DOI 10.37882/2223-2966.2024.8.16

МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЛОЖНЫХ СИСТЕМАХ: ИНТЕГРАЦИЯ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

INFORMATION SECURITY MEASURES IN COMPLEX SYSTEMS: INTEGRATION OF MODERN DIGITAL TECHNOLOGIES

K. Kashirin

Summary. Complex systems are an integral companion of human activity. In the context of digitalization, information risks and cyber threats are increasing, which requires the application of information security measures. The article presents the key processes and results of complex systems, provides an overview of existing digital technologies for information protection in information systems, and presents models for countering threats to information security in complex systems using advanced technologies.

Keywords: complex systems, information security, cyber threats, digital technologies, counteraction models.

Каширин Кирилл Дмитриевич
Московский авиационный институт
ki.kashirin@yandex.ru

Аннотация. Сложные системы — неотъемлемый спутник человеческой деятельности. В условиях цифровизации повышаются информационные риски и киберугрозы, что требует применения мер обеспечения информационной безопасности. В статье представлены ключевые процессы и результаты сложных систем, проведён обзор существующих цифровых технологий для защиты информации в информационных системах, а также представлены модели противодействия угрозам информационной безопасности в сложных системах, использующие передовые технологии.

Ключевые слова: сложные системы, информационная безопасность, киберугрозы, цифровые технологии, модели противодействия.

В XXI веке человеческое взаимодействие все чаще носит цифровой характер. По мере научно-технологического прогресса, во многом основанного сегодня на использовании передовых цифровых технологий, системы взаимодействия становятся всё более сложными. К наиболее общим примерам сложных систем можно отнести экосистемы планеты, глобальный климат, мозг человека, иммунную систему, города и городские системы (транспортные, коммуникационные, энергетические и т. д.), Вселенную и др. Сложные системы получили свое название потому, что они состоят из множества компонентов. Сложные системы проявляются в различных формах, будь то физические, биологические или социальные. Ввиду столь широкого спектра рассматриваемых объектов может возникнуть вопрос о целесообразности их изучения в рамках единой концептуальной парадигмы. Однако, несмотря на то что многие научные дисциплины традиционно исследуют составляющие систем сами по себе, наука о сложных системах направлена на понимание взаимосвязей между элементами внутри системы. В качестве примера понимания сути сложных систем можно показать различие между академическими дисциплинами и изучением сложных систем (рис. 1). На представленном изображении можно наблюдать примеры систем, которые, несмотря на наличие однотипных компонентов (молекулы, клетки и люди), демонстрируют разнообразие отношений между этими элементами. На рисунке каждая строка иллюстрирует определённый тип взаимодействия компонентов. Для случайных систем характерно независимое поведение их элементов, т. е. действия каждого компонента не оказывают влияния на остальные. Примером когерентных систем служат те, в которых элементы демонстрируют идентичное поведение; в таких системах параметры одной части системы (расположение, ориентация и скорость одной части) полностью определяют аналогичные параметры остальных частей. Коррелированные системы занимают промежуточное положение между этими двумя крайними типами. В таких системах поведение компонентов связано, однако не до такой степени, чтобы каждый элемент вел себя идентично другим. Например, форма одной части снежинки имеет корреляцию с формой остальных частей системы, но эта взаимосвязь не является абсолютной.

Также можно выделить ключевые процессы и результаты функционирования сложных систем. Изменчивое состояние, воспринимаемое как норма для таких систем, может привести к различным явлениям, включая фазовые переходы, катастрофические сломы и непредсказуемые последствия, что показано ниже (табл. 1).

