Аналитическая статья
УДК 316.421; DOI: 10.61260/2218-13X-2026-1-91-101

ЭСКИЗ СИСТЕМНОГО ПОДХОДА К ОПРЕДЕЛЕНИЮ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

✉Шакин Дмитрий Николаевич.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉dmitry_shakin@mail.ru

Аннотация. Актуальность исследования обусловлена возрастанием роли информации как стратегического ресурса и инструмента геополитического противоборства, что требует разработки научно обоснованных подходов к формированию и реализации стратегии информационной безопасности. Целью статьи является разработка эскиза системного подхода к определению стратегии информационной безопасности как модели управленческих действий, направленных на достижение целей обеспечения безопасности в информационной сфере. В работе стратегия рассматривается как комплексная система, включающая подсистемы политик информационной безопасности, внутренних стандартов и регламентов. Предложена классификация стратегий по уровням управления (глобальные, портфельные и функциональные), а также по объекту обеспечения безопасности (концептуальные, системные и объектовые стратегии). Раскрыта поведенческая сущность стратегии как модели деятельности организации, реализуемой через совокупность управленческих решений. Обоснована целесообразность применения риск-ориентированного подхода и цикла управления рисками информационной безопасности, включающего анализ обстановки, принятие решений, планирование, реализацию мероприятий и оценку эффективности. Кроме того, предложена модель оценки зрелости процессов управления информационной безопасностью на основе уровневого подхода. Перспективы дальнейших исследований связаны с углубленной разработкой методологии формирования стратегий информационной безопасности, развитием инструментов оценки их эффективности, а также исследованием взаимосвязи стратегии, государственной политики и экономических факторов в условиях развития информационного общества.

Ключевые слова: стратегия, информационная безопасность, риски, управление рисками

Для цитирования: Шакин Д.Н. Эскиз системного подхода к определению стратегии информационной безопасности // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 1. С. 91–101. DOI: 10.61260/2218-13X-2026-1-91-101

Analytical article

SKETCH OF A SYSTEMATIC APPROACH TO DETERMINING AN INFORMATION SECURITY STRATEGY

✉Shakin Dmitry N.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉dmitry_shakin@mail.ru

Abstract. The relevance of this research is determined by the increasing role of information as a strategic resource and a tool of geopolitical confrontation, which requires the development of scientifically based approaches to the formation and implementation of an information security strategy. The aim of the article is to develop a sketch of a systems approach to defining an information security strategy as a model of management actions aimed at achieving the goals of ensuring security in the information sphere.

In this paper, strategy is considered as a complex system, including subsystems of information security policies, internal standards and regulations. A classification of strategies by management levels (global, portfolio and functional), as well as by the object of security (conceptual, systemic and object strategies) is proposed. The behavioral essence of strategy as a model of an organization's activity, implemented through a set of management decisions is revealed. The feasibility of applying a risk-oriented approach and an information security risk management cycle, including situational analysis, decision-making, planning, implementation of measures and performance evaluation, is substantiated. In addition, a model for assessing the maturity of information security management processes based on a tiered approach is proposed. Prospects for further research are related to the in-depth development of methodology for the formation of information security strategies, the development of tools for assessing their effectiveness, as well as the study of the relationship between strategy, public policy and economic factors in the context of the development of the information society.

Keywords: strategy, information security, risks, risk management

For citation: Shakin D.N. A sketch of a systematic approach to defining an information security strategy // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2026. № 1. P. 91–101. DOI: 10.61260/2218-13X-2026-1-91-101

Введение

Среди известного многообразия стратегий от – классических военных до политических, экономических и социальных – стратегия информационной безопасности занимает место междисциплинарной категории. На современном этапе развития социума информация, кроме свойств стратегического национального ресурса, приобрела черты эффективного оружия в геополитической конкуренции, а борьба за информационное превосходство, под которым автор понимает способность более эффективно добывать, перерабатывать и распределять непрерывный поток информации о складывающейся в реальном масштабе времени обстановке, препятствуя противоборствующей стороне делать то же самое, занимает значимое место в общей системе противостояния государств и их союзов.

В связи с этим обеспечение информационной безопасности требует серьезного осмысления и системного взгляда на существующую проблему.

