Григорий П. Гавдан[1], Виталий Г. Иваненко[2], Элина П. Рыбалко[3], Денис П. Рыбалко[4]
[1,2,4]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[3]Российский университет дружбы народов (РУДН),
ул. Миклухо-Маклая, 6, Москва, 117198, Россия
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[3]e-mail: rybalko.elina@mail.ru, https://orcid.org/0000-0001-6292-2535
[4]e-mail: vicarium@yandex.ru, https://orcid.org/0000-0003-3627-695X

УСТОЙЧИВОСТЬ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2022.4.05

Аннотация. Целью статьи является рассмотрение устойчивости функционирования объектов критической информационной инфраструктуры (КИИ). Государства должны обеспечить должную защиту своих значимых (при их наличии) объектов КИИ. Для субъектов КИИ России, критических сфер экономики, которые имеют в своем составе сотни и даже тысячи объектов КИИ могут возникнуть значимые последствия и как следствие, это может привести к нарушению технологических процессов на значимом объекте КИИ. Для обеспечения устойчивой работы объекта отнесённого к КИИ требуется выполнить оценку его (устойчивого) функционирования. Оценка эффективности применяемых мер по обеспечению безопасности значимых объектов (ЗО) КИИ требует проведения оценки устойчивости их функционирования, которая по своей сути определяется устойчивостью их критических процессов. Однако в настоящее время общепринятый подход к проведению такой оценки отсутствует и его определение является актуальной задачей. Объектом исследования являются объекты КИИ. Предмет исследования – устойчивость функционирования данных объектов (КИИ) в условиях угроз информационной безопасности (ИБ). В статье исследуется устойчивость объектов КИИ. Проводится анализ нормативных правовых актов (НПА) и научных публикаций по теме исследования. Анализ НПА КИИ показал, что в данной области существуют проблемы, поэтому подход к обеспечению безопасности и устойчивости функционирования, как КИИ, так и отдельных ее объектов должен строиться на определенных принципах. В статье рассмотрены основные определения и проблемы, приведены источники, подтверждающие важность проведённого исследования. Результаты исследования могут быть использованы при рассмотрении подходов к оценке функционирования объектов КИИ и усовершенствовании оценки её устойчивости.

Ключевые слова: значимый объект, критическая информационная инфраструктура, критический процесс, угрозы информационной безопасности, оценка устойчивости функционирования объекта, устойчивость критического процесса.

Для цитирования: ГАВДАН, Григорий П. и др. УСТОЙЧИВОСТЬ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], т. 29, № 4, с. 53–66, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1453. DOI: http://dx.doi.org/10.26583/bit.2022.4.05.

Grigory P. Gavdan[1], Vitaliy G. Ivanenko[2], Elina P. Rybalko[3], Denis P. Rybalko[4]
[1,2,4]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[3]RUDN University,
Miklukho-Maklaya str., 6, Moscow, 117198, Russia
[1]e-mail: gpgavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[3]e-mail: rybalko.elina@mail.ru, https://orcid.org/0000-0001-6292-2535
[4]e-mail: vicarium@yandex.ru, https://orcid.org/0000-0003-3627-695X

Sustainability of the functioning of critical information infrastructure facilities

DOI: http://dx.doi.org/10.26583/bit.2022.4.05

Abstract. The purpose of the paper is to consider the sustainability of the functioning of critical information infrastructure (CII) facilities. The states should ensure proper protection of their significant (if any) CII facilities. Significant negative consequences may arise for the subjects of the CII of Russia, critical sectors of the economy that have hundreds or even thousands of CII objects in their composition. As a result, this may lead to disruption of technological processes at a significant CII object. In order to ensure the stable operation of an object classified as a CII, it is required to perform an assessment of its (sustainable) functioning. Evaluation of the effectiveness of the applied measures to ensure the safety of significant objects (ZO) of the CII requires an assessment of the stability of their functioning, which is inherently determined by the stability of their critical processes. However, currently there is no generally accepted approach to conducting such an assessment and its definition is an urgent task. The objects of the research are the CII objects. The subject of the study is the sustainability of the functioning of data (CII) objects in the conditions of threats to information security (IS). The stability of CII objects are examined. The analysis of regulatory legal acts (NPA) and scientific publications on the research topic is carried out. This analysis of the NPA of the CII showed that there are problems in this area, therefore, the approach to ensuring the safety and stability of the functioning of both the CII and its individual objects should be based on certain principles. The main definitions and problems are discussed, the arguments confirming the importance of the study are provided. The results of the study can be used when considering approaches to assessing the functioning of CII facilities and improving the assessment of its stability.

Keywords: significant object, critical information infrastructure, critical process, threats to information securlty, assessment of the stability of the functioning of the object, the stability of the critical process.

For citation: GAVDAN, Grigory P. et al. Sustainability of the functioning of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 29, no. 4, p. 53–66, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1453. DOI: http://dx.doi.org/10.26583/bit.2022.4.05.

Введение

Необходимость обеспечения устойчивости функционирования любой критической информационной инфраструктуры и отдельных её объектов вытекает из директивно заданных целей обеспечения безопасности, указанных в Федеральной законе от 26.07.2017 № 187-ФЗ и приказе ФСТЭК России от 25 декабря 2017 г. № 239. Не секрет, что от устойчивости функционирования любых объектов КИИ зависит существование государства [1] и безопасность его граждан [2].

В соответствии с ФЗ-187 критическая информационная инфраструктура (КИИ) – это объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов, при этом сети электросвязи, используемые для обеспечения функционирования объектов к КИИ *не относятся*.

Объектами КИИ являются автоматизированные системы управления (АСУ), информационно-телекоммуникационные сети (ИТКС) и информационные системы (ИС) субъектов КИИ.