Центральной парадигмой для моделирования динамики взаимодействующих систем в настоящее время считаются сложные сети. Тем не менее, такие сети в основном ограничены описанием взаимодействий между парами элементов. В реальности же системы зачастую характеризуются более сложными и высокоуровневыми

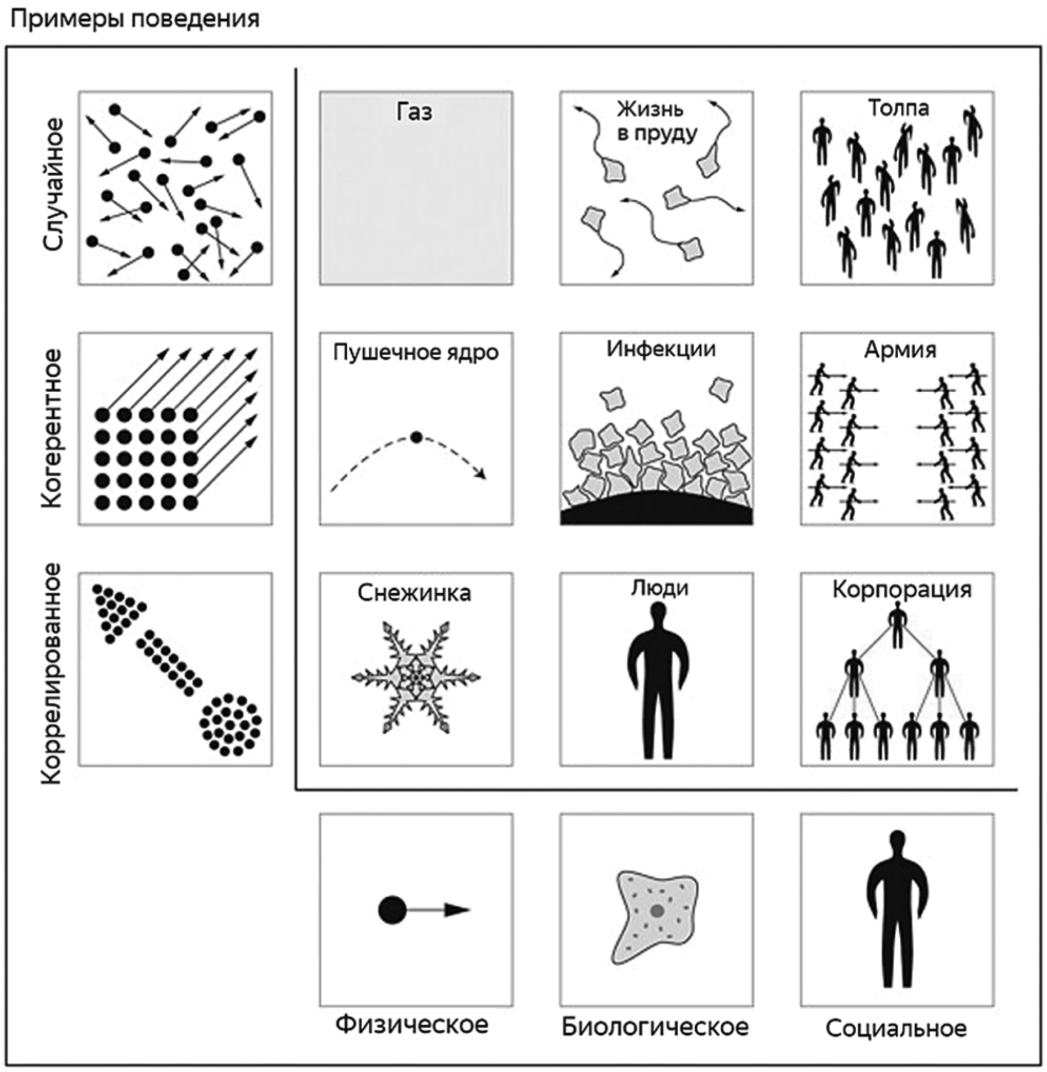

Рис. 1. Взаимосвязь компонентов систем: примеры поведения

Источник: [9]

Таблица 1.