Стратегия информационной безопасности – ключевой документ стратегического планирования, обладающий нормативной правовой силой, который определяет цели, задачи, принципы и основные направления государственной политики в области безопасности в информационной сфере и термин, требующий определения его содержания в условиях глобального общества. В статье с позиции системного подхода предпринята попытка определения сущности и содержания стратегии информационной безопасности.

Основы стратегии информационной безопасности

Под стратегией (др. греч. στρατηγία – искусство полководца) автор понимает практику и методологию деятельности в сфере управления, определяющие приоритетные направления достижения главной цели и подлежащие корректуре с учетом изменений факторов и условий объективной реальности [1–3].

Любая стратегия вытекает из деятельности государства, и в силу этого основные цели и задачи стратегии, а также направления ее развития определяются государственной политикой и состоянием экономики страны. В самом общем виде они формулируются в законодательных актах и доктринах государства.

Следует отметить, что взаимосвязь политики со стратегией усложняется в деятельности союзов и коалиций государств, где требуется согласованная межгосударственная политика и гармонизированная межнациональная стратегия.

Кроме этого, объективно существует взаимосвязь стратегии с экономикой, которая проявляется в том, что в конечном итоге стратегия зависит от достигнутого уровня развития технологий, производства, информатизации и цифровой трансформации государственного управления [4]. Реализуя достижение научно-технического прогресса, экономика создает благоприятные условия для развития стратегии. Наряду с этим, стратегия оказывает обратное воздействие на экономику, которое состоит в том, что экономика в своем развитии учитывает тенденции развития и требования, выдвигаемые стратегией.

Рассматривая категории *сущность* и *содержание* стратегии, следует отметить, что они присущи всем общественным явлениям, в том числе и информационной безопасности [5].

Если содержание представляет собой совокупность элементов и процессов, образующих рассматриваемый предмет в совокупности его существенных признаков, то для его определения необходимо представление явлений, процессов или предметов и как единого целого, и как совокупности отдельных составных частей.

Содержание характеризует различные стороны сущности.

Исходя из понимания сущности предмета как относительно устойчивой и определяющей стороне предмета, представляются различные подходы к пониманию сущности стратегии.

Стратегия, в том числе и стратегия информационной безопасности, может быть представлена как управление деятельностью по достижению главной цели в долгосрочной перспективе, в основе которого заложены детерминированные процессы, поддающиеся контролю.

Вместе с тем, стратегия может рассматриваться в аспекте развития отношений внутри различных систем и их позиций во внутренней и внешней среде управления. При этом важно не принимать внешнюю среду как нечто неизменное, к чему система должна приспособиться. Напротив, необходимо определять методы и способы воздействия на внешнюю среду с целью создания благоприятных условий для достижения главной цели с заданной эффективностью.

В этом случае стратегия информационной безопасности представляется как система, состоящая из следующих элементов (подсистем):

– подсистемы политик информационной безопасности, содержащей порядок и правила проводимых мероприятий и принимаемых мер;

– подсистемы внутренних стандартов, содержащей требования к реализации политик;

– подсистемы внутренних регламентов, содержащей описание реализуемых процессов.

Стратегия разрабатывается на долгосрочный период, формулируется в достаточно общих выражениях, а далее конкретизируется и уточняется в документах среднесрочного и текущего периода.

При этом соотношение определяемых целей и решаемых задач определяется уровнем управления реализуемыми процессами.

Цели высокого уровня управления достигаются решением ряда задач, каждая из которых на более низком уровне управления становится целью, для достижения которой необходимо решить следующий «портфель задач». Рассматриваемая процедура может быть реализована в один или несколько потоков с использованием последовательного, параллельного методов планирования или их сочетания с учетом имеемых материальных, временных и иных ресурсов.

В случае появления непредвиденных факторов, условий и обстоятельств, не учтенных в принятой стратегии, возникает необходимость перехода к формулированию стратегических задач, которые в последующем должны послужить основой для определения замысла новой стратегии. Поэтому успешная реализация принятой стратегии невозможна без обратной связи.

Важнейшим этапом формирования стратегии является определение стратегических ориентиров (векторов стратегии). Известными видами векторов стратегии как направления и силы перемещения в процессе формирования стратегии являются совокупность стратегических целей, миссия стратегии, ее ценности и видение результата будущего с привязкой к конкретным этапам реализации стратегии.