Субъектами КИИ являются государственные органы, государственные учреждения, российские юридические лица и/или индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в 13 сферах/областях КИИ (сферы КИИ), а также российские юридические лица и/или индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Объективно существующая вероятность нарушения функционирования объектов КИИ, обусловленная возможностью возникновения нежелательных антропогенных, техногенных или стихийных воздействий на их информационные элементы, заставляет рассматривать устойчивость объектов КИИ в условиях влияния на них угроз информационной безопасности (ИБ). Для оценки эффективности [3] применяемых мер по обеспечению безопасности значимых объектов (ЗО) КИИ необходимо проведение оценки устойчивости их функционирования [4], которая по своей сути определяется устойчивостью их

критических процессов. Однако в настоящее время общепринятый подход к проведению такой оценки отсутствует [1] и его определение является актуальной задачей [5].

Рассмотрим определение «устойчивость функционирования объектов КИИ» в условиях угроз ИБ и способ оценки данного показателя.

1. Определение устойчивости

Сформулировать определение можно с помощью близких понятий в действующих нормативных правовых актах РФ (НПА) в области обеспечения ИБ, а также с учетом существующих определений в иностранных документах.

В соответствии с ФЗ-187 объекты КИИ делятся на ***три типа***:

– информационные системы (ИС);
– информационно-телекоммуникационные сети (ИТКС);
– автоматизированные системы управления (АСУ).

Применительно к ИС общего пользования в соответствии с Приказом Минкомсвязи РФ от 25.08.2009 № 104 устойчивостью функционирования является способность системы сохранять свою целостность при отказе части компонентов системы, в условиях внутренних и внешних деструктивных информационных воздействий, а также способность возвращаться в исходное состояние.

Для АСУ военного назначения существует следующее определение устойчивости – комплексное свойство АСУ военного назначения, характеризуемое помехоустойчивостью, живучестью и надежностью АСУ.

Для ИТКС определение устойчивости функционирования в НПА РФ отсутствует, близким по значению понятием в данном случае будет определение устойчивости функционирования сети электросвязи – способность выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов.

В соответствии с публикацией Национального института стандартов и технологий США NIST SP 800-393[1] устойчивостью ИС (*Information System Resilience*) считается способность ИС[2] продолжать функционировать в неблагоприятных условиях или под давлением, даже если она находится в разрушенном или ослабленном состоянии, при сохранении основных эксплуатационных возможностей и восстанавливаться до эффективного рабочего состояния в сроки, соответствующие целевым потребностям.

Обобщив вышеизложенное, можно сформулировать следующее определение устойчивости функционирования объекта КИИ – это способность объекта КИИ выполнять свои основные функции:

– в неблагоприятных условиях (т.е. при попытках реализации угроз ИБ);

– в условиях непосредственной реализации в отношении него отдельных угроз ИБ;

– при отказе части компонентов объекта (т.е. в случае, когда отдельные угрозы ИБ уже реализуются);

– при восстанавливать штатное функционирование в допустимые сроки (т.е. после реализации угроз ИБ).

Способность объекта КИИ выполнять свои основные функции в неблагоприятных условиях можно рассматривать как защищенность объекта, в условиях реализации в отношении него угроз ИБ – живучесть объекта (в случае если угрозы целенаправленные)

[1]NIST Special Publication 800-30 Revision 1 Специальная публикация Национального института Стандартов и Технологий США. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (дата обращения: 11.10.2022).

[2]Nationale Strategiezum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) Национальная стратегия защиты критических инфраструктур Германии.
URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html (дата обращения: 11.10.2022).

либо стойкость объекта (в случае если угрозы случайные – обусловлены программными ошибками, техническими сбоями или ошибочными действиями персонала).

В рамках обеспечения информационной безопасности КИИ все объекты КИИ подвергаются категорированию в соответствии с Постановление 127, в процессе которого выделяют только те функции объекта КИИ, которые непосредственно влияют на критические процессы (КП):

– обработка информации, необходимой для обеспечения КП;
– осуществление управления, контроля или мониторинга КП.

Ввиду того, что в данной работе рассматриваются ЗО КИИ, при оценке устойчивости будут соответственно учитываться только те КП, нарушение которых может привести к возникновению значимого ущерба (значимые процессы – ЗП), под которым понимается ущерб, масштаб которого соответствует определенным в Постановлении 127 значениям показателей критериев значимости.

Функции ЗО КИИ, непосредственно влияющие на ЗП, и будут в нашем случае основными функциями объекта. В этой связи, устойчивость функционирования значимого объекта КИИ в условиях угроз ИБ можно определить, как способность объекта выполнять функции по управлению, контролю или мониторингу ЗП, и/или обработке информации, необходимой для обеспечения ЗП, при попытках реализации в отношении него угроз ИБ («защищённость»), в условиях реализации в отношении него угроз ИБ («живучесть» – в случае реализации целенаправленных угроз, «стойкость» – случайных угроз ИБ), а также способность восстанавливать («восстанавливаемость») свое штатное функционирование в допустимые сроки и адаптироваться к угрозам ИБ («адаптируемость»), рис. 1.

Рис. 1. Устойчивость функционирования ЗО КИИ
Fig. 1. Stability of the functioning of the OS CII

Поэтому важным является то, что при оценке устойчивости основополагающими будут свойства самого объекта. Здесь необходимо также отметить, что устойчивость функционирования ЗО КИИ в условиях угроз ИБ равна устойчивости выполнения ЗП только в том случае, если нарушение ЗП возможно лишь при нарушении функционирования ЗО КИИ. В противном случае устойчивость ЗП необходимо рассматривать в совокупности с устойчивостью физического объекта.

Вывод: по результатам анализа отечественных и иностранных НПА и научных публикаций сформулировано определение устойчивости функционирования ЗО КИИ в условиях угроз ИБ.

2. Устойчивость ЗО КИИ на примере АСУ ТП

Процесс обеспечения устойчивости функционирования объекта можно рассмотреть на примере АСУ ТП критически важных объектов. Предположим, что значимый процесс АСУ ТП состоит из функционирования информационных и неинформационных элементов, тогда процесс обеспечения устойчивости функционирования объекта можно представить в следующем виде, рис. 2.