Ключевые процессы и результаты сложных систем

Теории сложности	Процессы	Результаты
Эмерджентность	Ситуации неравновесия: напряжения, триггеры и небольшие события, выходящие за рамки нормы; положительная обратная связь и всплески усиления; фазовые переходы; самоорганизация	Непредсказуемые результаты: новые структуры, узоры и свойства внутри системы (например, распределённое лидерство), новый уровень анализа (например, сеть) или коллективное явление (например, коллективное действие); эмерджентность может принимать две формы: композиция или компиляция.
Коэволюция	Взаимозависимость и перекрёстные взаимосвязи; многоуровневая динамика; двусторонняя или обратная причинно-следственная связь	Взаимные влияния; взаимные адаптации и изменения с течением времени
Хаос	Чувствительность к начальным условиям; ограниченная траектория (например, странный аттрактор); зависимость от времени и необратимая динамика	Катастрофические сбои (например, системный риск, нарушения кибербезопасности); эскалация причин, ведущая к разрушительным социальным последствиям (например, нарушению жизни на большом масштабе)
Масштабируемая динамика	Нестабильность и большие вариации; единая причина, ведущая к цепочке взаимосвязанных событий	Самоподобие на разных масштабах; положительные или отрицательные крайние результаты; фрактальная динамика; степенные законы

Источник: [3]

взаимодействиями, включающими группы, состоящие из трех и более элементов [2].

В XXI веке к числу наиболее сложных систем присоединился Интернет — всемирная паутина, охватывающая сегодня миллионы сайтов, социальных сетей, пользователей и их взаимодействий. Согласно данным DataReportal, сегодня интернетом пользуются 5,35 млрд человек, или 66 % всего населения планеты [12].

В рамках капиталистической мир-системы общественное развитие при прочих равных условиях считается свободным. Как утверждал Валлерстайн, «свобода большинства подразумевает активное вовлечение большинства. Она подразумевает, что большинство имеет доступ к информации» [1, С. 196]. Действительно, с помощью современных средств коммуникации (главным образом, Интернета) большинство людей имеет возможность получать информацию и передавать ее другим практически мгновенно. Современного человека, проживающего в развитых и развивающихся странах и регионах, уже трудно представить без смартфона или персонального компьютера; компании в условиях усиливающейся конкурентной борьбы внедряют цифровые технологии в бизнес или изначально выстраивают цифровой бизнес; государства также стремятся к цифровому взаимодействию с населением. Все эти тенденции в современной научной литературе принято объединять под общим названием «индустрия 4.0», или четвёртая промышленная революция, которое отражает стремительное развитие технологий и их интеграцию в реальность, в частности, в реальные бизнес-процессы. Автоматизация, роботизация, искусственный интеллект, киберфизические системы, Интернет вещей — все эти и многие другие технологии и процессы формируют новую, «дополненную социальную реальность» [10]. Усложнение современного общества усиливается за счёт гиперсвязей и взаимных зависимостей, охватывающих людей, технологические артефакты, процессы и учреждения. Сложность оказывает влияние на человеческие возможности и опыт во всех аспектах. В ответ на вызовы, обусловленные цифровизацией, как отдельные индивиды, так и компании активно прибегают к цифровым решениям, что позволяет им эффективно решать возникающие непростые задачи [3]. В частности, одной из основных угроз в контексте цифровизации является информационная безопасность. В настоящее время появляется всё больше способов нарушения информационной безопасности. По данным лаборатории Касперского, в конце мая 2024 года по всему миру совершалось

