GOCHS (FC), 2015. 623 s.

18. Cvetkov A.A. Zadachi obrabotki dannyh monitoringa resursov raspredelennoj vychislitel'noj seti // Vestnik evrazijskoj nauki. 2014. № 4. C. 81–90.

19. Derbin E.A., Caregorodcev A.V. Informacionnoe protivoborstvo: konceptual'nye osnovy obespecheniya informacionnoj bezopasnosti. M.: INFRA-M, 2024. 267 s.

Информация о статье:
Статья поступила в редакцию: 11.08.2025; одобрена после рецензирования: 14.09.2025;
принята к публикации: 16.09.2025
Information about the article:
The article was submitted to the editorial office: 11.08.2025; approved after review: 14.09.2025;
accepted for publication: 16.09.2025

Сведения об авторах:
Метельков Александр Николаевич, доцент кафедры прикладной математики и безопасности 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:
Metel'kov Alexander N., associate professor of the department of applied mathematics and information technology security 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