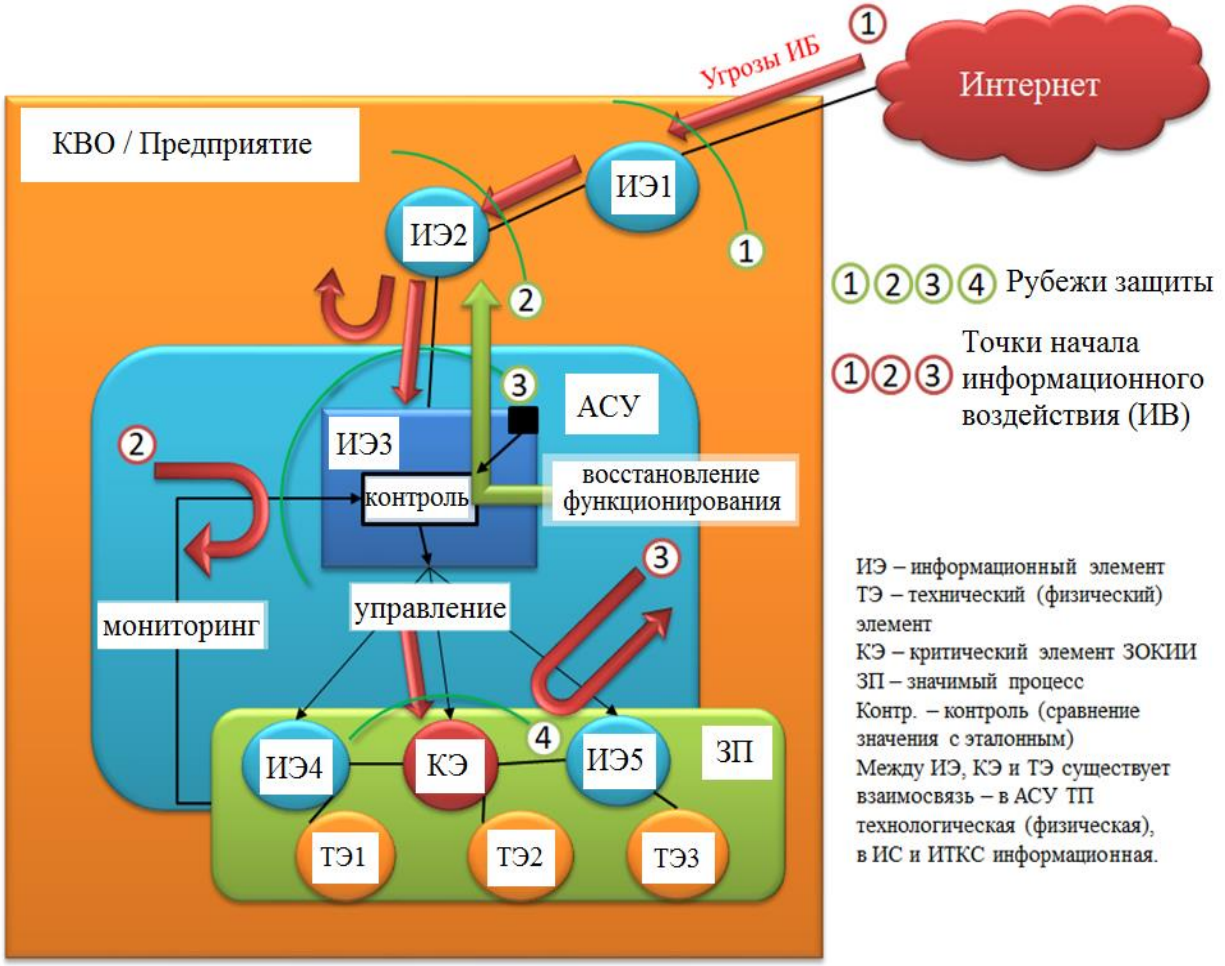

Рис. 2. Устойчивость АСУ ТП
Fig. 2. Stability of automated process control systems

Критические элементы ЗО КИИ (КЭ) – элементы объекта, которые непосредственно влияют на возникновение критического состояния ЗП, и на которые возможно осуществление информационного воздействия (посредством реализации угроз ИБ). На рис. 2 АСУ ТП изображена в виде обычного графа, что и будет использовано в дальнейшем для проведения оценки устойчивости объектов КИИ.

Кроме этого надо также отметить, что устойчивость функционирования ЗО КИИ (в рамках преднамеренных угроз ИБ) будет зависеть от расположения точки начала информационного воздействия и от количества рубежей до КЭ, которые необходимо преодолеть злоумышленнику для воздействия на ЗП. Процесс изменения устойчивости для данной АСУ ТП можно представить в виде графика (рис. 3).

Использование графического представления позволяет более четко визуализировать этапы обеспечения устойчивости. Применительно к рассматриваемому случаю на графике видно, что после восстановления своего функционирования система адаптировалась и больше не уязвима для угрозы № 4, угрозы № 2 и № 3 не устранены.