Таким образом, можно утверждать, что стратегические ориентиры – это более высокий уровень принятия управленческих решений, а стратегия, сформированная при одном наборе ориентиров, должна изменяться при изменении стратегических ориентиров (векторов стратегии).

Кроме этого, аналогично описанной выше взаимосвязи целей и задач на различных уровнях управления возникает типичная иерархия, при которой элементы стратегии высших уровней управления на нижних уровнях управления превращаются в стратегические ориентиры.

Для классификации (классифицирования) стратегий может быть применен принцип распределения объектов (подмножеств) по известным признакам [6].

Автор предлагает определить следующие основные классы стратегий:

1. *Глобальные* (стратегического уровня) *стратегии* – по признаку достижения преимущества в рассматриваемой сфере деятельности, например, достижения информационного преимущества в информационной сфере.

2. *Портфельные* (оперативного уровня) *стратегии* – по признаку управления набором процессов в сфере деятельности, например, управление деятельностью по защите информации, управление уязвимостями информационных систем.

3. *Функциональные* (тактического уровня) *стратегии* – по признаку принадлежности к деятельности, имеющей приспособительное значение в зависимости от внешних и внутренних факторов и условий.

Кроме этого, различные стратегии информационной безопасности могут быть уточнены по признаку отношения к объекту обеспечения безопасности:

1. *Концептуальные стратегии*, рассматривающие в качестве объекта обеспечения информационной безопасности информационную сферу.

2. *Системные стратегии*, рассматривающие в качестве объекта обеспечения безопасности информационные системы, информационную инфраструктуру и информационный ресурс.

3. *Объектовые стратегии*, рассматривающие в качестве объекта защиты непосредственно информационный объект.

Выбор класса стратегии предполагает анализ разновекторных направлений развития процесса и изменения стратегических ориентиров с последующей оценкой и выбором лучшей стратегической альтернативы для реализации.

При этом достижение целей стратегии, осуществляемых посредством принятых политик, стандартов и регламентов, можно рассматривать как среднесрочные и краткосрочные планы реализации стратегии, в процессе которых каждый уровень управления решает свои определенные задачи и осуществляет закрепленные за ним функции.

В этом случае можно говорить о поведенческой сущности стратегии как модели поведения, которой следует система (организация) для достижения целей с заданной эффективностью. При поведенческом подходе к определению сущности стратегии ее содержанием служит портфель (набор) решений, используемый для определения цикла деятельности.

Подобный подход используется, например, Счётной палатой США (англ. The Government Accountability Office) которая является федеральным агентством, осуществляющим аудиторские, оценочные и аналитическо-следственные действия (мероприятия) [7].

Основным содержанием этой стратегии является взаимосвязанный цикл управления безопасностью реализующий риск-ориентированный подход как метод организации и проведения мероприятий, при котором выбор формы, продолжительности, периодичности осуществления действий определяется отнесением деятельности объекта к определённой категории риска и определённому классу опасности. Оценить вероятность реализации риска, которую можно привязать к различным количественным показателям деятельности объекта, позволяют ключевые индикаторы риска (англ. Key Risk Indicator).

Управление риском при реализации данной стратегии представляет собой систему профилактических (превентивных) и контрольных мероприятий, осуществляемых в целях обеспечения допустимого уровня риска причинения ущерба (вреда) в соответствующей сфере деятельности, не превышающей «риск-аппетитов» как величины и типа соответствующего риска, который организация готова достичь и (или) поддерживать.

Решающая роль в реализации рассматриваемого подхода принадлежит лицу, принимающему решение (ЛПР), которое несет персональную ответственность за действия или бездействие, ведущие к нарушению требований по обеспечению безопасности.

Деятельность ЛПР в реализации стратегии может быть рассмотрена в виде цикла управления рисками, состоящего из пяти последовательных этапов, представленных на рисунке [7].

