К вопросу о цифровой зависимости критической инфраструктуры: что произойдёт при масштабном сбое информационных систем?

Сегодня работа банков, энергетики, транспорта, медицины, промышленности и государственных учреждений всё больше зависит от информационных систем. Управление технологическими процессами, расчёты, логистика и диспетчеризация осуществляются в цифровой среде, поэтому отказ информационной системы способен нарушить работу целого объекта или отрасли. Особенно заметно это на объектах критической информационной инфраструктуры (КИИ), для которых российское законодательство предусматривает специальную систему безопасности. Масштаб зависимости демонстрирует финансовый сектор: по данным Банка России, в 2025 году граждане получали онлайн почти 80% финансовых услуг, а компании – порядка около 90%.

Отказ критической системы не обязательно является результатом целенаправленной атаки: причиной может стать программная ошибка, отказ оборудования, нарушение электроснабжения или ошибка сотрудника. Один из наиболее опасных сценариев – это программы-вымогатели. Которые блокируют доступ к данным посредством шифрования. Для обычной корпоративной системы это приводит к значительным потерям, но для критической инфраструктуры последствия серьёзнее: если система управляет технологическим процессом, потеря доступа может остановить производство.

Отдельное значение приобретает резервное копирование. Наличие копии ещё не гарантирует восстановление: она может оказаться повреждённой, устаревшей или также зашифрованной в ходе атаки.

Доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.э.н., доцент Рожкова Р.С. подчёркивает необходимость регулярно проверять возможность восстановления, а для защиты от программ-вымогателей изолировать резервные данные. Важно и резервирование серверов, каналов связи и компонентов управления, причём резервные системы должны регулярно тестироваться. Не менее важен мониторинг: признаками атаки или сбоя могут быть резкий рост запросов, необычная активность администратора, массовое изменение файлов или одновременный отказ нескольких компонентов.

Доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.в.н., доцент Зайцев О.Н. делает акцент та том, что полностью исключить отказ невозможно, поэтому отдельным направлением становится обеспечение непрерывности деятельности. Организация должна заранее определить критически важные функции, последовательность их восстановления и допустимые интервалы недоступности, используя показатели RTO (допустимое время простоя системы после сбоя или отказа) и RPO (показатель, который характеризует объем данных, который организация может потерять при сбое и временной интервал в течении которого это может произойти).

Ситуация особенно осложняется, когда одновременно недоступны несколько взаимосвязанных систем. Поэтому архитектура критической инфраструктуры должна рассматриваться как единая система зависимостей, так называемая «органическая» система.

В российской практике в конце 2025 года можно отметить новый порядок в силовых министерствах и ведомствах, который регулирует информирование о компьютерных атаках и взаимодействие субъектов КИИ с государственной системой обнаружения и предупреждения атак. Важна не только защита, но и скорость передачи информации об инциденте: при масштабных атаках время между обнаружением и началом реагирования определяет размер последствий.

Таким образом, цифровизация критической инфраструктуры одновременно повышает её эффективность и увеличивает масштаб последствий отказа. Главное изменение подхода заключается в переходе от модели «не допустить инцидент» к модели «не допустить критических последствий инцидента».

Для этого необходим комплекс мер: резервирование, резервное копирование и проверка восстановления, сегментация сетей, постоянный мониторинг, управление доступом, планирование непрерывности деятельности и регулярные учения. Именно системный подход позволяет превратить цифровую зависимость из потенциальной уязвимости в управляемый риск.

В частности, устанавливаются жёсткие регламенты по срокам уведомления: о значимых инцидентах субъекты КИИ обязаны сообщать в течение нескольких часов с момента обнаружения, а о компьютерных атаках незамедлительно. За нарушение этих требований предусмотрены

меры административной и уголовной ответственности, что делает информационную безопасность не просто технической, но и юридически значимой зоной ответственности руководства организаций. Кроме того, новый порядок предполагает создание ведомственных и корпоративных центров мониторинга, обеспечивая единое информационное поле для реагирования.

Особое внимание уделяется категорированию объектов КИИ: чем выше значимость объекта, тем строже требования к резервированию, сегментации и периодичности проверок, что позволяет распределять ресурсы защиты пропорционально возможному ущербу. Наконец, регулярные учения и тренировки с имитацией масштабных атак становятся обязательным элементом деятельности субъектов КИИ, поскольку именно практика выявляет слабые места в организационных и технических мерах защиты.

Рожков Р.С.,
кандидат экономических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ

Зайцев О.Н,
кандидат военных наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