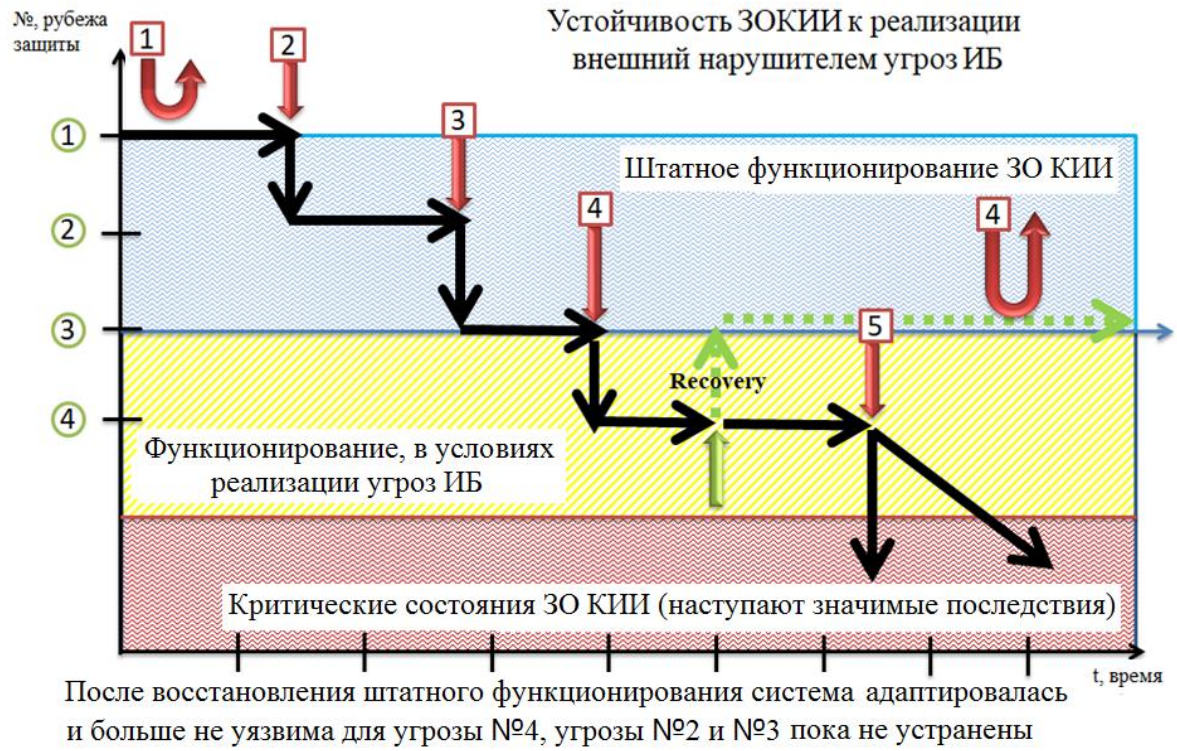

Рис. 3. Изменение устойчивости ЗО КИИ
Fig. 3. Change in stability SO CII

Вывод: приведенные принципы построения модели объекта КИИ и визуализации процесса изменения его устойчивости можно использовать в дальнейшем при проведении оценки устойчивости объектов КИИ.

3. Оценка устойчивости ЗО КИИ

Для определения принципов оценки устойчивости ЗО КИИ необходимо сначала описать существующие проблемы в области обеспечении безопасности объектов КИИ.

Ввиду того, что большинство ЗО КИИ представляют собой достаточно сложные и динамичные системы [6], субъекты КИИ могут столкнуться со следующими проблемами:

1) Формальное выполнение требований нормативных документов в отдельных случаях не обеспечивает фактической защиты, требуется проведение объективной оценки угроз ИБ [7].

2) Пропуск отдельных угроз ИБ и/или уязвимостей ввиду присутствия следующих факторов [8]:

– трудоемкость процесса выявления уязвимостей из-за большого количества и разнообразия элементов системы. Кроме того, по результатам анализа уязвимостей в обязательном порядке должно быть подтверждено отсутствие только тех уязвимостей, которые содержатся в Банке данных угроз безопасности информации ФСТЭК России, которому необходимо определенное время для обновления базы данных при появлении информации о новых уязвимостях. В рамках анализа уязвимостей предусмотрено также

проведение тестирования на проникновение, результаты которого будут зависеть от профессионализма проверяющего, и могут быть необъективными:

– при проведении оценки угроз ИБ требуется анализ большого объема данных, что обуславливает сложность данной работы, особенно до начала эксплуатации системы [9];

– экспертные оценки при формировании модели угроз ИБ не всегда бывают объективными [10].

3) Возможность появления новых (ранее неизвестных) угроз ИБ и/или уязвимостей [10], которая обуславливается следующими факторами:

– злоумышленники постоянно совершенствуют свои инструменты, используют новые методы и меняют направления своих атак, в том числе, в зависимости от сложившейся в мире обстановки (коронавирус, удаленная работа);

– инфраструктура объекта и модель угроз могут быстро меняться, реализация требований ИБ всегда будет запаздывать;

– новые угрозы ИБ и уязвимости появляются вместе с внедрением новых информационных технологий, например УБИ.135, УБИ.137, УБИ.138 – угрозы ИБ, возникающие при использовании облачных технологий и т.п. [11].

4) Невозможность полного блокирования отдельных угроз ИБ. Например: внедрение в систему и воздействие на нее вредоносного программного обеспечения – вирусы могут быть уже встроены в само оборудование [12]. Количество вирусов постоянно растет [13], только за второй квартал 2020 г. было выявлено 8 078 новых модификаций «шифровальщиков» и «майнеров». Вирусы постоянно совершенствуются и адаптируются к существующим методам противодействия [14] – современные злоумышленники располагают средствами для разработки, ПО, которое способно не только обходить антивирусы, но и выявлять технологии виртуализации («песочницы»). По словам экспертов, антивирусные программы просто не в состоянии предотвратить заражение. В 2019 г. вирусы применялись в 60–75% всех атак на госучреждения [14], в 2020 г. в 94% атак на промышленные предприятия [15].

5) Наличие в системе человеческого фактора. Человек был и остаётся наиболее уязвимым звеном в системе безопасности, поэтому нельзя сбрасывать со счетов возможность:

– реализации в отношении персонала методов социальной инженерии [10] (в 2019 г. социальная инженерия применялась примерно в 71% всех атак на госучреждения [14], в 2020 г. примерно в 67% атак на промышленные предприятия [15]);

– информационно-психологического воздействия в отношении персонала [16];

– недобросовестного отношение персонала (халатность) [14];

– непреднамеренных ошибок персонала [17];

– злонамеренных действий персонала [17].