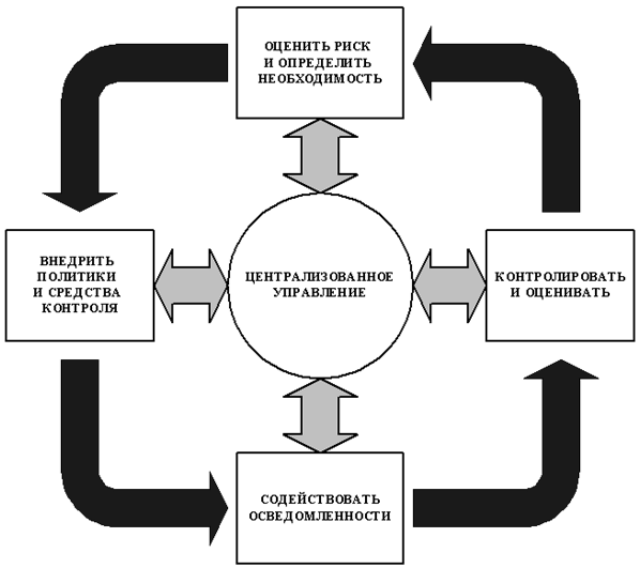

Рис. **Цикл управления рисками**

В целом весь цикл управления может быть представлен как последовательность действий, включающих в себя:

1. Уяснение целей и задач, определенных в стратегии с их уточнением в зависимости от результатов анализа меняющейся информационной обстановки.

2. Анализ и прогнозирование информационной обстановки с определением перечня важнейших и уязвимых объектов информационных систем (информационных объектов).

К важнейшим информационным объектам относятся информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети, деструктивное информационное воздействие на которые приведет к дезорганизации функционирования (ущербу) всей системы управления.

Под уязвимыми объектами понимаются информационные объекты, которые могут быть выявлены и в результате деструктивного воздействия на них переведены в неисправное и (или) неработоспособное состояние.

3. Определение замысла и выработка решения реализации стратегии.

4. Планирование мероприятий и мер по достижению целей стратегии с заданной эффективностью.

5. Доведение плана реализации стратегии до сотрудников с учетом их вовлеченности в процесс реализации стратегии.

6. Всестороннее обеспечение процесса реализации стратегии, в том числе дополнительная подготовка (обучение) сотрудников с учетом действующих факторов и условий.

7. Контроль выполнения спланированных мероприятий и мер.

8. Оценку эффективности достижения поставленных целей.

Ожидаемая эффективность реализации стратегии оценивается посредством критериев оценки эффективности, например, «полезности» проведенных мероприятий и внедренных мер защиты. Оценка полезности позволяет получить ответ на вопрос о том, как изменились по абсолютному или относительному значению показатели эффективности обеспечения безопасности государства с учетом вклада от реализации стратегии информационной безопасности.

Для централизованного управления рисками информационной безопасности целесообразно определить оперативную группу в составе от 5 до 10 сотрудников.

Возглавляет группу руководитель органа (организации) или уполномоченное им лицо.

По решению руководителя органа (организации) в состав группы включаются:

1) работники органа (организации), являющиеся специалистами в области осуществляемых видов деятельности, в области информационных технологий и связи, по эксплуатации основного технологического оборудования, а также работники, на которых возложены функции обеспечения безопасности объекта защиты;

2) работники органа (организации), на которых возложены функции обеспечения безопасности информационных объектов;

3) работники подразделения по защите информации ограниченного доступа в органе (организации);

4) работники структурного подразделения по гражданской обороне и чрезвычайным ситуациям или работники, уполномоченные на решение задач в этой области.

Кроме этого, в оперативную группу могут включаться работники иных подразделений органа (организации), в том числе финансово-экономического подразделения, а также представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативному правовому регулированию в установленной сфере деятельности по согласованию с ними.

Оперативная группа является:

– организатором процесса реализации стратегии, обеспечивающим непрерывный анализ рисков информационной безопасности и реализацию компенсирующих мер;

– центром компетенций для подразделений организаций, реализующим поиск новых знаний и оказание консультационных высокопрофессиональных услуг;

– системой оперативного доведения до руководителя органа (организации) правдивой информации о состоянии информационной безопасности, выполняемых мероприятиях, принимаемых мерах и результатах оценки их эффективности.

Оперативная группа позволяет централизовано управлять всем циклом, исключая дублирование задач различными подразделениями органа (организации).

При решении задач всестороннего обеспечения процесса реализации стратегии проводится учет имеющихся ресурсов, их распределение и пополнение в соответствии с реализуемыми задачами и условиями информационной обстановки. С этой целью разрабатываются специальные программы, выполнение которых должно способствовать развитию ресурсов, в том числе программы повышения квалификаций и (или) профессиональной переподготовки сотрудников органа (организации) по вопросам информационной безопасности.

Сотрудники должны знать алгоритм действий при утечке информации (данных) или реализации компьютерной атаки на информационную инфраструктуру органа (организации).

Сотрудники органа (организации) должны обладать соответствующими знаниями, умениями и навыками в различных аспектах реализации порядка действий по обеспечению информационной безопасности в случаях несанкционированного доступа к защищаемой информации [8], при реализации угроз безопасности информации типа «отказ в обслуживании», угроз, связанных с внедрением нежелательного контента на информационном ресурсе или угроз, связанных с внедрением вирусов-шифровальщиков.

В общем случае порядок действий сотрудников органа (организации) должен предусматривать:

– информирование руководителя органа (организации) и оповещение сотрудников с проведением инструктажа о мерах безопасности, а также доведение информации до федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности в установленные нормативными правовыми актами сроки;

– выявление и анализ масштаба и критичности (ущерба) компьютерного инцидента с охранением (по возможности) образцов вредоносного кода, которые должны быть изолированы и размещены в безопасной среде для дальнейшего анализа и проведения расследования;

– нейтрализацию последствий компьютерных атак в сочетании с полной проверкой информационных систем для обнаружения вредоносных программ и учетных записей с целью выявления фактов их компрометации;

– восстановление (минимизации ущерба) данных с установкой актуальных обновлений безопасности с предварительным тестированием их работоспособности и совместимости;

– взаимодействие с организациями, выполняющими работы и оказывающими услуги по защите информации на основании лицензии на указанный вид деятельности;

– актуализацию принятых политик безопасности и внедрение мер по совершенствованию системы информационной безопасности с учетом результатов проведенного расследования компьютерного инцидента для повышения устойчивости органа (организации) к актуальным угрозам безопасности информации.

Требования и содержание политик безопасности зависят от результатов прогнозирования, выявления и оценки угроз безопасности информации, полученных на первом этапе цикла управления.

Политики безопасности более высокого уровня управления должны определять цели, представленные в политиках безопасности более низкого уровня управления информационной безопасностью. Политики высокого уровня определяют обязательные требования, принятые руководителем органа (организации), в то время как политики низкого уровня содержат практические руководства, обязательные для структурных подразделений, на которые возложены функции по обеспечению информационной безопасности, подразделения, обслуживающие информационные системы, и подразделения, обеспечивающие функционирование этих систем. Такой подход делает политики безопасности доходчивыми для понимания сотрудников, непосредственно выполняющих работы по обеспечению информационной безопасности и сотрудников, участвующих в реализации критических процессов.

Критические процессы являются внутренними в цикле деятельности органа (организации) и представляют собой явление, которое при ненадлежащей организации и (или) несоблюдении условий может представлять фактическую или потенциальную опасность для обеспечения качества продукции (услуг) при незначительном изменении параметров воздействия на систему. По степени влияния на конечный результата среди критических процессов выделяют:

– основные (горизонтальные) процессы (производственные процессы, процессы жизненного цикла, бизнес-процессы);

– управленческие (вертикальные) процессы (процессы менеджмента, организационные процессы);

– вспомогательные процессы (обеспечивающие процессы и поддерживающие процессы);

Содержание стратегии информационной безопасности определяют именно основные критические процессы и их взаимосвязь с типовыми объектами, подлежащими защите (объектами защиты).

На этапе содействия осведомленности пользователей о содержании политик информационной безопасности необходимо обеспечить доступ к актуальным версиям документа до момента предоставления доступа к защищаемым ресурсам.

Следует учитывать, что сотрудники, выполняющие функции по администрированию безопасности, обладают аутентификационной информацией, а также информацией о наличии в информационных системах уязвимостей и возможностью удаленного доступа. Доступность такой информации для сторонних лиц может быть использована для несанкционированного доступа к защищаемой информации, нарушения ее целостности и конфиденциальности.

