УДК 004.056

Григорий П. Гавдан[1], Александр Н. Вавичкин[2], Виталий Г. Иваненко[3],
Юлия Д. Кулешова[4], Элина П. Рыбалко[5]
[1,2,3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[4]Государственный университет просвещения,
ул. Веры Волошиной, 24, Мытищи, Московская область, 141014, Россия
[5]Российский университет дружбы народов,
ул. Миклухо-Маклая, 6, Москва, 117198, Россия
[1]e-mail: gpgavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: anvavichkin@mephi.ru, https://orcid.org/0000-0001-9755-2167
[3]e-mail: vgivanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[4]e-mail: juliaybogdanova@mail.ru, https://orcid.org/0000-0001-8556-9340
[5]e-mail: rybalko.elina@mail.ru, https://orcid.org/0000-0001-6292-2535

УСТОЙЧИВОСТЬ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ В АСПЕКТЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2023.2.02

Аннотация. Киберпреступность сегодня приносит злоумышленникам доход (затрагивая и объекты критической информационной инфраструктуры) примерно 1,5 трлн долл. в год, а значит и защищённость критической информационной инфраструктуры (КИИ) продолжает требовать к себе должного внимания. Целью статьи является исследование технологических процессов в аспекте обеспечения безопасности информационной инфраструктуры. В настоящее время общепринятый подход к проведению такой оценки отсутствует и его определение остаётся актуальной задачей. Важно также понимать, что *не всегда* устойчивость технологических (в том числе и значимых, критических) процессов обеспечивает их безопасность (безопасность управления), также как и обеспечение безопасности *не обеспечивает* выполнение технологических процессов. Объектом исследования являются объекты КИИ. Предметом исследования являются технологические процессы в условиях угроз информационной безопасности. Проводится анализ нормативных правовых актов (НПА) и научных публикаций по теме исследования. Анализ НПА КИИ показал, что в данной области существуют проблемы. Для формулирования конкретных мер устойчивости показателей можно использовать приведённую матрицу устойчивости. В статье сформулированы требования к показателям оценки. По результатам работы установлено, что оценка устойчивости функционирования объектов может быть реализована на реальных значимых объектах КИИ, коэффициенты устойчивости элементов могут быть детализированы более подробно. Рассмотрены определения и проблемы, приведены основные источники, подтверждающие важность исследования. Результаты исследования могут быть использованы при рассмотрении подходов к оценке устойчивости технологических процессов в аспекте безопасности КИИ.

Ключевые слова: безопасность управления, значимый объект, критическая информационная инфраструктура, угрозы информационной безопасности, устойчивость критического процесса.
Для цитирования: Гавдан, Григорий П. и др. УСТОЙЧИВОСТЬ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ В АСПЕКТЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], т. 30, № 2, с. 38–52, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1500. DOI: http://dx.doi.org/10.26583/bit.2023.2.02.

Grigory P. Gavdan[1], Alexander N. Vavichkin[2], Vitaliy G. Ivanenko[3],
Yulia D. Kuleshova[4], Elina P. Rybalko[5]
[1,2,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[4]State university of education,

Vera Voloshina str., 24, Mytishchi, Moscow region, 141014, Russia
[5]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: anvavichkin@mephi.ru, https://orcid.org/ 0000-0001-9755-2167
[3]e-mail: vgivanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[4]e-mail: juliaybogdanova@mail.ru, https://orcid.org/0000-0001-8556-9340
[5]e-mail: rybalko.elina@mail.ru, https://orcid.org/0000-0001-6292-2535

Sustainability of technological processes in the aspect of security of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2023.2.02

Abstract. Cybercrime today brings attackers income (affecting critical information infrastructure objects) of about $1.5 trillion per year, which means that the security of critical information infrastructure (CII) continues to require due attention. The purpose of the article is to study technological processes in the aspect of ensuring the security of information infrastructure. Currently, there is no generally accepted approach to conducting such an assessment and its definition remains an urgent task. It is also important to understand that the stability of technological (including significant, critical) processes does not always ensure their safety (management safety), as well as ensuring safety does not ensure the execution of technological processes. The object of the study is the objects of CII. The subject of the study is technological processes in the context of threats to information security. The analysis of regulatory legal acts (RLA) and scientific publications on the research topic is carried out. The analysis of the RLA of the CII showed that there are problems in this area. To formulate specific measures of sustainability of indicators, you can use the given sustainability matrix. The article formulates the requirements for evaluation indicators. Based on the results of the work, it was found that the assessment of the stability of the functioning of objects can be implemented on real significant objects of the CII, the stability coefficients of the elements can be detailed in more detail. Definitions and problems are considered, the main sources confirming the importance of the study are given. The results of the study can be used when considering approaches to assessing the sustainability of technological processes in the aspect of CII safety.

Keywords: management security, significant object, critical information infrastructure, threats to information security, stability of critical process.
For citation: GAVDAN, Grigory P. et al. Sustainability of technological processes in the aspect of security of critical information infrastructure. IT Security (Russia), [S.l.], v. 30, no. 2, p. 38–52, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1500. DOI: http://dx.doi.org/10.26583/bit.2023.2.02.

Введение

В выступлении на XXVII сессии Комиссии по предупреждению преступности и уголовному правосудию было (14.05.2018 в городе Вена) заявлено[1] Генсекретарём ООН А. