ТРАНСФОРМАЦИЯ ОБЪЕКТА ЗАЩИТЫ В УСЛОВИЯХ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Метельков А.Н.[1]

Ключевые слова: *изменения, воздействие, защита, объект, информационная безопасность, технологии, виртуализация, искусственный интеллект.*

Аннотация

Цель: *показать, что современные доктринальные подходы к определению объекта защиты в сфере информационной безопасности и существующие коллизии в классификации соответствующих инцидентов (в т.ч. компьютерных атак) обусловливают необходимость выделения приоритетных объектов технической защиты информации и нормативного закрепления их дефиниций, а также критериев отнесения к данной категории объектов защиты в требованиях регуляторов. Работа направлена на выявление изменений в нормативных требованиях к объекту защиты для обеспечения устойчивости и безопасности информационных систем, данных и инфраструктуры в условиях повышения технологичности и количества компьютерных атак*

Метод: *с использованием системного подхода объект защиты исследован как совокупность взаимосвязанных компонентов и их связей с внешней средой, формирующей новые угрозы безопасности информационным ресурсам. Изменение содержания объекта защиты продемонстрировано методом анализа нормативных правовых актов и стандартов, а также сравнительно-правового исследования нормативных требований государственного регулятора.*

Результат: *автором выделены особенности генезиса объекта защиты в современных условиях, раскрыто актуальное понимание объекта защиты в информационной инфраструктуре, выявлена тенденция усложнения и конкретизации объекта защиты, а также ориентация требований государственного регулятора на выделение из широкого спектра потенциальных опасностей наиболее значимых угроз информационной безопасности и угроз безопасности информации. С учетом опыта отражения компьютерных атак на российскую критическую и иную информационную инфраструктуру усилия операторов информационных систем сфокусированы ФСТЭК России на наиболее чувствительных объектах защиты. Установлено, что различные подходы к определению понятия «защита информации» расширяют сферу регулирования и конкретизируют границы идентификации угроз информационной безопасности, включая компьютерные инциденты. Введение новых требований к организации системы защиты информационных систем посредством уточнения объектов защиты способствует концентрации практических мер и мероприятий на противодействии актуальным угрозам информационной безопасности и безопасности информации.*

DOI: 10.24412/1994-1404-2026-2-44-51

Введение и постановка задачи

Современный этап жизни мирового сообщества ознаменован переходом от информатизации к цифровой трансформации, то есть глубокому изменению бизнес-процессов, социальных взаимодействий и моделей управления на основе больших данных, искусственного интеллекта (ИИ) и платформенных решений. Цифровая трансформация ставит перед российской правовой системой беспрецедентные вызовы, требующие регулирования принципиально новых явлений: алгоритмов ИИ, оборота больших данных, функционирования цифровых платформ, обеспечения «цифровых прав» человека, защиты от новых киберугроз и информационных воздействий. Государственная политика становится все более активной, комплексной и директивной, стремясь одновременно стимулировать технологическое развитие, управлять рисками и использовать цифровизацию для достижения стратегических национальных приоритетов, в число которых

[1] ***Метельков Александр Николаевич****, кандидат юридических наук, доцент, доцент кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России, г. Санкт-Петербург, Российская Федерация.*

E-mail: metelkov5178@mail.ru

включена информационная безопасность. Активная роль государства, пытающегося реагировать на инновационные изменения и управлять ими, ведет к усложнению и ускорению динамики правового регулирования и, как следствие, понятийного аппарата правовой информатики. В период цифровой трансформации на первый план выдвинулись такие новые понятия, как «информационные ресурсы Российской Федерации», «объект защиты», «искусственный интеллект» и целый ряд других. Как объекты защиты информации сейчас рассматриваются большие фундаментальные модели [1, с. 30], объекты интеллектуальных прав[2]. Применение систем интеллектуальных агентов для защиты информации (ЗИ) [2] требует выделения такой многоагентной системы в качестве объекта защиты.

Задачей исследования является обоснование необходимость определения в нормативных актах государственных регуляторов в сфере обеспечения информационной безопасности и защиты информации вводимых новых терминов для их применения в решении практических задач при использовании современных информационных технологий в обстановке динамики и усложнения угроз информационной безопасности информационных ресурсов.

