DOI 10.37882/2223-2966.2024.7.39

ФАКТОРЫ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ СФЕРЫ[1]

THE FACTORS OF ENSURING CYBER STABILITY OF INFORMATION SPHERE OBJECTS

A. Tsaregorodtsev
M. Valeev

Summary. The digitalization policy of the Russian Federation provides for the implementation of the following directions in order to ensure strategic stability and cyber stability: changing approaches to ensuring information security, transition to technological independence, development of digital ecosystems, development of the regulatory framework in the field of information security and information law, development of the personnel base, development of mechanisms of resistance to information and psychological impact, development of methods to counter organized cyber attacks on critical information infrastructure facilities, work to ensure the security of information and communication technologies operating on the basis of cloud platforms. The article considers the main factors of ensuring cyber stability of information facilities.

Keywords: control system, cyber stability, information security, digital sovereignty, information asset.

Царегородцев Анатолий Валерьевич
Д.т.н., профессор, главный научный сотрудник, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» (Москва)
anvtsaregorodtsev@fa.ru
Валеев Михаил Владимирович
Аспирант, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» (Москва)
waleew.miha@hotmail.com

Аннотация. Политика цифровизации Российской Федерации предусматривает реализацию следующих направлений в целях обеспечения стратегической стабильности и киберустойчивости: изменение подходов к обеспечению информационной безопасности, переход к технологической независимости, развитие цифровых экосистем, развитие нормативно-правовой базы в области информационной безопасности и информационного права, развитие кадровой базы, разработка механизмов резистентности к информационно-психологическому воздействию, разработка методик противодействия организованным кибератакам на объекты критической информационной инфраструктуры, работы по обеспечению безопасности ИКТ, функционирующих на основе облачных платформ. В статье рассмотрены основные факторы обеспечения киберустойчивости объектов информационной сферы.

Ключевые слова: система управления, киберустойчивость, информационная безопасность, цифровой суверенитет, информационный актив.

Введение

Современное общество сталкивается с целым рядом вызовов, которые связаны с его цифровизацией. Стремительное развитие и распространение информационных технологий, и их проникновение во все сферы деятельности существенным образом определяют векторы развития цифрового государства. Информационные технологии выходят на новый трансграничный уровень и становятся катализатором экономических отношений, а также определяют темпы развития цифрового общества. Цифровое государство в значительной степени закладывает фундамент для всего общества в целом и для общественно-политических институтов в частности. Таким образом, складывается определенная система экономических, политических, социальных, культурных, правовых оснований, определяющих новые стандарты жизни в глобализированном цифровом обществе.

Интенсивное развитие цифровых технологий, с одной стороны, открывает новые перспективы для общественных институтов с точки зрения доступа к неограниченным потокам информации, и, с другой стороны — в условиях глобализации и повсеместной интеграции такие возможности становятся инструментом для реализации политических целей и задач, которые не всегда отвечают принятым международно-правовым нормам и служат осуществлению интересов, подрывающих стратегическую стабильность и международную безопасность.

Расширяются масштабы использования отдельными государствами средств оказания информационно-психологического воздействия, направленного на дестабилизацию экономической ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

Реализация политики открытости субъектов, возможность получения открытых данных способствует возник-

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

новению дополнительных рисков. Эпидемиологическая ситуация в мире напрямую повлияла на переход большого количества организаций на удаленную работу, увеличение экономических сделок в сети интернет, и, как следствие, создало благоприятные условия, способствующие росту киберпреступности.

Специалисты в области информационный безопасности и политики солидаризируются во мнении, что традиционное понимание государственного суверенитета сегодня претерпевает заметные изменения. Цифровизация создает дополнительные риски с точки зрения стратегической стабильности государств. Мы становимся свидетелями появления нетипичных способов военно-политического воздействия, к которым можно отнести информационные/кибервойны. Такое положение дел формулирует для государства своего рода сверхзадачу — обеспечение государственного суверенитета в его цифровом измерении — цифрового суверенитета.

1. Система управления обеспечением киберустойчивости объектов информационной сферы

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ [6] введено понятие критической информационной инфраструктуры (КИИ) и ее безопасности. Субъектами КИИ являются государственные органы и учреждения, российские юридические лица и индивидуальные предприниматели, которым на праве собственности или на ином законном основании принадлежат автоматизированные информационные системы (АИС), автоматизированные системы управления (АСУ) и информационно-телекоммуникационные сети (ИТС), функционирующие в критически важных для государства областях деятельности.

