

УДК 004.056

Э.П. РЫБАЛКО¹

Научный руководитель – доцент Г.П. ГАВДАН²

¹*АО «Межотраслевой центр мониторинга», Москва*

²*Национальный исследовательский ядерный университет «МИФИ», Москва*

УСТОЙЧИВОСТЬ ФУНКЦИОНИРОВАНИЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В настоящее время в Российской Федерации уделяется достаточно большое внимание и качественной работе государственных информационных систем (ГИС) и организации их устойчивого функционирования, которая к тому же не утратила свою актуальность. В свою очередь, оценка эффективности применяемых мер по обеспечению безопасности ГИС требует проведения оценки (их) устойчивого функционирования, которая определяется устойчивостью критических процессов этих ГИС. Объектом исследования являются ГИС. Предмет исследования есть устойчивость функционирования данных ГИС в условиях угроз информационной безопасности. Проведённый анализ научных публикаций по теме исследования показал, что в данном направлении в настоящее время имеется мало публикаций. По результатам работы установлено, что в данной области существуют нерешенные проблемы.

Введение

Открытость государственных информационных систем (ГИС) имеет большое значение для общества и правительства и обеспечивает прозрачность деятельности государственных органов [1]. Это означает, что граждане могут легко получать доступ к информации о действиях и решениях правительства, что обеспечивает им получить представление и сформулировать мнение о состоянии российского общества [1]. Так, в соответствии с базовым Федеральным Законом от 27 июля 2006 г. № 149-ФЗ в области информатизации, информационных технологий и защите информации. Данные, содержащиеся в ГИС, а также иные имеющиеся в распоряжении (государственных органов) сведения и документы являются национальными информационными ресурсами [2].

Устойчивость функционирования ГИС

Объективно существующая вероятность нарушения устойчивого функционирования ГИС, обусловленная возможностью возникновения нежелательных антропогенных, техногенных или стихийных воздействий на их информационные элементы, заставляет рассматривать устойчивость ГИС в условиях влияния на них угроз информационной безопасности [2].

Для оценки эффективности применяемых мер по обеспечению безопасности ГИС необходимо проведение оценки устойчивости их функционирования. В настоящее время общепринятый подход к проведению такой оценки отсутствует и его определение остаётся актуальной задачей [2]. Проблема устойчивости критической информационной инфраструктуры представлена [3] в работе авторской группы. В качестве угроз нарушителя – компьютерных атак могут рассматриваются целенаправленные программно-аппаратные воздействия, приводящие к нарушению (блокированию, искажению) информационно-вычислительных процессов функционирования ГИС [4].

Заключение

Сформулируем следующее определение устойчивости функционирования ГИС – это способность ГИС выполнять свои основные функции:

- в неблагоприятных условиях (т.е. при попытках реализации УИБ);
- в условиях непосредственной реализации на ГИС отдельных из УИБ;
- при отказе части компонентов объекта (т.е. в случае, когда отдельные угрозы ИБ уже реализуются);
- восстанавливать штатное функционирование в допустимые сроки.

Способность ГИС выполнять свои основные функции в любых условиях можно рассматривать как защищенность ГИС, в условиях реализации в отношении её угроз ИБ – живучесть ГИС в случае целенаправленных угроз либо стойкость ГИС (в случае если эти угрозы случайные – обусловлены программными ошибками, техническими сбоями или ошибками персонала).

Список литературы

1. Шматова У. В. Вопросы обеспечения открытости государственных информационных систем в России / У.В. Шматова // Актуальные проблемы и перспективы развития потребительского рынка: Материалы XII Международной научно-практической конференции студентов и учащихся, Пермь, 04–12 декабря 2023 года. Том 1. – Пермь: Пермский институт (филиал) ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», 2023. – С. 396–400. – EDN VOLPBC (дата обращения: 01.09.2024).
2. Пенерджи Рустем В., Гавдан Григорий П. Информационная безопасность государственных информационных систем. Безопасность информационных технологий, [S.l.], т. 27, № 3, с. 26–42, 2020. ISSN 2074-7136. DOI: <http://dx.doi.org/10.26583/bit.2020.3.03>. – EDN PEHWST.
3. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования. Радиопромышленность. 2018, № 4, с. 59–67. URL: <https://elibrary.ru/item.asp?id=36511234> – EDN YPERPV (дата обращения: 01.09.2024).
4. Антонов С.Г., Анциферов И.И., Климов С.М. Методика инструментально-расчетной оценки устойчивости объектов критической информационной инфраструктуры при информационно-технических воздействиях. Надежность. 2020, 20(4):35–41. DOI: <https://doi.org/10.21683/1729-2646-2020-20-4-35-41> (дата обращения: 10.09.2024).