Установленными в НПА КИИ мерами вышеуказанные угрозы можно значительно уменьшить (организация контроля физического доступа к компонентам системы, реализация правил разграничения доступа, информирование и обучение персонала, контроль за обеспечением безопасности объекта и т.д.), однако полностью исключить их невозможно. Принимая во внимание тот факт, что изнутри на систему воздействовать гораздо легче и последствий для функционирования может быть гораздо больше, реализация данных угроз может подорвать значительную часть системы безопасности объекта.

6) Может понадобиться значительное время для блокировки (устранения) обнаруженных угроз (уязвимостей) в процессе функционирования объекта [18].

Учитывая существующие проблемы, при оценке устойчивости ЗО КИИ необходимо придерживаться таких принципов, которые позволят исключить или минимизировать данные проблемы либо их деструктивное влияние на результаты работы.

Одной из причин существования указанных проблем является значительная сложность ЗО КИИ. Поэтому до начала проведения оценки устойчивости ЗО КИИ

необходимо создать упрощенную модель объекта. Сформулируем принципы оценки устойчивости ЗО КИИ, табл. 1.

Таблица 1. Существующие проблемы и принципы оценки устойчивости ЗО КИИ

Существующие проблемы	Принципы оценки устойчивости ЗО КИИ
Формальное выполнение требований нормативных документов в отдельных случаях не обеспечивает фактической защиты	При оценке устойчивости необходимо исходить из того, что система и её элементы всегда находятся в уязвимом состоянии и всегда имеются возможности для реализации отдельных угроз. Под угрозами ИБ, в данном случае, понимаются все возможные (на данном объекте) угрозы ИБ вне зависимости от потенциала нарушителя или сложности их реализации. Учёт угроз ИБ и уязвимостей системы, в данном случае, целесообразно осуществлять в виде анализа возможных последствий их реализации
Возможность пропуска отдельных угроз ИБ и/или уязвимостей элементов системы в ходе оценки угроз ИБ	
Возможность появления новых (ранее не известных) угроз ИБ и/или уязвимостей	
Невозможность полного блокирования отдельных угроз ИБ и/или устранения отдельных уязвимостей	
Наличие в системе человеческого фактора	При оценке устойчивости объекта необходимо учитывать возможные последствия от реализации целенаправленных и случайных угроз ИБ сотрудниками субъекта КИИ и/или персоналом объекта КИИ
Значительное время для блокировки отдельных угроз ИБ и/или устранения отдельных уязвимостей, обнаруженных в процессе функционирования объекта	Оценка устойчивости должна позволять заблаговременно обнаруживать такие элементы объекта, информационное воздействие на которые может привести к возникновению критической ситуации в кратчайшие сроки

При этом упрощенная модель объекта, в рассматриваемом случае, будет учитывать только информационные связи между элементами объекта и возможные состояния этих элементов после осуществления на них информационных воздействий (ИВ).

Из-за существенных различий в поведении системы в условиях целенаправленных и случайных ИВ устойчивость ЗО КИИ можно разделить на две составляющие:

– устойчивость к целенаправленным ИВ;
– устойчивость к случайным ИВ.

При оценке устойчивости объекта в условиях целенаправленных ИВ будут использоваться следующие допущения:

1) Каждый интерфейс, по которому элементы объекта взаимодействуют между собой, должен быть учтен как информационная связь [7].

2) Если два элемента объекта имеют информационную связь (проводная/беспроводная сеть, переносные носители информации), то возможно ИВ с одного элемента на другой и наоборот [19].

3) Злоумышленник может использовать любую информационную связь между элементами объекта для «перемещения» по объекту [20].

4) Злоумышленник знает архитектуру объекта, т.е. будет выбирать кратчайший маршрут для доступа к элементам объекта, которые непосредственно влияют на возникновение критического состояния значимого процесса и на которые возможно осуществление ИВ (критические элементы). Первым этапом целенаправленной атаки является сбор данных об атакуемой системе, в том числе и через сотрудников организации (инсайдеры). В случае если нарушитель сам является сотрудником организации, информация об архитектуре объекта

может быть доступна ему в силу служебного положения, неизвестную информацию он может добыть злонамеренными действиями внутри организации [20].

5) ЗО КИИ в большинстве случаев имеют информационные связи с корпоративной информационной сетью субъекта КИИ, ИВ на которую может стать угрозой ИБ для ЗО КИИ. Поэтому в рамках оценки условной устойчивости ЗО КИИ целесообразно рассматривать информационное пространство субъекта КИИ в целом – это ЗО КИИ и прилегающая информационная инфраструктура субъекта КИИ (корпоративная сеть) [9].

Вывод: основные принципы, сформулированные в данном разделе, позволят исключить/минимизировать существующие проблемы в области обеспечения безопасности ЗО КИИ при проведении оценки устойчивости функционирования объектов.

4. Отличие устойчивости от информационной безопасности объекта

В системах, предоставляющих критически важные услуги, устойчивость характеризуется четырьмя способностями: планировать/готовиться, поглощать, восстанавливаться и адаптироваться к известным и неизвестным угрозам [21].

Планирование/подготовка – создание основы для обеспечения выполнения процессов и функционирования объектов во время неблагоприятного события (сбоя или атаки).

Поглощение – поддержание наиболее важных функций объектов и выполнения процессов при отражении или локализации неблагоприятного события.

Восстановление – восстановление всех функций активов и доступности услуг до их функциональных возможностей до события.

Адаптация – использование знаний о неблагоприятном событии для изменения правил, конфигурации системы, обучения персонала или реализации иных мер по повышению устойчивости.

Данное определение вполне согласуется с тем, которое было сформулировано ранее (рис. 4):

- способность планировать/готовиться – защищённость;
- способность поглощать – живучесть/стойкость;
- способность восстанавливаться – восстанавливаемость;
- способность адаптироваться – адаптируемость.

Ключевым понятием устойчивости функционирования ЗО КИИ является принятие возможности реализации угрозы ИБ как вероятного события.

Основное внимание в данном случае уделяется способности системы адаптироваться и восстанавливаться, а не просто защищаться. Устойчивость в большей степени характеризует то, что происходит после реализации угрозы ИБ, и требует готовности, как к известным, так и к неизвестным угрозам [21].