С позиций объектов информационной сферы киберустойчивость гарантирует, что восстановление системы происходит с учетом правил взаимосвязанных компонентов кибернетической инфраструктуры и объектов информационной сферы. Таким образом, киберустойчивость представляет собой набор принципов для обеспечения бесперебойной работы систем с целью обеспечения выполнения их миссии и состоит из трёх ключевых компонент: обеспечение кибербезопасности, обеспечение непрерывности деятельности, управление информационными рисками.

На рис. 1. представлен цикл обеспечения киберустойчивости, который устанавливает последовательность действий для развёртывания и обеспечения программы обеспечения киберустойчивости, включающую «целеполагание — анализ факторов риска — разработку

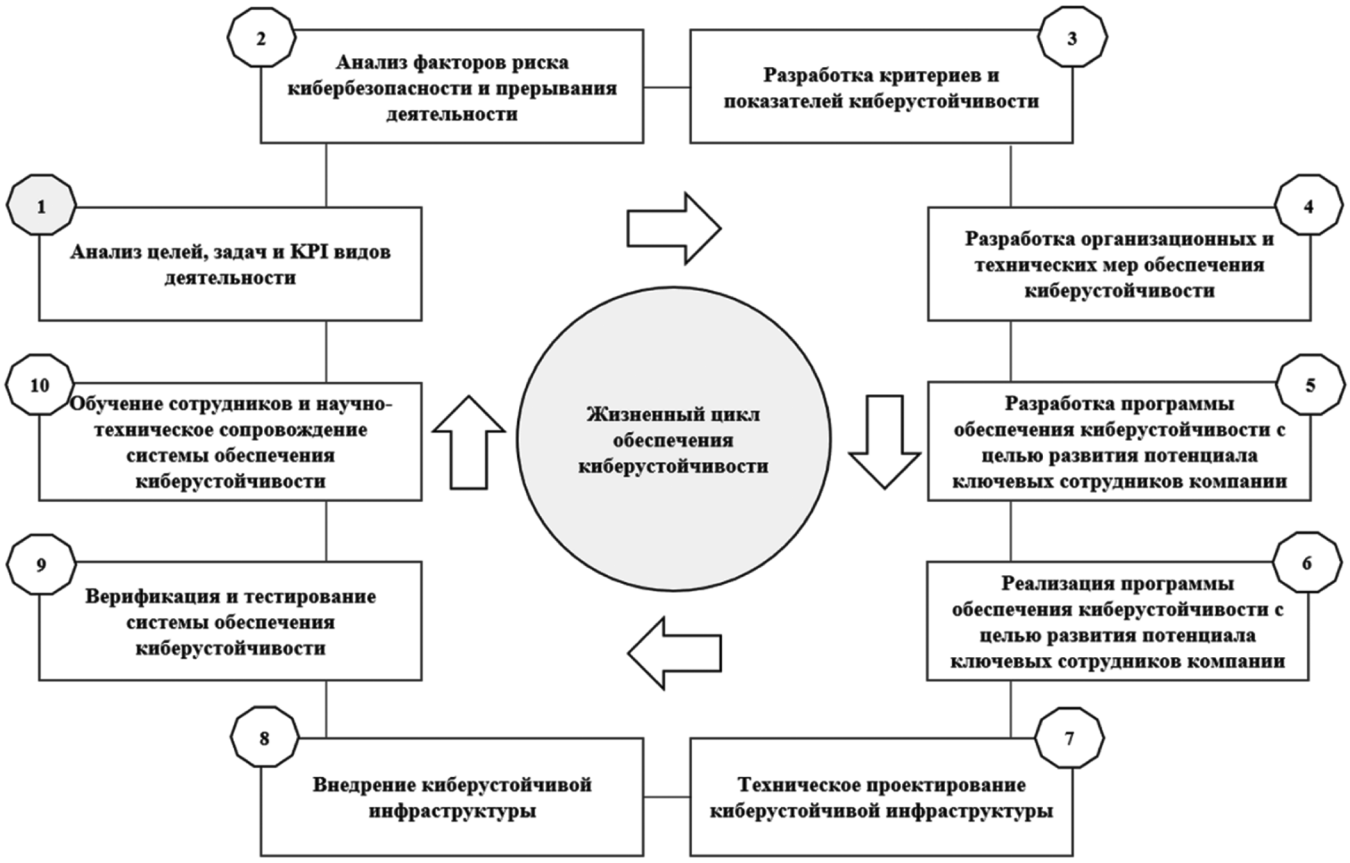

Рис. 1. Жизненный цикл обеспечения киберустойчивости

показателей киберустойчивости — разработку технических мер — программу переподготовки сотрудников — техническое проектирование — внедрение — верификацию достигнутых результатов».