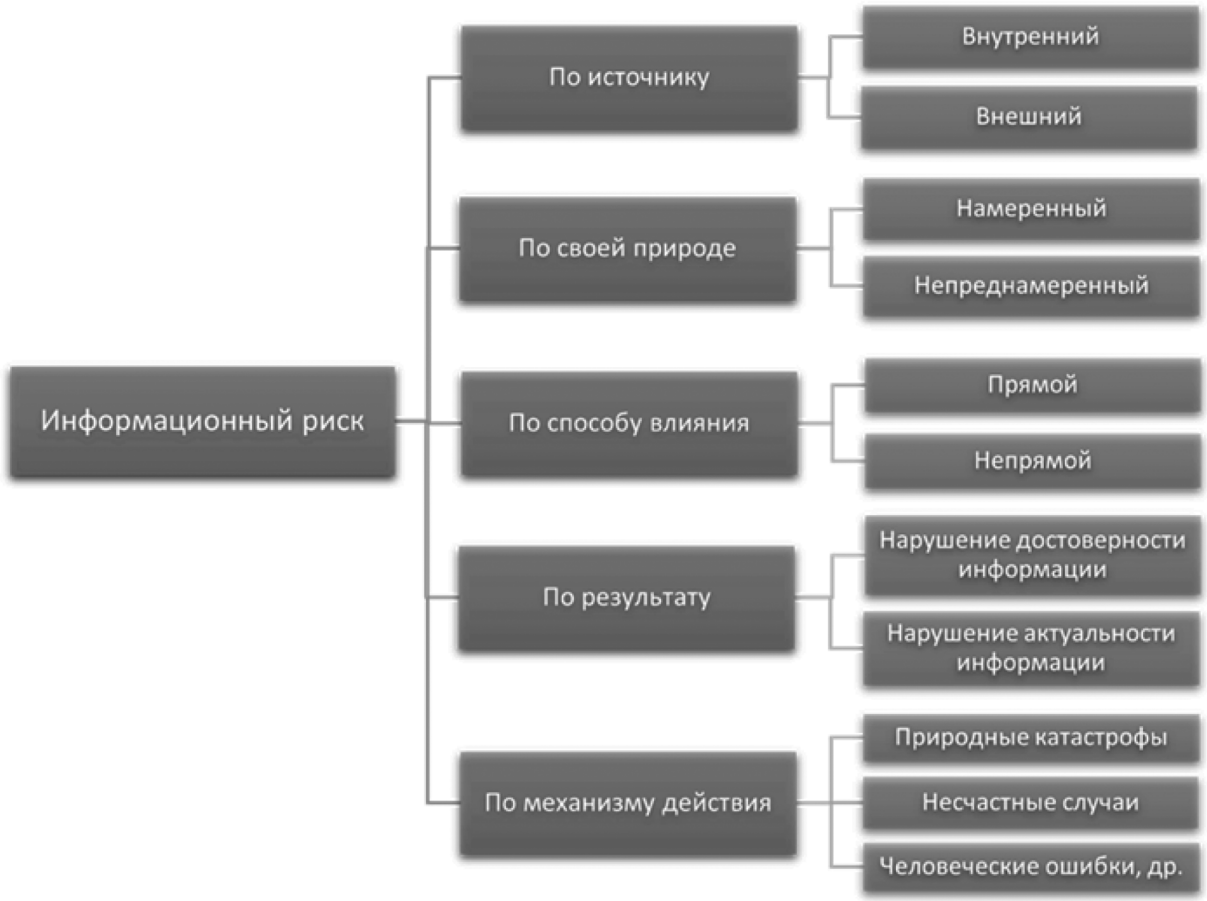

Рис. 2. Классификация информационных рисков

Источник: [5]

14,1 миллиона кибератак в режиме реального времени, при этом наиболее заражаемыми странами являются Россия, Китай, США, Бразилия и Вьетнам [11].

Бурное развитие информационных технологий и связанных с ними услуг, таких как Интернет вещей, в значительной степени увеличило необходимость информационной безопасности для защиты ценных данных, которые сохраняются в этих системах. При этом в настоящее время безопасность информации организаций всё чаще определяется эффективностью деятельности их специалистов в области информационной безопасности, которые должны обладать навыками сбора, анализа и использования данных, а также нести ответственность за обеспечение защиты пользовательской информации [6].

Развитие культуры информационной безопасности в организациях играет ключевую роль в снижении угроз, связанных с утечкой информации и другими инцидентами. Становление культуры информационной безопасности началось уже давно и остается крайне важным в наше время. Современные научные исследования и практика бизнеса направлены на противодействие различным рискам, угрожающим защите информации. Формирование и поддержание культуры информационной безопасности стало важным элементом управления рисками [4].