Обеспечение устойчивости – это циклический процесс, основанный на постоянном совершенствовании систем предотвращения, поглощения, восстановления и адаптации.

В отличие от этого, ИБ направлена на защиту от реализации уже известных угроз ИБ, рис. 5.

Возможны также случаи, когда действия, направленные на повышение безопасности, наоборот приводят к понижению устойчивости объекта, например, ответные действия, предпринятые механизмом поддержки безопасности, приведут к каскадным сбоям и, в конечном итоге, к «поломке» компьютера, отключению критически важного программного обеспечения или повреждению важных данных.

Таким образом, «механизмы» контроля, предназначенные для поддержки безопасности информации, могут фактически нанести ущерб устойчивости [3].

Данная проблема достаточно актуальна, в качестве примера можно привести средство защиты информации от несанкционированного доступа SecretNet.

Реализация же функций по защите от НСД приводит к существенному замедлению работы системы, а в некоторых случаях является даже причиной отказа работы системы.

Рис. 4. Устойчивость, способности системы
Fig. 4. Stability, system capabilities

Рис. 5. Устойчивость и информационная безопасность
Fig. 5. Sustainability and information secURLty

ЗАКЛЮЧЕНИЕ

По результатам анализа отечественных и иностранных нормативных правовых актов и научных публикаций в статье сформулировано определение устойчивости функционирования значимых объектов КИИ в условиях угроз ИБ и установлено следующее:

– обеспечение устойчивости – это циклический процесс;

– ключевым понятием устойчивости функционирования ЗО КИИ является принятие возможности реализации угрозы ИБ как вероятного события;

– обеспечение ИБ объекта является обязательным, но не достаточным условием для обеспечения его устойчивого функционирования;

– применение отдельных мер обеспечения безопасности ЗО КИИ в зависимости от различных ситуаций может, как повысить, так и понизить устойчивость объекта.

Приведенные принципы построения модели объекта КИИ и визуализации процесса изменения его устойчивости (в разделе 2) можно использовать в дальнейшем при проведении оценки устойчивости объектов КИИ.

«Механизмы» контроля, предназначенные для поддержки безопасности информации, могут фактически нанести ущерб устойчивости. Данная проблема достаточно актуальна, в качестве примера можно привести средство защиты информации от несанкционированного доступа SecretNet. Реализация же функций по защите от НСД приводит к существенному замедлению работы системы, а в некоторых случаях является даже причиной отказа работы системы. Результаты исследования могут быть использованы при рассмотрении подходов оценки функционирования объектов КИИ и её усовершенствовании.

СПИСОК ЛИТЕРАТУРЫ:

1. 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 (дата обращения: 01.10.2022). – EDN YPERPV.
2. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры. Труды учебных заведений связи. 2020, № 4, с. 91–103. URL: https://cyberleninka.ru/article/n/kognitivnoe-modelirovanie-destruktivnyh-zloumyshlennyh-vozdeystviy-na-obektahkriticheskoy-informatsionnoy-infrastruktury (дата обращения: 01.10.2022).
3. Kott A. and Linkov I. To Improve Cyber Resilience, Measure It, in Computer. 2021, vol. 54, no. 2, p. 80–85. DOI: http://dx.doi.org/10.1109/MC.2020.3038411.
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.
5. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве. Наукоемкие технологии в космических исследованиях Земли. 2018, т. 10, № 2, с. 52–61. URL: https://cyberleninka.ru/article/n/metodika-otsenki-ustoychivosti-funktsionirovaniya-obektov-kriticheskoy-informatsionnoy-infrastruktury-funktsioniruyuschey-v/viewer (дата обращения: 01.10.2022).
6. Квасов М.Н., Криков А.П., Прохоров М.А. Практические рекомендации по обеспечению устойчивости функционирования автоматизированных систем специального назначения критически важными объектами в условиях деструктивных информационных воздействий. Известия ТулГУ. Технические науки. 2019, № 6, с. 14–21. URL: https://cyberleninka.ru/article/n/prakticheskie-rekomendatsii-po-obespecheniyu-ustoychivosti-funktsionirovaniya-avtomatizirovannyh-sistem-spetsialnogo-naznacheniya/viewer (дата обращения: 01.10.2022).
7. Митюков Е.А. Типовая архитектура распределенной АСУ ТП. Молодежная наука в развитии регионов. 2019, т. 1, с. 9–10. URL: https://www.elibrary.ru/item.asp?id=37318247 (дата обращения: 05.10.2022) – EDN IUZGDS.
8. Кубарев А.В. Вопросы реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Кибербезопасность цифрового предприятия. Онлайн-конференция, 4 декабря 2020. URL: https://www.all-over-ip.ru/2020/program/cybersecURLty (дата обращения: 06.10.2022).