При выборе разумного баланса между процедурами предотвращения инцидентов киберустойчивости, обнаружения потенциально опасных событий и реагирования на инциденты киберустойчивости организация должна учитывать, являются ли экономически эффективным акцент на предотвращение инцидентов киберустойчивости и следует ли вместо этого обеспечить быстрое обнаружение потенциально опасных событий и обеспечить быстрое реагирование на инциденты киберустойчивости. Подобные решения должны приниматься в рамках единой согласованной концепции, основанной на оценке и склонности организации к риску.

Разработка и внедрение средств управления киберустойчивостью на основе риск-ориентированного подхода должны быть достигнуты путем внедрения системы управления, движимой стратегическими целями и задачами организации. Концепция киберустойчивости организации должна использовать жизненный цикл управления устойчивым развитием, а именно, «стратегия — проектирование — трансформация — эксплуатация — непрерывное совершенствование».

Существуют альтернативные методы и подходы, которые могут быть использованы как самостоятельно, так и в сочетании с данной моделью жизненного цикла обеспечения киберустойчивости.

2. Факторы обеспечения киберустойчивости

На уровень киберустойчивости информационной системы (ИС) влияет ряд факторов, сложным и, зачастую, противоречивым образом. В данном разделе будут рассмотрены некоторые из этих факторов и то, каким образом можно ими управлять или использовать для повышения уровня устойчивости ИС.

Фактор управления сложностью ИС

Устойчивость ИС во многом зависит от сложности связей между компонентами ИС. Для повышения устойчивости в некоторых случаях следует использовать более сложную связь между двумя компонентами ИС, создавая избыточность её функций. С другой стороны, большая сложность ИС может снизить отказоустойчивость сети за счет большого количества способов, которыми один отказавший компонент ИС может вызвать отказ другого. Поэтому в большинстве случаев следует, по возможности, избегать большей сложности, если она напрямую не поддерживает функции устойчивости.

Фактор выбора топологии ИС

Выбор топологии ИС является определяющим фактором повышения киберустойчивости. Большинство ранних исследований касались фундаментальных уязвимостей различных сетей в зависимости от их топологических свойств. Особый интерес вызвала классификация свойств сетей в соответствии с распределением степени их узлов на сети с экспоненциальным распределением узлов (Wireless Network, Mesh Network) и немасштабируемые сети, в применении к теории графов. Немасштабируемые графы гораздо более устойчивы к случайным сбоям и ошибкам узлов, чем графы с экспоненциальным распределением степеней, но немасштабируемые модели сетей (Web, Power Greed) становятся все более уязвимыми для целевых атак (дискредитация высокоуровневых узлов). Доказана устойчивая зависимость между топологией и методами анализа влияния топологии на устойчивость; разработаны, основанные на топологии, методы анализа распространения кибератак и их влияния на киберустойчивость компонент ИС.

Фактор избыточности ресурсов ИС

Дополнительные компоненты ИС повышают отказоустойчивость. В частности, наращивание ёмкости узлов сети генерации и распределения электроэнергии может снизить вероятность каскадных отказов и ускорить восстановление услуг. Добавление локального хранилища и влияние на распределение узлов с различными функциями в сети также приводит к повышению устойчивости за счет наличия дополнительных ресурсов.

Отказоустойчивость может быть улучшена путем добавления нескольких функциональных возможностей к каждому узлу (обычно подразумевая потребность в дополнительных ресурсах), путем обработки большего количества источников ввода (требующих большего количества ресурсов для получения входных данных и для обработки) или путем комбинации нескольких механизмов параллельной обработки. Тем не менее, стратегия наращивания ресурсов и создание избыточности на постоянной основе являются фактором увеличения сложности и может стать причиной увеличения времени восстановления ИС в случае сбоя или отказа в обслуживании.

Резервирование следует использовать имея чёткое представление о том, что, добавляя идентичное избыточное программное обеспечение или оборудование, вредоносное ПО сможет скомпрометировать несколько избыточных ресурсов одновременно. В случае, если вводится определённое разнообразие и избыточные ресурсы существенно различаются, возрастает сложность ИС, что потенциально негативным образом воздействует на киберустойчивость.