С целью исключения или максимального затруднения несанкционированного распространения указанной информации рекомендуется обеспечить мониторинг их действий в информационной системе, обратив особое внимание на факты копирования (переноса) информации, содержащейся в информационной системе, на съемные носители информации, передачи электронных документов по электронной почте, установки и запуска стороннего программного обеспечения. В случае прекращения деятельности сотрудника в органе (организации) удалить учетные записи для доступа к электронной почте и иным сегментам информационной системы, провести полную инвентаризацию программного обеспечения и данных, содержащихся на его автоматизированном рабочем месте, на предмет наличия стороннего программного обеспечения и каналов удаленного доступа и удалить неиспользуемое в работе программное обеспечение. Необходимо выполнить превентивный набор мер, направленных на определение перечня сегментов информационной системы, к которым сотрудник имел доступ, и обеспечить внеплановую смену паролей. До смены паролей обеспечить мониторинг удаленного доступа к этим сегментам информационной системы.

Для исследования зрелости процессов управления, реализуемых стратегией информационной безопасности, может быть применена известная интегрированная модель зрелости возможностей Capability Maturity Model Integration, реализующая методологический подход для улучшения процессов в органах (организациях) с целью повышения эффективности их функционирования через оценку и развитие имеемых возможностей по нескольким, предлагаемым автором, уровням зрелости:

1. Бессистемный (турбулентный) уровень, при котором реализуемые процессы управления информационной безопасностью в значительной степени зависят от уровня индивидуальной подготовки отдельных сотрудников, а орган (организация) не обеспечивает системность в достижении поставленной цели с заданной эффективностью. Ключевые области процесса: создание базовой инфраструктуры управления.

2. Начальный (базовый) уровень, на котором внедряются базовые практики управления, реализуются основные (ключевые, критические) и вспомогательные структурированные процессы, направленные на детальный анализ каждого аспекта деятельности органа (организации) и позволяющие устранить те элементы, которые делают управление неэффективным. Ключевые области процесса: управление с учетом факторов и условий, имеемых ресурсов и возможных рисков, мониторинг, контроль и устранение выявленных нарушений. Достижение поставленной цели с заданной эффективностью носит вероятностный характер и не может быть достаточно адекватно описано детерминистическими категориями.

3. Определенный (детерминированный) уровень, на котором структурированные процессы стандартизированы, согласованы и документированы, а их реализацию обеспечивают последовательность и предсказуемость с четкими ролями и обязанностями сотрудников органа (организации). Ключевые области процесса: интегрированное управление информационной безопасностью с гарантированным достижением поставленной цели с заданной эффективностью.

4. Развитый (инновационный) уровень, на котором реализуется стратегические ориентиры (векторы стратегии). Орган (организация) активно адаптируется к факторам и условиям и оптимизирует структурированные процессы. Ключевые области процесса:

организационные инновации в управлении, причинно-следственный анализ и решения, гарантирующие предотвращение повторных проблем посредством анализа первопричин. Ключевые области процесса: инновационное управление информационной безопасностью с возможностью превышения заданной эффективности.

При корректировке стратегии следует избегать характерных ошибок, к числу которых относятся:

– постановка нереалистичных (амбициозных) целей, которые невозможно достичь с имеющимися ресурсами;

– отсутствие адаптации стратегии в ответ на изменения факторов и условий, вследствие чего она утратит свою эффективность;

– недооценка противоборствующей стороны (эвентуальных конкурентов), способная привести к утрате имеемых позиций.

В заключение следует отметить, что реализация описанной стратегии информационной безопасности, соответствующей по предложенной автором классификации – системной стратегии, является лишь первым шагом на пути построения эффективной системы обеспечения информационной безопасности.

Заключение

Реальные условия развития социума объективно показывают, что при определении направлений развития стратегии информационной безопасности ее следует рассматривать как высшую область государственной деятельности.

По существу, она может быть охарактеризована как специфически государственная форма активного отношения к окружающему миру, содержание которой составляет его целенаправленное изменение с целью реализации единой государственной политики для обеспечения безопасности страны и защиты интересов граждан при использовании информационных технологий.