9. Гарипов И.Р. Расчет риска нарушения информационной безопасности автоматизированной системы управления технологическим процессом. Молодежный вестник Уфимского государственного авиационного технического университета. 2019, № 1(20), с. 41–44. URL: https://elibrary.ru/item.asp?id=41122554 (дата обращения: 06.10.2022). – EDN OBHJPP.
10. 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.
11. Петухов А. Актуальные вызовы и возможности для информационной безопасности промышленных систем и предприятий. Кибербезопасность цифрового предприятия. Онлайн-конференция, 4 декабря 2020. URL: https://www.all-over-ip.ru/hubfs/AoIP%20ADAPT/AoIP_4-12-2020_Петухов.pdf?hsLang=ru (дата обращения: 10.10.2022).
12. Медведев В. Вы хотите защитить КИИ? Мы вас обрадуем – начать нужно с другого. Защита информации в АСУ ТП. Безопасность критической информационной инфраструктуры. Онлайн-конференция, 16 июля 2020. URL: https://www.itsec.ru/adapt/conference 16.07 (дата обращения: 10.10.2022).
13. Андрианов А.С., Вечёркин В.Б., Прохоров М.А., Цветков А.С. Разработка подхода к автоматизации процесса первичной обработки исходных данных для анализа устойчивости автоматизированных систем специального назначения в условиях деструктивных воздействий. Известия ТулГУ. Технические науки. 2018, № 10, с. 463–472. URL: https://cyberleninka.ru/article/n/razrabotka-podhoda-k-avtomatizatsii-protsessa-pervichnoy-obrabotki-ishodnyh-dannyh-dlya-analiza-ustoychivosti-avtomatizirovannyh/viewer (дата обращения: 11.10.2022).
14. Душкин В.В. Перспективные информационные технологии и актуальные угрозы: тренды и прогнозы. Национальный форум информационной безопасности «ИНФОФОРУМ» – Москва 2020. URL: https://infoforum.ru/conference/conference/program/cid/59?cid=59 (дата обращения: 11.10.2022).
15. Гусляев Г.А. Кибербезопасность, цифровые риски и угрозы. Кибербезопасность цифрового предприятия. Онлайн-конференция, 4 декабря 2020. URL: https://www.all-over-ip.ru/2020/program/cybersecURLty (дата обращения: 11.10.2022).
16. Климов С.М., Поликарпов С.В., Рыжов Б.С., Тихонов Р.И., Шпырня И.В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий. Вопросы кибербезопасности. 2019, № 6(34), с. 37–48. DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-37-48.
17. Кузнецов Д.Ю., Моделирование угроз на основе сценариев действий нарушителя. Национальный форум информационной безопасности «ИНФОФОРУМ» – Москва 2020. URL: https://infoforum.ru/conference/conference/program/cid/59?cid=59 (дата обращения: 11.10.2022).
18. Шушунова Т.Н., Лопаткин Д.С., Вакуленко В.Ф. Поиск подходов к оценке кибербезопасности цифровой трансформации химического комплекса. Экономическая безопасность. 2021, т. 4, № 4, с. 1005–1018. DOI: http://dx.doi.org/10.18334/ecsec.4.4.113496. – EDN BYZZTJ.
19. Муханова А.А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах. Вестник НГУ. Серия: Информационные технологии. 2013, т. 11, № 2, с. 55–72. URL: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-i-uyazvimostey-informatsionnoy-bezopasnosti-v-korporativnyh-sistemah (дата обращения: 11.10.2022).
20. Безукладников И.И., Миронова А.А., Южаков А.А. Таргетированные атаки в промышленных информационно-управляющих системах. Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. 2017, № 2(34), с. 54–66. DOI: http://dx.doi.org/10.15350/2306-2819.2017.2.54. – EDN ZAXPYH.
21. Linkov I., Eisenberg D.A., Plourde K. et al. Resilience metrics for cyber systems. Environ Syst Decis 33, 471–476 (2013). DOI: https://doi.org/10.1007/s10669-013-9485-y.

REFERENCES:

[1] Minaev V.A., Korolev I.D., Zelencova E.V., Zaharchenko R.I. Kriticheskaya informacionnaya infrastruktura: ocenka ustojchivosti funkcionirovaniya // Technologies and production RADIO INDUSTRY (RUSSIA). 2018, vol. 28, no. 4, p. 59–67. URL: https://elibrary.ru/item.asp?id=36511234 (дата обращения: 01.10.2022) (in Russian).– EDN YPERPV.
[2] Maksimova E.A. Kognitivnoe modelirovanie destruktivnyh zloumyshlennyh vozdejstvij na ob"ektah kriticheskoj informacionnoj infrastruktury. Trudy uchebnyh zavedenij svyazi. 2020, № 4, s. 91–103. URL: https://cyberleninka.ru/article/n/kognitivnoe-modelirovanie-destruktivnyh-zloumyshlennyh-vozdeystviy-na-obektahkriticheskoy-informatsionnoy-infrastruktury (accessed: 01.10.2022) (in Russian).
[3] Kott A. and Linkov I. To Improve Cyber Resilience, Measure It, in Computer. 2021, vol. 54, no. 2, p. 80–85. DOI: http://dx.doi.org/10.1109/MC.2020.3038411.

[4] Antonov S.G., Anciferov I.I., Klimov S.M. Metodika instrumental'no-raschetnoj ocenki ustojchivosti ob"ektov kriticheskoj informacionnoj infrastruktury pri informacionno-tekhnicheskih vozdejstviyah. Nadezhnost'. 2020, 20(4):35-41. DOI: https://doi.org/10.21683/1729-2646-2020-20-4-35-41 (in Russian).

[5] Zaharchenko R.I., Korolev I.D. Metodika ocenki ustojchivosti funkcionirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury funkcioniruyushchej v kiberprostranstve. Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2018, т. 10, no. 2, s. 52–61. URL: https://cyberleninka.ru/article/n/metodika-otsenki-ustoychivosti-funktsionirovaniya-obektov-kriticheskoy-informatsionnoy-infrastruktury-funktsioniruyuschey-v/viewer (accessed: 01.10.2022) (in Russian).

[6] Kvasov M.N., Krikov A.P., Prohorov M.A. Prakticheskie rekomendacii po obespecheniyu ustojchivosti funkcionirovaniya avtomatizirovannyh sistem special'nogo naznacheniya kriticheski vazhnymi ob"ektami v usloviyah destruktivnyh informacionnyh vozdejstvij. Izvestiya TulGU. Tekhnicheskie nauki. 2019, № 6, s. 14–21. URL: https://cyberleninka.ru/article/n/prakticheskie-rekomendatsii-po-obespecheniyu-ustoychivosti-funktsionirovaniya-avtomatizirovannyh-sistem-spetsialnogo-naznacheniya/viewer (accessed: 01.10.2022) (in Russian).

[7] Mityukov E.A. Tipovaya arhitektura raspredelennoj ASU TP. Molodezhnaya nauka v razvitii regionov. 2019, t. 1, s. 9–10.URL: https://www.elibrary.ru/item.asp?id=37318247 (accessed: 05.10.2022) (in Russian). – EDN IUZGDS.