Фактор дизайна процесса восстановления ИС

Компоненты ИС должны быть спроектированы таким образом, чтобы в случае отказа или взлома была возможность возврата в безопасный устойчивый режим функционирования. При проектировании процессов восстановления ИС, необходимо руководствоваться следующими ключевыми принципами:

— компонент ИС в неисправном режиме не должен причинять никакого вреда себе или другим компонентам ИС и её окружению;
— должна быть предусмотрена возможность гибко изменить состояние компонента ИС в процессе восстановления системы.

Отказы, сбои, связанные с физической неисправностью оборудования, воздействием человеческого фактора, зачастую необратимы или требуют существенного времени и трудозатрат на устранение последствий. В случае отказа логических компонент ИС (например, баз данных), возврат к нормальному состоянию работы ИС проходит по другим сценариям, без привлечения существенных ресурсов на восстановление работоспособности ИС. Однако следует заметить, что стандартная практика обеспечения киберустойчивости одной компоненты ИС может не обеспечивать функцию ИС «поглощать отказ» (оставаться работоспособной в условиях воздействия дестабилизирующих факторов), и, следовательно, снизить общую устойчивость ИС.

Фактор влияния каскадных сбоев функционирования ИС

Для повышения способности ИС поглощать кибервоздействия, одним из определяющих факторов является способность ИС защищаться от каскадных сбоев. Каскадный сбой — сложное событие, состоящее из цепи независимых друг от друга сбоев или отказов компонент ИС. Архитектура ИС может иметь склонность к «эффекту домино» вследствие отсутствия контроля факторов риска обеспечения киберустойчивости, что может привести к существенным негативным последствиям даже при незначительных отклонениях от нормального функционирования.

Каскадный сбой значительно ограничивает объем ресурсов ИС, который может быть задействован для эффективного поглощения и восстановления ИС и, как следствие, обеспечить её отказоустойчивое функционирование. Следовательно, зависимости или связи между узлами (компонентами) ИС должны разрабатываться таким образом, чтобы свести к минимуму вероятность легко распространяется последствий отказов или сбоев от одного узла к другому. В идеале ссылки (переходы) от одной компоненты ИС к другой должны пассивно и активно фильтровать распространение сбоев. Одной из возможных форм такой фильтрации является буферизация.

Фактор использования буферизации данных ИС

Ключевая функция ИС состоит в том, чтобы обеспечить беспрепятственный непрерывный доступ пользователей к набору определённых услуг. Буферизация данных (кэширование, локальных хранилища данных) составляет механизм киберустойчивости, который исключает необходимость постоянного доступа к компонентам ИС. Если одна из компонент глобальной ИС (источник данных) становится недоступной, должна быть предусмотрена возможность переключиться на локальный источник данных.

Фактор использования агентов обеспечения киберустойчивости ИС

Агенты обеспечения киберустойчивости — люди или инструменты, созданные на основе методов машинного обучения (искусственные агенты), которые способны применять активные, заранее определённые меры по анализу причин и сдерживанию последствий распространения кибератак на ИС и её компоненты, включая меры по «поглощению воздействий» и адаптации ИС к работе в условиях ограниченного функционирования её компонент.

Для эффективной работы агенты должны иметь планы действий в чрезвычайной и непредвиденной ситуации, операционные процессы функционирования и взаимодействия и соответствующую профессиональную подготовку (в случае, если агентом обеспечения киберустойчивости является человек). Возможно использование в качестве агентов обеспечения киберустойчивости пользователей ИС. Однако там, где это возможно, ИС должна быть обеспечена набором искусственных автономных (частично автономных) интеллектуальных агентов, которые способны выполнять действия по «поглощению воздействий» и восстановлению ИС в автономном режиме.

Фактор анализа рисков обеспечения киберустойчивости ИС

Анализ угроз обеспечения киберустойчивости ИС должен быть направлен на выявление адаптивных методов и процедур адресного воздействие злоумышленников на состояние киберустойчивости ИС с целью разработки предиктивных мер «поглощения воздействий», реактивных мер по сдерживанию распространения кибератак и скорейшему восстановлению работоспособности ИС.

Для создания риск ориентированной среды активного подавления атак злоумышленников необходимо использовать методы теоретико-игрового и сценарного анализа, которые позволяют учитывать возможности,

намерения, тактику, методы и процедуры вероятного противника, а также разрабатывать механизмы и процессы «поглощения воздействий» и восстановления таким образом, чтобы с большей вероятностью успеха противостоять действиям злоумышленника.

