DOI 10.37882/2223-2966.2024.7.40

СТРАТЕГИЧЕСКИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ СФЕРЫ[1]

STRATEGIC PRINCIPLES OF ENSURING CYBER STABILITY OF INFORMATION SPHERE FACILITIES

A. Tsaregorodtsev
M. Valeev

Summary. The use of digital technologies is an undeniable incentive for the development of the economy and the transformation of public and state institutions, but at the same time they are sources of new risks. Digitalization and openness of economic entities pose certain threats to the sovereignty of states, create additional opportunities for information and technological impact from the outside world on the information infrastructure of the state. The article discusses the main directions of ensuring strategic stability and cyber stability, as well as the key principles of ensuring cyber stability of information sphere objects.

Keywords: control system, cyber resilience, 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. Применение цифровых технологий являются неоспоримым стимулом развития экономики и трансформации общественных и государственных институтов, но одновременно являются источниками новых рисков. Цифровизация и открытость экономических субъектов создают определённые угрозы суверенитету государств, создают дополнительные возможности информационного и технологического воздействия со стороны внешнего мира на информационную инфраструктуру государства. В статье рассматриваются основные направления обеспечения стратегической стабильности и киберустойчивости, а также ключевые принципы обеспечения киберустойчивости объектов информационной сферы.

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

Введение

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.

1. Жизненный цикл обеспечения киберустойчивости объектов информационной сферы

С позиций объектов информационной сферы 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.

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

Концепция киберустойчивости организации должна использовать жизненный цикл управления устойчивым развитием, а именно, «стратегия — проектирование — трансформация — эксплуатация — непрерывное совершенствование»:

1. Стратегия обеспечения киберустойчивости — деятельность по обеспечению киберустойчивости основана на четко понимаемых целях и способствует достижению целей управления организацией. Стратегические инициативы затрагивают критические информационные активы: информацию, инфраструктуру, процессы, услуги, заинтересованные стороны и пр., в терминах рисков киберустойчивости.
2. Проектирование процессов киберустойчивости — создание системы управления, «люди — процессы — технологии» и средств контроля (контрольная среда), которые должны соответствовать замыслу стратегии. При проектировании выбираются соответствующие меры контроля, процедуры, проводится обучение сотрудников, в целях предотвращения нанесения вреда наиболее важным информационных активам.
3. Трансформация процессов обеспечения киберустойчивости — результаты проектирования внедряются в процессы операционной деятельности организации. В ходе трансформации проверяется правильность работы средств управления: привязка инцидента к критическим информационным активам и, однозначное понимание ущерба от реализации события инцидента.
4. Эксплуатация системы управления киберустойчивостью — управление элементами системы обеспечения киберустойчивости, а также выявление событий и инцидентов, связанных с киберустойчивостью, и управление ими. Управление элементами системы обеспечения киберустойчивости включает в себя постоянное тестирование средств контроля, с целью убедиться, что они эффективны и адекватны.
5. Непрерывное совершенствование процессов обеспечения киберустойчивости — процессы эффективны в постоянно меняющейся среде. Процесс восстановления после инцидента включает в себя анализ «причина — следствие — ущерб» с целью извлекать уроки из своего опыта, соответствующим образом внося изменения в процедуры, обучение, дизайн и стратегию.

2. Стратегические принципы обеспечения киберустойчивости

Принцип управления критичными информационными активами

Информационные активы (ИА), которые являются общими для реализации нескольких функций организации, следует относить к критичным информационным активам (КИА). Компрометация КИА увеличивает возможности злоумышленников получить контроль сразу над несколькими функциями организации. Анализ КИА должен включать:

— Определение видов операционных процессов организации, в которых задействован КИА — является общим для нескольких видов деятельности, является уникальным для определённых видов деятельности и процессов, критически важен для выполнения определённых процедур.
— Определение того, какие свойства или атрибуты КИА делают информационный актив критичным, обладающим высокой ценностью для выполнения операционных процедур организации, понимание приемлемого уровня отказа.

Приемлемый уровень отказа — обратная величина уровня общей надёжности КИА, которая варьируется в зависимости от реализуемого свойства и вида деятельности организации.

Определение компромиссов между критическими свойствами и приемлемыми уровнями отказов является центральным элементом эффективного управления рисками обеспечения киберустойчивости.

На основе стратегий, которые лучше всего подходят для данного типа КИА, можно определить наиболее подходящие принципы структурного проектирования, которые позволяют приоретизировать объекты инфраструктуры в соответствии с выбранными методами обеспечения киберустойчивости, и, тем самым, снизить уровень риска.