Понятие объекта защиты

Обеспечение информационной безопасности (ИБ) и защита информации должны начинаться с установления объекта защиты. Во многом характер объекта защиты определяет меры, мероприятия, методы и средства обеспечения ИБ и ЗИ. В условиях динамичного развития информационных технологий сам объект защиты меняется и трансформируется, что требует его четкой идентификации на каждом этапе появления новых технологий. Изменения в технологиях, появление новых методов и средств отражаются на понятийном аппарате в информационной сфере. Заметные изменения происходят в терминологических системах регуляторов. Рассмотрим эти изменения на примере терминосистемы, выстраиваемой ФСТЭК России.

Используемые понятия в информационной безопасности должны носить дискурсивный характер, то есть находиться в определённой логической корреляции с общепризнанными понятиями. В дефинитивном плане правовой термин — это слово (или определённое сочетание слов), унифицированно используемое в сфере правовых отношений, которое обозначает правовое понятие и отличается заданной моносемичностью (т. е. строгой смысловой определённостью, однозначностью), функциональной устойчивостью[3]. Важнейшим из этих компонентов являются объекты защиты: от их состава зависят и методы, и средства защиты, и мероприятия по защите информации. Объекты защиты следует отличать от объектов воздействия. Объект защиты, то есть то, что подлежит охране, отличается от объекта воздействия — того, на что может быть направлено деструктивное воздействие при реализации угрозы. Теоретически эти объекты могут пересекаться и даже в крайнем случае совпадать. Объект защиты по своему смысловому объёму шире, чем объект воздействия. Объект защиты включает в себя не только информацию, но и её носители, процессы и связанные с ними ресурсы, в то время как объект воздействия сосредотачивается на определённых элементах, которые могут пострадать от реализации внешних или внутренних угроз.

В методическом документе ФСТЭК России от 5 февраля 2021 г. «Методика оценки угроз безопасности информации»[4] в числе основных задач, решаемых при оценке угроз безопасности информации, выделены инвентаризация систем и сетей и определение возможных объектов воздействия таких угроз. В работе [3, с. 33—34] на основе анализа данных информационной системы (ИС) предприятия определены группы информационных ресурсов и элементов систем и сетей, которые могут являться объектами воздействия. К ним отнесены: информация, содержащаяся в системах и сетях; программно-аппаратное обеспечение для хранения и обработки информации; программное обеспечение (прикладное, системное, серверы приложений, системы управления базами данных, системы виртуализации, веб-приложения); машинные носители, содержащие защищаемую информацию и данные аутентификации (жёсткие диски, установленные в автоматизированные рабочие места (АРМ) сотрудников, eToken[5]); телекоммуникационное оборудование (включая программное обеспечение для управления телекоммуникационным оборудованием); средства защиты информации.

Современные представления об объекте защиты в информационной сфере усложняются, особенно в части её технической защиты.

В требованиях по защите информации, изложенных в приказе ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»[6], по сравне-

---

[2] Национальная стратегия развития искусственного интеллекта на период до 2030 года, утверждена указом Президента Российской Федерации от 10 октября 2019 г. № 490. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения 03.05.2026).

[3] Юридическая техника: учебное пособие / Под ред. Т.Я. Хабриевой, Н.А. Власенко. Москва: Эксмо, 2010. С.95.

[4] Методика оценки угроз безопасности информации. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения 09.05.2026).

[5] eToken — это электронное устройство (обычно в форм-факторе USB-флеш-накопителя) или программный продукт для двухфакторной аутентификации пользователя и защиты данных. Содержит защищённую память для хранения цифровых сертификатов, ключей шифрования и другой конфиденциальной информации.

[6] Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202506170011 (дата обращения: 10.05.2026).

нию с аналогичными требованиями в утратившем юридическую силу ведомственном приказе от 11 февраля 2013 г. № 17, объекты защиты расширены и конкретизированы. Согласно действующим требованиям регулятора, организация деятельности по защите информации включает составление перечня объектов защиты, которые охватывают программные, программно-аппаратные средства, ИС, сети и подсети, образующие информационно-телекоммуникационную инфраструктуру. В ИС согласно нормативным требованиям ФСТЭК России должны быть реализованы базовые меры защиты самих ИС и информации, содержащейся в них. Из перечня таких мер можно обособить соответствующие им объекты защиты.

В ГОСТ Р 50922-2006 «Защита информации. Основные термины» и определения (далее — ГОСТ Р 50922)[7] объект ЗИ определяется как информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью ЗИ (п. 2.5.1), в котором носитель ЗИ является физическим лицом или материальным объектом, включая физическое поле, в котором информация отражается в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (п. 2.5.3).

В рекомендациях по стандартизации Р 50.1.053—2005 «Информационные технологии. Основные термины и определения в области технической защиты информации»[8] (п. 3.1) в числе объектов технической ЗИ выделены защищаемые информационные ресурсы (автоматизированной ИС), автоматизированная ИС и информационная технология. При этом информационные ресурсы определены узко, в традиционном понимании, как документы и массивы документов, используемые в АИС.

Одним из важных элементов создания системы защиты информации в организации является определение объектов защиты.

Согласно национальному стандарту ГОСТ Р 27.102-2021 «Надежность в технике. Надежность объекта. Термины и определения»[9] объект представляет собой элемент, устройство, систему, функциональную единицу, оборудование, изделие, которые можно рассматривать в отдельности. Объект может состоять из аппаратных средств, программное обеспечение или из того и другого одновременно. Объект может включать в себя и персонал.

Родственным понятию «объект ЗИ» является понятие «защищаемого объекта информатизации», под которым понимается объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

В стандарте выделяют правовую, техническую, криптографическую и физическую защиту информации. К объектам ЗИ при физической ЗИ относят охраняемую территорию, здание (сооружение), выделенное помещение, информацию и (или) информационные ресурсы объекта информатизации.

В качестве объектов защиты рассматриваются информационные ресурсы в организации, такие как ИС персональных данных, автоматизированные системы управления (АСУ) технологическим процессом, государственные ИС, значимые объекты критической информационно инфраструктуры (КИИ) [4, с. 2]: ИС, информационно-телекоммуникационная сеть (ИТКС), АСУ. Обеспечение безопасности значимых объектов КИИ, в том числе являющихся АСУ технологическим процессом, имеет важное значение для функционирования как производственного комплекса, так и для обеспечения безопасности страны [5, с. 2].

В автоматизированной системе (АС) диспетчеризации авторы [2, с. 44—45] выделяют такие объекты защиты, как:

- информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию и представленных на магнитных, оптических и других носителях;
- информацию, передаваемую по каналам связи;
- ОТСС обработки информации (средства вычислительной техники, на которых обрабатывается информация, включая серверы, АРМ, коммуникационное оборудование и линии связи);
- программные и аппаратные компоненты системы ЗИ;
- материальные носители информации;
- электронные файлы и документы, содержащие информацию;
- помещение оператора;
- ключевую, аутентифицирующую и парольную информацию;
- конфигурационную, управляющую, а также остаточную информацию на носителях информации;
- документацию на СЗИ.

В требованиях ФСТЭК России в АС[10] объектами защиты признаны: данные о параметрах управляемого (контролируемого) объекта или процесса, программно-технический комплекс, включающий технические средства и средства защиты информации. К сведениям о параметрах управляемого (контролируемого) объекта или процесса регулятором отнесены входные/выходные сведения, командная информация,

[7] Защита информации. Основные термины и определения. ГОСТ Р 50922-2006. М. : Стандартинформ, 2008. 8 с.

[8] Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации. Р 50.1.053-2005. М. : Стандартинформ, 2005. 16 с.

[9] Надежность в технике. Надежность объекта. Термины и определения: ГОСТ Р 27.102-2021. М. : Российский институт стандартизации, 2024. 35 с.

[10] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утв. приказом ФСТЭК России от 14 марта 2014 г. № 31 // СПС «КонсультантПлюс» (дата обращения 09.05.2026).

контрольно-измерительная и иная критически важная технологическая информация. Программно-технический комплекс охватывает АРМ, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства, а также микропрограммное, общесистемное и прикладное программное обеспечение.

На основе анализа инцидентов информационной безопасности в работе [6, с. 218] названы основные проблемы автоматизированных систем, построенных на базе технологии промышленного Интернета вещей, среди которых выделен низкий уровень защищенности конечных узлов. Все чаще обнаруживаются в промышленном оборудовании, включая большинство устройств и ИС, используемых с уязвимостями без учета требований безопасности. Ситуация осложняется тем, что интеллектуальные устройства и датчики обладают ограниченными вычислительными ресурсам, что делает невозможным использование антивирусных средств для защиты таких устройств. С другой стороны, производители таких устройств не заинтересованы в длительной поддержке и выпуску обновлений безопасности для устранения обнаруженных уязвимостей.

В статье [7, с. 239] авторами под конечными точками понимаются компьютеры и ноутбуки, мобильные телефоны, офисная техника, серверы.