Фактор микросегментации компонент ИС

Благодаря микросегментации киберустойчивость становится более динамичной, масштабируемой и согласованной как внутри ИС, так и в среде обмена данными. Компоненты ИС могут быть развернуты быстрее и переконфигурированы с меньшим количеством ошибок.

Микросегментация решает проблемы блокирования горизонтального перемещения данных путем деления ИС на управляемые разделы. Это делает киберустойчивость динамичной, позволяя, в частности, выразить политики кибербезопасности в терминах концепций компонент ИС и реконфигурировать их автоматически при изменениях инфраструктуры. Кроме этого, микросегментация — экономичное решение, если использовать уже имеющиеся инфраструктурные компоненты.

Заключение

Реализация информационной функции государства оказывается сопряжённой со значительными рисками на внешнем уровне и влечет получение обществом ложной, искаженной или неполной информации. Очевидно, что подобные риски формируют неблагоприятное отношение общества к органам государственной власти, обостряют социальные, экономические и политические противоречия, что свидетельствуют о возможности их трансформации в масштабную угрозу национальной безопасности.

Структура информационного риска в контексте киберустойчивости представлена рядом факторов гетерогенного характера, которые не могут быть однозначно отнесены к той или иной сфере деятельности, в частности риски утраты целостности и подотчетности финансовых данных, потери конфиденциальности данных о клиентах, потери доступности производственных систем, утраты конфиденциальности интеллектуальной собственности, нарушения целостности систем управления могут иметь источник происхождения на любом уровне технологического пакета, включая системы средств массовой информации (социальные медиа) через механизмы влияния и методы социальной инженерии. В этой связи в статье предлагается рассматривать формирование принципов обеспечения киберустойчивости через понятие «информационной сферы» как среды обращения информации по стадиям жизненного цикла (создание — распространение — использование — хранение — уничтожение), при котором субъекты реализуют свои потребности и возможности по отношению к информации. Авторами рассмотрены ключевые факторы обеспечения киберустойчивости объектов информационной сферы.

ЛИТЕРАТУРА

1. Царегородцев, А.В. Цифровой суверенитет: актуальные проблемы и решения: монография / А.В. Царегородцев, С.В. Романовский. — Москва: ИНФРА-М, 2024. — 209 с.
2. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО Университета. 2016. № 6 (51). С. 76–91. https://vestnik.mgimo.ru/jour/article/view/640/625#
3. Ефремов А.А. Обеспечение государственного суверенитета Российской Федерации в информационном пространстве в документах стратегического планирования // Академический юридический журнал. 2017. №. 2. С. 11–20.
4. Лившиц И.И., Неклюдов А.В. Обеспечение цифрового суверенитета России // Стандарты и качество. 2017. №. 8. С. 58–61.
5. Царегородцев А.В. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем: монография / А.В. Царегородцев, С.В. Романовский, С.Д. Волков. — М.: Научно-издательский центр «ИНФРА-М», 2024. — 198 с.
6. Aydın A., Bensghir T.K. Digital Data Sovereignty: Towards a Conceptual Framework // 2019 1st International Informatics and Software Engineering Conference (UBMYK). IEEE, 2019. С. 1–6. DOI: 10.1109/UBMYK48245.2019.8965469
7. Couture S. The Diverse Meanings of Digital Sovereignty // Network Sovereignty Blog. August 5th, 2020. [Электронный ресурс]: https://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/
8. Khrustaleva O. From national sovereignty to digital sovereignty. Russia's data localization law and its implications [Электронный ресурс]: https://www.researchgate.net/publication/318452584_From_national_sovereignty_to_digital_sovereignty_Russia's_data_localization_law_and_its_implications
9. Kolontaevskaya I.F., Kamenskaya E.V., Uvarova I.A. Legal enforcement of import substitution in the field of digital sovereignty protection of the Russian Federation // International Scientific and Practical Conference on Digital Economy (ISCDE 2019). Atlantis Press. 2019.Vol. 105. P. 844–847. https://www.atlantis-press.com/proceedings/iscde-19/125924721
10. Avizienis, A.; Laprie, J.-C.; Randell, B.; Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Secur. Comput.2004, 1, 11–33. [Google Scholar] [CrossRef]
11. Hopkins, S.; Kalaimannan, E.; John, C.S. Foundations for Research in Cyber-Physical System Cyber Resilience using State Estimation. In Proceedings of the 2020 SoutheastCon, Raleigh, NC, USA, 28–29 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–2, ISBN 978-1-7281-6861-6. [Google Scholar].

Журнал «Современная наука: актуальные проблемы теории и практики»