Принцип адаптивности архитектуры информационных систем

Принцип адаптивности архитектуры информационных систем имеет целью развитие киберустойчивости через признание необходимости гибкости использования методов как в части стратегии управления рисками, так и в части допущения о том, что непредвиденные изменения будут происходить в технической и операционной среде на протяжении всего срока службы ИС.

В контексте киберустойчивости гибкость — это свойство ИС или инфраструктуры, которую можно переконфигурировать, в которой можно перераспределять ресурсы и в которой можно повторно использовать те или иные компоненты с целью обеспечения глубины киберзащиты, способности выбирать и использовать стратегии контрмер для широкого спектра сбоев или злонамеренных действий. Принцип адаптивности согласуется с представлением о том, что инфраструктура позволяет быстро изменять форму систем и настроек для достижения тактических целей обеспечения киберустойчивости.

Таким образом, при анализе уязвимостей необходимо учитывать способность к адаптивному реагированию и закладывать необходимую избыточность для формирования гибкости к деструктивным воздействиям.

Принцип анализа скорости распространения и снижения уровня деструктивных последствий кибератаки

Большинство архитектур обеспечения киберустойчивости рассматривают внешние ИС как вредоносные. Этот принцип прослеживается в архитектурах киберфизических систем (CPS) и Интернета вещей (IoT). Однако ИС и их компоненты могут быть скомпрометированы на длительное время без обнаружения факта самого факта компрометации, в некоторых случаях факт взлома может оставаться незамеченным на протяжении длительного периода.

Этот принцип подразумевает необходимость анализа механизмов возможности снижения скорости распространения атак и величины потенциальных последствий успешного взлома ИС, в частности продолжительность и охват деструктивных последствий, вызванных действиями злоумышленника, а также скорость их распространения. Анализ скорости распространения и снижения уровня деструктивных последствий кибератаки включает определение различных типов или форм системных последствий и привязку этих системных последствий к видам деятельности организации.

Принцип предиктивного анализа появления новых угроз

Киберпреступники вкладывают время и ресурсы в сбор разведывательных данных на ИС в целях совершенствования существующих и разработки новых тактик, методов и процедур (TTPs) взлома. Через некоторое время инструменты, разработанные злоумышленниками, становятся общедоступными, что ещё больше ставит под угрозу киберустойчивость ИС. Принцип предиктивного анализа появления новых угроз подразумевает метод анализа и комплексной имитации реальных атак на ИС, в котором злоумышленник явным образом представлен в качестве интеллектуального субъекта (Red Teaming), инициатора атаки.

Принципы структурного (операционного) проектирования обеспечения киберустойчивости

Принципы структурного проектирования служат отправной точкой для внедрения методов и средств киберустойчивости. Отдельные принципы проектирования киберустойчивости сформулированы с целью формирования операционной и конструктивной избыточности, здесь может быть сформулирован более конкретный единый принцип проектирования, который демонстрирует, каким образом разнообразие архитектурных компонент и избыточность должны использоваться вместе в целях обеспечения гибкости, и как найти компромисс между обеспечением гибкости и уменьшением области атаки. Принципы структурного проектирования должны формироваться на этапе проектирования и соответствовать концептуальному принципу «cyber resilience by design».

Принцип оценки уровня доверия к информационным системам

Принцип оценки уровня доверия к ИС — ограничение количества доверенных элементов системы, наращивание усилий, по обеспечению защиты и мониторинга объектов информационной сферы.

Уменьшение размера набора доверенных объектов за счет минимизации предположений о том, чему можно доверять, снижает площадь поверхности атак и затраты на обеспечение кибербезопасности. Когда ИС уже разработана, внесение изменений в архитектуру ИС приведут к увеличению затрат.

Другой формой применения данного принципа проектирования заключается в ограничении наследования полномочий, это означает, что привилегии или права доступа, связанные с одним классом компонентов ИС, не распространяются на классы или экземпляры ИС «по умолчанию».

Сведение к минимуму количества элементов с требованиями постоянной надежности снижает количество контролей, необходимых для определения постоянной надежности, и, тем самым, снижается стоимость сопровождения компонент ИС.

Принцип контроля прозрачности использования информационных систем

Принцип контроля прозрачности использования ИС — контроль компонент ИС, которые могут быть обнаружены и исследованы злоумышленником в процессе сканирования инфраструктуры организации.