Широкое распространение технологий виртуализации и появление в связи с этим новых уязвимостей и угроз, их эксплуатирующих, потребовало закрепления в стандартах термина «виртуализация». Согласно ГОСТ Р 56938—2016[11] под этим термином «виртуализация» объединяется множество информационных технологий, призванных уменьшать затраты на развертывание компьютерной сети организации, повышать отказоустойчивость применяемых серверных решений и достигать других преимуществ. Виртуализация в отношении разных объектов (программ, вычислительных систем, систем хранения данных, вычислительных сетей, памяти, данных) представляет собой имитацию программного и/или аппаратного обеспечения, в среде которого функционируют различные программы. При использовании данной технологии создаются виртуальные и виртуализованные объекты доступа. Такие объекты нуждаются в защите наравне с другими объектами ИС, в том числе аппаратные средства ИС, используемые для реализации технологий виртуализации. В случае применения виртуализации к объектам защиты относят средства формирования и управления виртуальной инфраструктурой: гипервизоры I типа, обеспечивающие низкоуровневую виртуализацию аппаратных ресурсов сервера; гипервизоры II типа, предоставляющие среду виртуализации в пределах пользовательской операционной системы (ОС); гипервизоры системы хранения данных, абстрагирующие и унифицирующие доступ к разнородным хранилищам; консоли управления виртуальной инфраструктурой, организующие единый интерфейс для администрирования виртуальных машин, сетей и хранилищ. В целях обеспечения информационной безопасности объектами ЗИ также признаются элементы виртуализированной информационно-телекоммуникационной инфраструктуры, в том числе:

- виртуальные вычислительные системы (в т.ч. виртуальные машины и виртуальные серверы);
- распределённые и централизованные системы виртуализированного хранения данных;
- логические каналы передачи данных, реализованные в рамках виртуализированной сетевой среды;
- виртуализированный аппаратные компоненты: виртуальные центральные процессоры (vCPU), виртуальные жёсткие диски (vHDD), виртуальная оперативная память (vRAM), виртуализированный сетевое оборудование (активное и пассивное);
- встроенные виртуальные средства защиты информации и специализированные программно-аппаратные комплексы ЗИ, спроектированные для функционирования в среде виртуализации;
- периметр виртуальной инфраструктуры, охватывающий задействованные физические ресурсы: ядра центрального процессора, адресное пространство оперативной памяти, сетевые интерфейсы (NIC), порты подключения внешних устройств (USB, PCIe и пр.).

Защита перечисленных объектов реализуется посредством комплексного применения виртуальных средств ЗИ и специализированных решений для среды виртуализации и иных категорий средств защиты информации, совместимых с виртуализированными средами.

Наряду с виртуализацией реализация на практике идеи использования унифицированных контейнеров поставили их в ряд важных объектов защиты. Контейнеры позитивно отличаются от виртуальных машин. В научных публикациях [12] указываются их следующие возможности:

- совместное использование ресурса базовой операционной системы, что делает их более эффективными;
- малое время запуска и остановки контейнеров;
- минимальность или полное отсутствие накладных расходов для приложений, запускаемых в контейнерах, по сравнению с приложениями, инициируемыми под прямым управлением базовой ОС;

[11] Защита информации. Защита информации при использовании технологий виртуализации. Общие положения. ГОСТ Р 56938—2016. Москва: Стандартинформ, 2016. 32 с.

[12] Бец М.О. Вопросы развития облачной информационной инфраструктуры федеральных органов исполнительной власти России // Информационные технологии, связь и защита информации МВД России. 2017. С. 28.

– переносимость контейнеров обеспечивает потенциальную возможность устранения программных ошибок, вызываемых изменениями рабочей среды;
– возможность включения большего числа контейнеров, чем при использовании отдельных виртуальных машин на одном хосте.

В диссертации М.И. Паршукова [8, с. 99] обоснованно выделяются расхождения в трактовке понятия «защита информации» между нормативно-правовым и нормативно-техническим регулированием. В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», защита информации определяется целевым образом — как совокупность правовых, организационных и технических мер, направленных на предотвращение: утечки информации; несанкционированного доступа; случайных или преднамеренных воздействий на информацию. ГОСТ Р 50922[13] даёт деятельностную трактовку и классифицирует защиту информации по методам реализации, акцентируя внимание на правовой, технической (включая криптографические методы) и физической видам защиты.

Правовая модель объектов технической ЗИ, основанная на актуальных требованиях ФСТЭК России представлена на рис. 1. Ранее действовавшая модель описана в работе [9], которая фрагментарно представлена на рис. 2.

Исследователями отмечается, что выбор мер защиты происходит «в условиях изменений состава объекта защиты» [10, с. 61]. В актуальной модели объект защиты представлен более структурировано и максимально конкретно. Однако инновационные термины, не имеющие своего закрепления в техническом регулировании, на наш взгляд, целесообразно было бы раскрыть и дать дефиниции, установленные регулятором. Например, английское слово orchestra заимствовано из латинского orchestra, а оно —

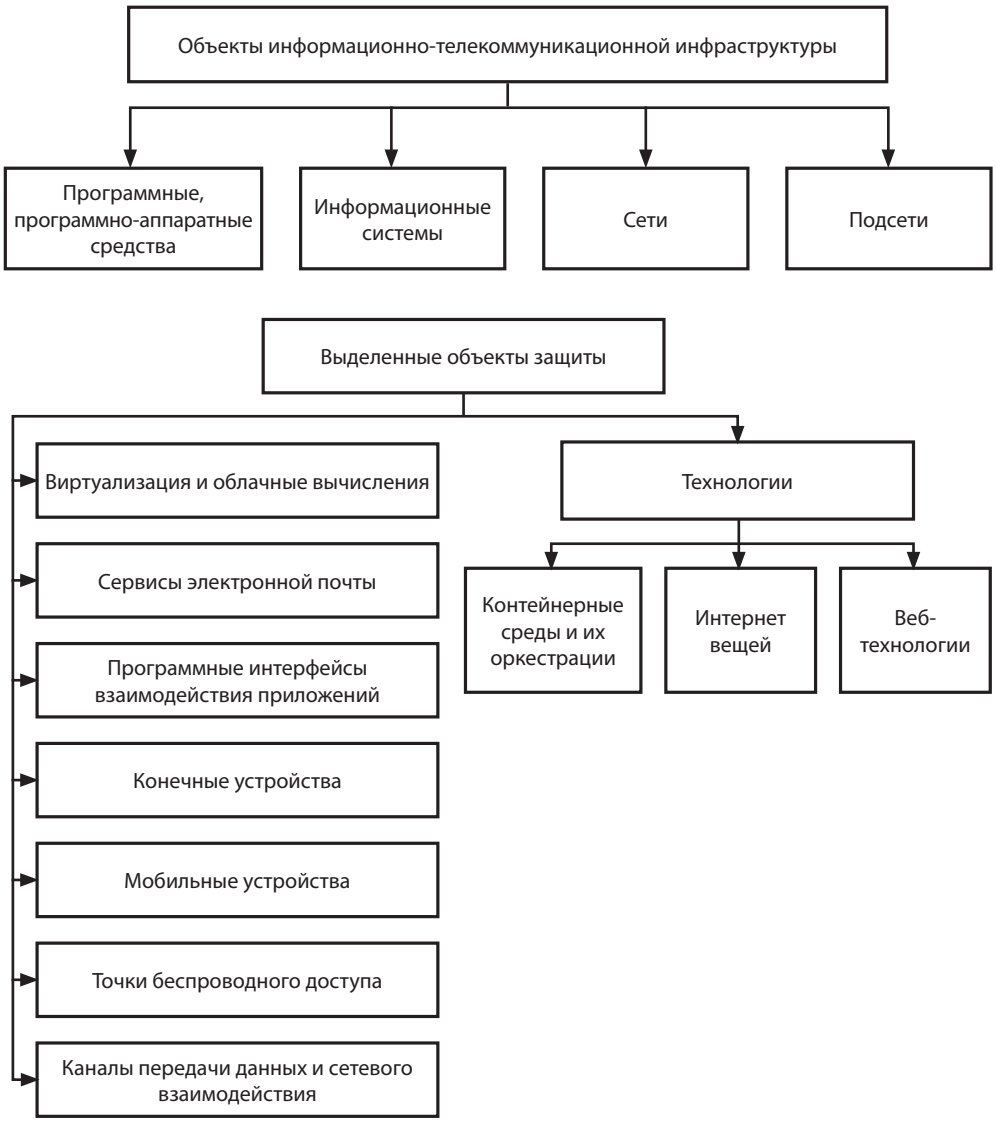

Рис. 1. Легальная модель объектов технической защиты информации

[13] Защита информации. Основные термины и определения. ГОСТ Р 50922-2006. М. : Стандартинформ, 2006. 12 с.

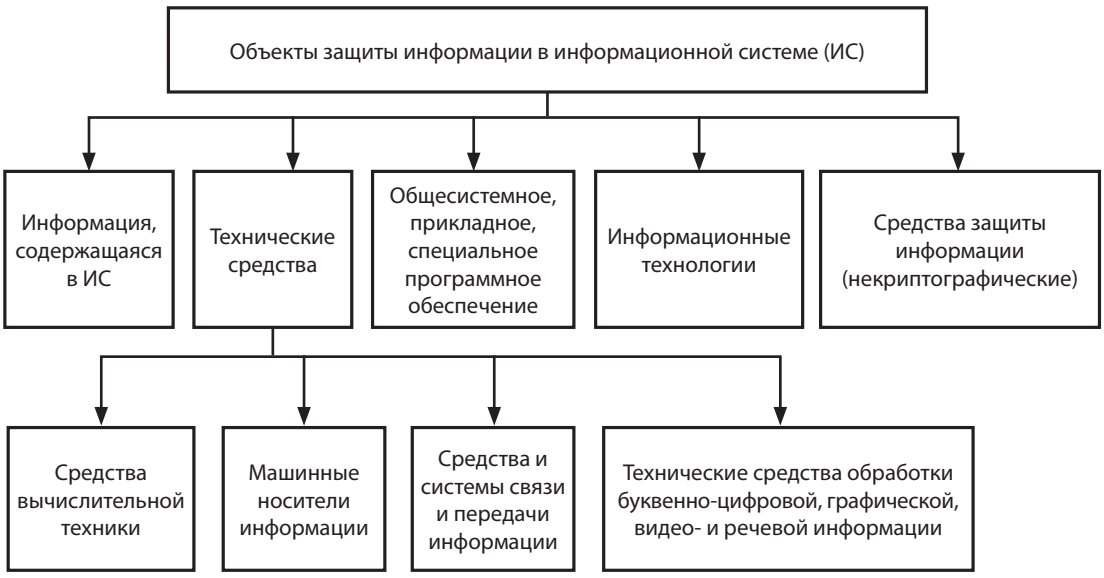

Рис. 2. Инфологическая модель объектов технической защиты информации некриптографическими средствами

из древнегреческого ὀρχήστρα (orchēstra). В музыкальном контексте «оркестрация» (или «оркестровка») закрепилась как технический термин со значениями: 1) распределение партий музыкального произведения между инструментами оркестра; 2) адаптация сочинения для исполнения оркестром; 3) искусство подбора тембров, сочетания инструментов, то есть создание оркестровой фактуры. Перенос термина «оркестрация» в современную область информационных технологий метафорически произошел в XX—XXI веках в сферы, где требуется координированное взаимодействие множества элементов информационной инфраструктуры и микросервисной архитектуры. Оркестрация означает централизованное управление цепочками задач или сервисами. Роль «дирижёра» выполняет программа или платформа (например, Kubernetes для контейнеров, Camunda для бизнес-процессов). Под оркестрацией данных понимается организация их перемещения и обработки между системами: запуск задач по расписанию, контроль зависимостей, уведомления о сбоях и др.

Действующую легальную модель в части защиты технологий (контейнерных средств и их оркестрации, интернета вещей, веб-технологий), на наш взгляд, можно дополнить в качестве самостоятельного объекта защиты технологией ИИ.

Указанное расхождение имеет существенное прикладное значение при реагировании на инциденты информационной безопасности: субъект правоприменения ориентируется на достижение целевого результата (например, предотвращение утечки данных), тогда как специалист по информационной безопасности — на выполнение полного комплекса регламентированных ГОСТом защитных мероприятий.

В случае если ИС является значимым объектом КИИ Российской Федерации, защита содержащейся в ней информации должна обеспечиваться в соответствии с нормативными правовыми актами, принятыми на основании статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и соответствующими требованиями ФСТЭК России.

Необходимо еще раз отметить, что чисто техническими средствами решить задачу построения эффективной системы защиты невозможно. Необходим комплекс организационных, законодательных, физических и технических мер[14].

Выводы

1. Различие в определении понятия «защита информации» создаёт разночтения в оценке инцидентов информационной безопасности, включая компьютерные инциденты.

2. Многоликость понимания объекта защиты в обеспечении ИБ и ЗИ размывает и расширяет фронт защиты информационных ресурсов, которые включают ИС, АСУ, ИКТС. С учётом динамики высокотехнологичных угроз в информационной сфере объект защиты не только приобретает более ясные и конкретные очертания, но и одновременно нуждается в терминологической определённости при использовании инновационных понятий.

3. Бурное развитие виртуализации, искусственного интеллекта и других технологий приводит к трансформации объекта защиты в требованиях регулятора,

[14] Лукацкий А. Атаки на информационные системы. Типы и объекты воздействия // Электроника: Наука, технология, бизнес. 2000. № 1 (25). С. 21.

в которых более четко конкретизируются целевые объекты, такие как конечные устройства, среда виртуализации, контейнерные среды и их оркестрации и др.

4. Широкое использование инновационных терминов (точки доступа, оркестрация, конечные устройства) не дополняется раскрытием их легального содержания, что затрудняет понимание и применение защитных мер на практике с учетом внедрения новых технологий, динамики и усложнения угроз ИБ информационных ресурсов.

Литература

1. Грибунин В.Г., Майоров С.А., Мурашко А.А. Об атаках на большие фундаментальные модели // Вопросы кибербезопасности. 2025. № 4 (68). С. 30—34.
2. Язов Ю.К., Авсентьев А.О. Проблемные вопросы управления защитой информации от утечки по техническим каналам с применением многоагентных систем // Вопросы кибербезопасности. 2024. № 6 (64). С. 85—97. DOI: 10.21681/2311-3456-2024-6-85-97.
3. Вершинина С.П., Вовченко А.В., Вовченко В.Н., Костюченко Е.Ю., Новохрестов А.К., Петриченко Г.В., Реуцких В.А., Солодков М.В., Сорокина М.А. Внедрение систем защиты в объекты КИИ / Под общ. ред. А.А. Шелупанова. Томск: В-Спектр, 2021. 92 с.
4. Комаров В.В., Буйневич М.В. Оценка и мониторинг защищенности информационных ресурсов как нештатная ситуация // Информационные технологии и телекоммуникации. 2023. Т. 11. № 4. С. 1—14. DOI: 10.31854/2307-1303-2023-11-4-1-14.
5. Будников С.А., Коваленко С.М., Бочарова А.И. Методика оценки эффективности систем безопасности автоматизированных систем управления // Вопросы кибербезопасности. 2023. № 3 (55). С. 2—12.
6. Марков Г.А., Крундышев В.М. Особенности обеспечения информационной безопасности в системах промышленного интернета вещей. С. 217—220. DOI: 10.18720/IEP/2024.1/53.
7. Печеникина М.В., Калач А.В. Современные системы защиты конечных устройств / Сборник материалов Всерос. науч.-практ. конф. «Актуальные проблемы деятельности подразделений УИС» (Воронеж, 20 октября 2022 г.). Воронеж : Издательско-полиграфический центр «Научная книга», 2022. С. 237—240.
8. Паршуков М.И. Теоретические основания формирования понятийного аппарата информационного права в Российской Федерации: дис. … д-ра юрид. наук: 5.1.2. Екатеринбург, 2026. 340 с.
9. Метельков А.Н. Комплексная инфологическая модель объектов защиты конфиденциальной информации // Вестник Санкт-Петербургского университета ГПС МЧС России. 2024. № 2. С. 80—90.
10. Авсентьев О.С., Томилова Э.А. Модели адаптивного управления защитой информации в процессе создания государственной информационной системы // Доклады ТУСУР, 2024, т. 27, № 4. С. 61—73.

SECTION:
INFORMATION PROTECTION METHODS AND SYSTEMS

TRANSFORMATION OF THE PROTECTED OBJECT IN THE CONTEXT OF MODERN INFORMATION SECURITY THREATS

***Metelkov A.N.*[15]**

Keywords: *changes, impact, protection, object, information security, technology, virtualization, artificial intelligence.*

Abstract

Purpose of work: *the purpose of the article is to show that modern doctrinal approaches to determining the object of protection in the field of information security and the existing conflicts in the classification of relevant incidents (including computer attacks) necessitate the allocation of priority objects of technical information protection and the regulatory*

[15] ***Aleksandr N. Metelkov****, Ph.D. (Law), Associate Professor, Associate Professor at the Department of Applied Mathematics and Information Technology Security, Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint Petersburg, Russian Federation.*

E-mail: metelkov5178@mail.ru

consolidation of their definitions, as well as criteria for classifying this category of objects of protection in the requirements of regulators. The work is aimed at identifying changes in the regulatory requirements for the object of protection to ensure the stability and security of information systems, data and infrastructure in the context of increased manufacturability and the number of computer attacks.

***Research methods:** using a systematic approach, the object of protection is studied as a set of interrelated components and their connections with the external environment, which forms new threats to the security of information resources. The change in the content of the object of protection is demonstrated by analyzing regulatory legal acts and standards, as well as comparative legal research of the regulatory requirements of the state regulator.*

***Results of the study:** the author highlights the features of the genesis of the object of protection in modern conditions, reveals the current understanding of the object of protection in the information infrastructure, reveals the tendency to complicate and specify the object of protection, as well as the orientation of the requirements of the state regulator to identify the most significant threats to information security and information security from a wide range of potential hazards. Taking into account the experience of repelling computer attacks on Russian critical and other information infrastructure, the efforts of information system operators are focused by the FSTEC of Russia on the most sensitive protection facilities. It is established that different approaches to the definition of the concept of "information protection" expand the scope of regulation and specify the boundaries of identification of threats to information security, including computer incidents. The introduction of new requirements for the organization of the information system protection system by clarifying the objects of protection contributes to the concentration of practical measures and measures to counteract current threats to information security and information security.*

References

1. Gribunin V.G., Maiorov S.A., Murashko A.A. Ob atakakh na bol'shie fundamental'nye modeli // Voprosy kiberbezopasnosti. 2025. No. 4 (68). S. 30—34.
2. Iazov Iu.K., Avsent'ev A.O. Problemnye voprosy upravleniia zashchitoi informatsii ot utechki po tekhnicheskim kanalam s primeneniem mnogoagentnykh sistem // Voprosy kiberbezopasnosti. 2024. No. 6 (64). S. 85—97. DOI: 10.21681/2311-3456-2024-6-85-97.
3. Vershinina S.P., Vovchenko A.V., Vovchenko V.N., Kostiuchenko E.Iu., Novokhrestov A.K., Petrichenko G.V., Reutskikh V.A., Solodkov M.V., Sorokina M.A. Vnedrenie sistem zashchity v ob"ekty KII / Pod obshch. red. A.A. Shelupanova. Tomsk : V-Spektr, 2021. 92 s.
4. Komarov V.V., Buinevich M.V. Otsenka i monitoring zashchishchennosti informatsionnykh resursov kak neshtatnaia situatsiia // Informatsionnye tekhnologii i telekommunikatsii. 2023. T. 11. No. 4. S. 1—14. DOI: 10.31854/2307-1303-2023-11-4-1-14.
5. Budnikov S.A., Kovalenko S.M., Bocharova A.I. Metodika otsenki effektivnosti sistem bezopasnosti avtomatizirovannykh sistem upravleniia // Voprosy kiberbezopasnosti. 2023. No. 3 (55). S. 2—12.
6. Markov G.A., Krundyshev V.M. Osobennosti obespecheniia informatsionnoi bezopasnosti v sistemakh promyshlennogo interneta veshchei. S. 217—220. DOI: 10.18720/IEP/2024.1/53.
7. Pechenikina M.V., Kalach A.V. Sovremennye sistemy zashchity konechnykh ustroistv / Sbornik materialov Vseros. nauch.-prakt. konf. "Aktual'nye problemy deiatel'nosti podrazdelenii UIS" (Voronezh, 20 oktiabria 2022 g.). Voronezh : Izdatel'sko-poligraficheskii tsentr "Nauchnaia kniga", 2022. S. 237—240.
8. Parshukov M.I. Teoreticheskie osnovaniia formirovaniia poniatiinogo apparata informatsionnogo prava v Rossiiskoi Federatsii: dis. … d-ra iurid. nauk: 5.1.2. Ekaterinburg, 2026. 340 s.
9. Metel'kov A.N. Kompleksnaia infologicheskaia model' ob"ektov zashchity konfidentsial'noi informatsii // Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii. 2024. No. 2. S. 80—90.
10. Avsent'ev O.S., Tomilova E.A. Modeli adaptivnogo upravleniia zashchitoi informatsii v protsesse sozdaniia gosudarstvennoi informatsionnoi sistemy // Doklady TUSUR, 2024, t. 27. No. 4. S. 61—73.