[8] Kubarev A.V. Voprosy realizacii Federal'nogo zakona «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii». Kiberbezopasnost' cifrovogo predpriyatiya. Onlajn-konferenciya, 4 dekabrya 2020. URL: https://www.all-over-ip.ru/2020/program/cybersecURLty (accessed: 06.10.2022) (in Russian).

[9] Garipov I.R. Raschet riska narusheniya informacionnoj bezopasnosti avtomatizirovannoj sistemy upravleniya tekhnologicheskim processom. Molodezhnyj vestnik Ufimskogo gosudarstvennogo aviacionnogo tekhnicheskogo universiteta. 2019, № 1(20), s. 41–44. URL: https://elibrary.ru/item.asp?id=41122554 (accessed: 06.10.2022) (in Russian). – EDN OBHJPP.

[10] Penerdji Rustem V., Gavdan Grigory P. Information security of state information systems. IT Security, [S.l.], v. 27, no. 3, p. 26–42, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.3.03 (in Russian). – EDN PEHWST.

[11] Petuhov A. Aktual'nye vyzovy i vozmozhnosti dlya informacionnoj bezopasnosti promyshlennyh sistem i predpriyatij. Kiberbezopasnost' cifrovogo predpriyatiya. Onlajn-konferenciya, 4 dekabrya 2020. URL: https://www.all-over-ip.ru/hubfs/AoIP%20ADAPT/AoIP_4-12-2020_Петухов.pdf?hsLang=ru (accessed: 10.10.2022) (in Russian).

[12] Medvedev V. Vy hotite zashchitit' KII? My vas obraduem - nachat' nuzhno s drugogo. Zashchita informacii v ASU TP. Bezopasnost' kriticheskoj informacionnoj infrastruktury. Onlajn-konferenciya, 16 iyulya 2020. URL: https://www.itsec.ru/adapt/conference16.07 (accessed: 10.10.2022) (in Russian).

[13] Andrianov A.S., Vechyorkin V.B., Prohorov M.A., Cvetkov A.S. Razrabotka podhoda k avtomatizacii processa pervichnoj obrabotki iskhodnyh dannyh dlya analiza ustojchivosti avtomatizirovannyh sistem special'nogo naznacheniya v usloviyah destruktivnyh vozdejstvij. Izvestiya TulGU. Tekhnicheskie nauki. 2018, № 10, s. 463–472. URL: https://cyberleninka.ru/article/n/razrabotka-podhoda-k-avtomatizatsii-protsessa-pervichnoy-obrabotki-ishodnyh-dannyh-dlya-analiza-ustoychivosti-avtomatizirovannyh/viewer (accessed: 11.10.2022) (in Russian).

[14] Dushkin V.V. Perspektivnye informacionnye tekhnologii i aktual'nye ugrozy: trendy i prognozy. Nacional'nyj forum informacionnoj bezopasnosti «INFOFORUM» – Moskva 2020. URL: https://infoforum.ru/conference/conference/program/cid/59?cid=59 (accessed: 11.10.2022) (in Russian).

[15] Guslyaev G.A. Kiberbezopasnost', cifrovye riski i ugrozy. Kiberbezopasnost' cifrovogo predpriyatiya. Onlajn-konferenciya, 4 dekabrya 2020. URL: https://www.all-over-ip.ru/2020/program/cybersecURLty (accessed: 11.10.2022) (in Russian).

[16] Klimov S.M., Polikarpov S.V., Ryzhov B.S., Tihonov R.I., SHpyrnya I.V. Metodika obespecheniya ustojchivosti funkcionirovaniya kriticheskoj informacionnoj infrastruktury v usloviyah informacionnyh vozdejstvij. Voprosy kiberbezopasnosti. 2019, № 6 (34), s. 37–48. DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-37-48 (in Russian).

[17] Kuznecov D.YU. Modelirovanie ugroz na osnove scenariev dejstvij narushitelya. Nacional'nyj forum informacionnoj bezopasnosti «INFOFORUM» – Moskva 2020. URL: https://infoforum.ru/conference/conference/program/cid/59?cid=59 (accessed: 11.10.2022) (in Russian).

[18] SHushunova T.N., Lopatkin D.S., Vakulenko V.F. Poisk podhodov k ocenke kiberbezopasnosti cifrovoj transformacii himicheskogo kompleksa. Ekonomicheskaya bezopasnost'. 2021, t. 4, № 4, s. 1005–1018. DOI: http://dx.doi.org/10.18334/ecsec.4.4.113496 (in Russian). – EDN BYZZTJ.

[19] Muhanova A.A., Revnivyh A.V., Fedotov A.M. Klassifikaciya ugroz i uyazvimostej informacionnoj bezopasnosti v korporativnyh sistemah. Vestnik NGU. Seriya: Informacionnye tekhnologii. 2013, t. 11, № 2,

s. 55–72. URL: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-i-uyazvimostey-informatsionnoy-bezopasnosti-v-korporativnyh-sistemah (accessed: 11.10.2022) (in Russian).

[20] Bezukladnikov I.I., Mironova A.A., YUzhakov A.A. Targetirovannye ataki v promyshlennyh informacionno-upravlyayushchih sistemah. Vestnik Povolzhskogo gosudarstvennogo tekhnologicheskogo universiteta. Ser.: Radiotekhnicheskie i infokommunikacionnye sistemy. 2017, № 2(34), s. 54–66. DOI: http://dx.doi.org/10.15350/2306-2819.2017.2.54 (in Russian). – EDN ZAXPYH.

[21] Linkov I., Eisenberg D.A., Plourde K. et al. Resilience metrics for cyber systems. Environ Syst Decis 33, 471–476 (2013). DOI: https://doi.org/10.1007/s10669-013-9485-y.

Поступила в редакцию – 30 сентября 2022 г. Окончательный вариант – 03 ноября 2022 г.
Received – September 30, 2022. The final version – November 03, 2022.