Контроль прозрачности позволяет противодействовать попыткам разведки извне или внутри системы. Прозрачность использования информационных ресурсов организации, возможно контролировать, например, намеренно добавляя «мусор» к сетевому трафику. Прозрачность процедур обмена информацией, процесса разработки или проектирования ИС может быть ограничена за счет обеспечения сокрытия проведения операций (OPSEC), а также сегрегации процессов проектирования и эксплуатации ИС.

Прозрачность процедур обмена информацией должна контролироваться на уровне физического, логического и/или гибридного методов обеспечения кибербезопасности.

Принцип контроля наличия субъективного вмешательства в функционирование ИС

Принцип контроля наличия субъективного вмешательства в функционирование ИС — ограничение причин и последствий реализации событий рисков компрометирующих действий в отношении ИС, связанных с нарушением функций управления киберустойчивостью по причине отсутствия согласованных действий в части снижения площади распространения кибератак.

Анализ операционных полномочий субъекта должен выявлять характер поведения, который приемлем только в отношении его должностных обязанностей. Выявление любых исключений из правил предотвращает нежелательные последствия такого поведения. Поведение субъекта может стать компромиссом между утверждёнными правилами и гибкостью, обоснованной необходимостью выполнения операционных процедур «в срок». Должна быть обеспечена возможность прерывания деятельности субъекта на основе данных мониторинга, в случае, когда есть объективные основания для подозрений в ошибочных действиях.

Принцип эшелонированной защиты функционирования ИС

Принцип эшелонированной защиты функционирования информационной системы — сочетание принципа зонирования защиты и разделения полномочий. Эшелонированная защита — интеграция людей, процессов и технологий для создания системы защиты организации на различных уровнях её функционирования. Эшелонированная защита — архитектура безопасности, построенная путем применения набора согласованных друг с другом структурированных методов реализации контрмер в целях предотвращения и сдерживания атак злоумышленников. Эшелонированная защита ограничивает продвижение злоумышленника по вертикали многоуровневой архитектуры ИС, защита на одном уровне предотвращает распространение взлома на другом уровне.

Принцип планирования и управления разнообразием

Принцип планирования и управления разнообразием заключается в создании неоднородностей характеристик архитектуры, программного обеспечения ИС, возможностей пользователей. Разнообразие — это свойство, которое способно повысить устойчивость ИС в отношении внешних воздействий. Планирование и управление разнообразием это подход, при котором компоненты ИС и программного обеспечения, не являются копиями, а независимо разработаны для удовлетворения требований системы. В этой парадигме необходимо получать свидетельства того, что отказы компонент ИС происходят независимо, поскольку рост числа совпадающих отказов свидетельствует о несостоятельности реализации принципа планирования и управления разнообразием. Разнообразие (обычно в сочетании с избыточностью) — это хорошо зарекомендовавший себя метод повышения устойчивости системы.

Можно выделить несколько подходов к достижению разнообразия — архитектурное разнообразие, разнообразие проектов, синтетическое (или автоматизированное) разнообразие, информационное разнообразие, разнообразие методов управления и пр.

Реализация принципа планирования и управления разнообразием потенциально может увеличить площадь поверхности атаки.

Принцип обеспечения избыточности

Принцип обеспечения избыточности — устоявшийся принцип проектирования устойчивой архитектуры ИС. Реализация данного принципа повышает доступность критически важных функций, но требует защиты избыточных ресурсов.

Поскольку вредоносные программы могут распространяться по однородным компонентам ИС, избыточность для обеспечения киберустойчивости необходимо применять в сочетании с разнообразием, избыточность необходимо рассматривать для всех уровней многоуровневой архитектуры ИС. Вместе с тем, избыточность, в сочетании с распределённой архитектурой, может повысить сложность ИС и создать проблемы масштабируемости.

Принцип обеспечения универсальности расположения ресурсов

Принцип обеспечения универсальности расположения ресурсов — это формирование архитектуры компонент ИС, для которых не требуется фиксированное пространственное местоположение. Для создания архитектуры компонент ИС с изменяющимся местоположением могут использоваться различные подходы — виртуализация, репликация, распределение (функциональности или хранимых данных), физическая мобильность и функциональное перемещение. Репликация может осуществляться по географическим точкам, аппаратным платформам или виртуальным машинам.

Принцип обеспечения универсальности расположения ресурсов подразумевает использование динамиче-

ского позиционирования, обеспечивает избыточность и гибкость в управлении данными.

Принцип мониторинга состояния информационных систем

Принцип мониторинга состояния информационных систем заключается в обеспечении ситуационной осведомленности, выявлении потенциально подозрительного поведения компонент ИС и прогнозировании необходимости внесения изменений в целях повышения уровня безопасности и надёжности компонент ИС.