Информационная безопасность сегодня вышла за рамки технических аспектов и превратилась в одну из ключевых управленческих задач текущего десятилетия. Усиленная цифровизация, особенно после кризиса, вызванного пандемией COVID-19, еще более обострила потребность в глубоких знаниях в области информационной безопасности среди руководителей компаний [8].

Можно выделить такие проблемы информационной безопасности, как идентификация, контроль доступа, целостность данных, конфиденциальность информации, неприкосновенность (неопровержимость) данных [7]. В общем смысле существует большое количество информационных рисков (рис. 2).

С течением времени сложность информационных систем продолжает расти, что делает вопросы обеспечения информационной безопасности все более значимыми для любой организаций [10]. В этом контексте особое внимание уделяется интеграции современных цифровых технологий и совершенствованию методов защиты информации.

Анализ современной научной литературы позволил выделить ключевые цифровые технологии для защиты информации в информационных системах (табл. 2).

Эти современные цифровые технологии играют ключевую роль в обеспечении информационной безопасно-

Таблица 2.
Обзор существующих цифровых технологий для защиты информации в информационных системах

Технология	Применение для защиты информации в информационных системах
Криптография	Применяется для шифрования конфиденциальной информации, обеспечения безопасности транзакций и проверки подлинности цифровых подписей
Контроль доступа	Используется для реализации политик безопасности путем предоставления или отказа в доступе к ресурсам на основе учетных данных пользователя и заранее определенных правил
Сетевая безопасность	Применяется для защиты сетевой инфраструктуры с помощью брандмауэров, систем обнаружения вторжений и безопасных протоколов
Безопасность конечных устройств	Применяется для защиты устройств с помощью антивирусного программного обеспечения и инструментов обнаружения угроз
Безопасность данных	Обеспечивает защиту данных с помощью шифрования, безопасного контроля доступа и технологий предотвращения утечек данных
Облачная безопасность	Обеспечивает безопасность облачных систем с помощью шифрования, контроля доступа и посредников безопасности облачного доступа
Безопасность приложений	Обеспечивает защиту приложений с помощью тестирования безопасности и развертывания веб-брандмауэров приложений
Системы SIEM (управление информацией о безопасности и событиями безопасности)	Используются для сбора, анализа и мониторинга журналов безопасности и событий из различных систем, что позволяет быстро обнаруживать и реагировать на потенциальные инциденты безопасности
Автоматизация безопасности	Повышает безопасность за счет автоматизации процессов обнаружения и реагирования на угрозы, что сокращает время и усилия, необходимые для идентификации и устранения угроз
Безопасность блокчейна	Обеспечивает защиту данных в блокчейн-сетях с помощью криптографических методов и механизмов консенсуса, что поддерживает безопасность и целостность децентрализованных транзакций и записей
Модель нулевого доверия	Применяется для строгого контроля доступа и постоянной проверки пользователей и устройств, обеспечивая доступ только авторизованным лицам к критическим системам и данным
Искусственный интеллект и машинное обучение	Используются для повышения безопасности за счет выявления аномалий и прогнозирования потенциальных угроз
Физическая безопасность	Применяются для защиты физических активов с помощью биометрического контроля доступа и систем мониторинга окружающей среды

Источник: составлено автором на основе обобщения литературы

Таблица 3.