Опережающее развитие теории информационной безопасности, опирающееся на объективные тенденции развития информационного общества, должно способствовать более точному прогнозированию и оценке угроз в информационной сфере, повышению обоснованности разработки основных направлений стратегии обеспечения информационной безопасности, а также целенаправленной подготовке всех элементов государственной системы защиты информации с учетом меняющихся факторов и условий.

Сегодня становится очевидным, что интересы информационной безопасности государства требуют новых подходов к связям между стратегией, политикой и экономикой. Зависимости стратегии от экономики, политики и ее связь с безопасностью государства объективно нуждаются в наполнении обратных связей новым содержанием.

Именно такой характер реально существующих, но недостаточно еще теоретически исследованных и систематизированных связей, вызывает необходимость уточнения категории «Стратегия информационной безопасности».

Определение стратегии информационной безопасности как термина и документа стратегического планирования еще требует своего дальнейшего осмысления.

Список источников

1. Большой энциклопедический словарь / гл. ред. А.М. Прохоров. М.: Советская энциклопедия; СПб.: Фонд «Ленингр. Галерея», 2002. 1628 с.

2. О Стратегии национальной безопасности Российской Федерации: Указ Президента Рос. Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

3. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 09 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности / М.А. Вус [и др.] // Информатизация и связь. 2012. № 9. С. 7–15. EDN PUQQQL.

5. Шакин Д.Н. Эскиз системного подхода к определению сущности и содержания информационной безопасности // Информационные технологии и телекоммуникации. 2013. Т. 1. № 3. С. 52–60. EDN RUMBWH.

6. Ансофф И. Стратегический менеджмент. Классическое издание. СПб.: Питер, 2009. 344 с.

7. Информационная безопасность: монография / С.М. Доценко [и др.]. М.: Оружие и технологии, 2009. 256 с.

8. Буйневич М.В., Матвеев А.В., Смирнов А.С. Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2022. № 3. С. 1–17. EDN OGPXZX.

References

1. Bol'shoj enciklopedicheskij slovar' / gl. red. A.M. Prohorov. M.: Sovetskaya enciklopediya; SPb.: Fond «Leningr. Galereya», 2002. 1628 s.

2. O Strategii nacional'noj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 2 iyulya 2021 g. № 400. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

3. O Strategii razvitiya informacionnogo obshchestva v Rossijskoj Federacii na 2017–2030 gody: Ukaz Prezidenta Ros. Federacii ot 09 maya 2017 g. № 203. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

4. Eskiz sistemnogo podhoda k formirovaniyu ponyatijnogo apparata informacionnoj bezopasnosti / M.A. Vus [i dr.] // Informatizaciya i svyaz'. 2012. № 9. S. 7–15. EDN PUQQQL.

5. Shakin D.N. Eskiz sistemnogo podhoda k opredeleniyu sushchnosti i soderzhaniya informacionnoj bezopasnosti // Informacionnye tekhnologii i telekommunikacii. 2013. T. 1. № 3. S. 52–60. EDN RUMBWH.

6. Ansoff I. Strategicheskij menedzhment. Klassicheskoe izdanie. SPb.: Piter, 2009. 344 s.

7. Informacionnaya bezopasnost': monografiya / S.M. Docenko [i dr.]. M.: Oruzhie i tekhnologii, 2009. 256 s.

8. Bujnevich M.V., Matveev A.V., Smirnov A.S. Aktual'nye problemy podgotovki specialistov v oblasti informacionnoj bezopasnosti MChS Rossii i konstruktivnye podhody k ih resheniyu // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MChS Rossii». 2022. № 3. S. 1–17. EDN OGPXZX.

Информация о статье:
Статья поступила в редакцию: 12.12.2025; одобрена после рецензирования: 10.03.2026;
принята к публикации: 13.03.2026

Information about the article:
The article was submitted to the editorial office: 12.12.2025; approved after review: 10.03.2026;
accepted for publication: 13.03.2026

Информация об авторах:
Шакин Дмитрий Николаевич, профессор кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат военных наук, доцент, e-mail: dmitry_shakin@mail.ru, SPIN-код: 2620-6710

Information about authors:
Shakin Dmitry N., 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 military sciences, associate professor, e-mail: dmitry_shakin@mail.ru, SPIN: 2620-6710