В силу особенностей проектирования архитектур системные компоненты ИС могут не иметь возможности обменивается информацией о состоянии друг друга, что создаёт определённые трудности соблюдения политик безопасности и мониторинга соответствия политикам. Однако практически каждый компонент современных ИС предоставляет данные по его доступности для взаимодействия. Корреляция данных мониторинга, включая данные о состоянии компонент ИС на всех уровнях архитектуры ИС может выявить потенциальные проблемы на раннем этапе, что позволит предотвратить инцидент.

Принцип обеспечения ситуационной осведомленности

Ситуационная осведомленность — это восприятие событий в отношении времени и пространства, понимание их значения и понимание их статуса в ближайшем будущем.

Целью ситуационной осведомленности являются активное обнаружение и анализ информации, относящейся к немедленной операционной стабильности и безопасности, и координация такой информации на предприятии, чтобы гарантировать, что все организационные подразделения работают в рамках общей операционной картины. Ситуационная осведомленность позволяет организации понять операционную среду критичных сервисов и среду влияния на их работу.

Принцип адаптивного управления ресурсами с учётом рисков

Принцип адаптивного управления ресурсами с учётом рисков включают изменение частоты запланированных изменений, повышение уровня кибербезопасности, перераспределение ресурсов, изоляция подозрительных компонентов ИС. Принцип адаптивного управления ресурсами с учётом рисков может применяться в сочетании с динамическим изменением привилегий пользователей.

Принцип адаптивного управления ресурсами с учётом рисков должен основываться на ситуационной осведомленности — управленческие решения должны основываться на признаках изменений в характеристиках действий злоумышленника, изменений в характеристиках компонентов ИС, изменений в операционных процедурах пользователей, выявлении новых угроз киберустойчивости.

Принцип постоянства обновлений

Принцип постоянства обновлений заключается в перманентном обновлении элементов системы, что сводит к минимуму продолжительность нахождения злоумышленников в ИС, позволяет удалить вредоносное программное обеспечение и восстановить поврежденные данные. Принцип постоянства обновлений — это стратегия уменьшения площади поверхностей атак во временном измерении.

Принцип обеспечения надежности

Принцип обеспечения надежности заключается в периодическом контроле целостности и корректности данных, программного обеспечения (ПО), поведения отдельных пользователей, работы системных компонентов и служб, что способствует снижению вероятности взлома ИС.

Принцип снижения площади поверхности атаки

Поверхность атаки — это совокупность компонент ИС, которые доступны потенциальному нарушителю. Принцип снижения площади поверхности атаки — это уменьшение объема выполняемого кода, уменьшение количества точек входа в ИС, доступных для ненадежных пользователей, исключение услуг, запрашиваемых относительно небольшим числом пользователей.

Заключение

Информационные риски в контексте киберустойчивости разнообразны и затрагивают разные сферы деятельности. Угрозы, такие как утечка финансовых данных, потеря конфиденциальности информации о клиентах, сбои в информационных системах, могут возникать на любом уровне информационной инфраструктуры. В статье предложено рассматривать киберустойчивость через призму «информационной сферы» — среды, где информация проходит жизненный цикл от создания до уничтожения. Авторы анализируют стратегические принципы обеспечения киберустойчивости объектов в этой сфере.

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. Рубанов В. Цифровой суверенитет хранения и обработки данных // Деловой журнал Neftegaz.RU. 2019. № 4 (88). С. 76–78. https://magazine.neftegaz.ru/articles/tsifrovizatsiya/504404-tsifrovoy-suverenitet-khraneniya-i-obrabotki-dannykh/
3. Соловых Н.Н. Цифровизация: риски и угрозы обеспечения цифрового суверенитета России // Потенциал роста современной экономики: возможности, риски, стратегии. 2018. С. 1302–1310.
4. 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.
5. Bodeau, D.; Graubart, R. Cyber Resilience Metrics: Key Observations 2016. Available online: https://www.mitre.org/sites/default/files/publications/pr-16-0779-cyber-resilience-metrics-key-observations.pdf (accessed on 15 November 2023).
6. Hukerikar, S.; Engelmann, C. Resilience Design Patterns-A Structured Approach to Resilience at Extreme Scale (version 1.0). 2016. Available online: https://arxiv.org/abs/1708.07422 (accessed on 15 November 2023).
7. Carias, J.F.; Labaka, L.; Sarriegi, J.M.; Hernantes, J. An Approach to the Modeling of Cyber Resilience Management. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6, ISBN 978-1-5386-6451-3. [Google Scholar]

Журнал «Современная наука: актуальные проблемы теории и практики»