Модели противодействия угрозам информационной безопасности в сложных системах, использующие передовые технологии

Модель	Используемые технологии	Ключевые компоненты	Примеры применения
Анализ поведения и обнаружение аномалий	Машинное обучение, искусственный интеллект	Сбор данных, выделение признаков, обучение моделей, обнаружение аномалий, автоматизированная реакция	Обнаружение вторжений, выявление мошенничества, мониторинг инсайдерских угроз
Архитектура Zero Trust (нулевое доверие)	Облачные вычисления, микросегментация, управление идентификацией	Микросегментация, непрерывная аутентификация, принцип минимальных привилегий, безопасность конечных устройств	Защита облачных сред, обеспечение безопасности удаленной работы, безопасность корпоративных сетей
Безопасность на основе блокчейна	Блокчейн, криптография	Децентрализация, неизменность, механизмы консенсуса, умные контракты	Защита цепочек поставок, защита данных в здравоохранении, предотвращение цифрового мошенничества
Платформы искусственного интеллекта для киберугроз	Искусственный интеллект, анализ больших данных	Сбор данных, распознавание шаблонов, прогнозная аналитика, автоматизированная реакция	Проактивное выявление угроз, усиление центров управления безопасностью, оперативная информация
Квантовая криптография и постквантовая безопасность	Квантовые вычисления, продвинутые криптографические алгоритмы	Квантовое распределение ключей, постквантовые алгоритмы, квантовая генерация	Защищенная связь для военных, защита критической инфраструктуры

Источник: составлено автором на основе обобщения литературы.

сти в сложных системах, предоставляя возможности для формирования разнообразных моделей для противодействия угрозам.

К основным моделям противодействия информационным рискам в сложных системах, использующим передовые технологии, можно отнести следующие: модель поведенческого анализа и обнаружения аномалий, архитектура нулевого доверия (ZTA), модели безопасности на основе блокчейна, платформы для анализа угроз на основе искусственного интеллекта, квантовая криптография и постквантовые модели безопасности. Их ключевые компоненты и примеры применения представлены ниже (табл. 3).

Таким образом, современные цифровые технологии активно используются для мониторинга, предупреждения и обнаружения нарушений информационной безопасности. Сегодня можно выделить пять основных моделей: модель поведенческого анализа и обнаружения аномалий, архитектура нулевого доверия (ZTA), модели безопасности на основе блокчейна, платформы для анализа угроз на основе искусственного интеллекта, квантовая криптография и постквантовые модели безопасности.

ЛИТЕРАТУРА

1. Валлерстайн И. Миросистемный анализ: введение / пер. Н. Тюкиной. М.: Издательский дом «Территория будущего», 2006. (Серия «Университетская библиотека Александра Погорельского»). 248 с.
2. Battiston F. et al. The physics of higher-order interactions in complex systems // Nature Physics. 2021. Vol. 17. №. 10. P. 1093–1098.
3. Benbya H. et al. Complexity and information systems research in the emerging digital world // Mis Quarterly. 2020. Vol. 44. №. 1. P. 1–17.
4. Da Veiga A. et al. Defining organisational information security culture — Perspectives from academia and industry // Computers & Security. 2020. Vol. 92. P. 1–13.
5. Kuzminykh I. et al. Information security risk assessment // Encyclopedia. 2021. Vol. 1. №. 3. P. 602–617.
6. Ma X. IS professionals' information security behaviors in Chinese IT organizations for information security protection // Information Processing & Management. 2022. Vol. 59. №. 1. P. 1–17.
7. Mallaboyev N.M. et al. Information security issues // Conference Zone. 2022. P. 241–245.
8. Podrecca M. et al. Information security and value creation: The performance implications of ISO/IEC 27001 // Computers in Industry. 2022. Vol. 142. P. 1–14.
9. Siegenfeld A.F., Bar-Yam Y. An introduction to complex systems science and its applications // Complexity. 2020. Vol. 2020. №. 1. P. 1–16.
10. Thomas P., Nicholas D. The Fourth Industrial Revolution: Shaping New Era // Journal of International Affairs. 2018. Vol. 72. №. 1. P. 17–22.
11. Интерактивная карта киберугроз // Лаборатория Касперского. URL: https://cybermap.kaspersky.com/ru/stats (дата обращения: 09.06.2024).
12. Digital 2024: Global Overview Report / DataReportal URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения: 09.06.2024).

Журнал «Современная наука: актуальные проблемы теории и практики»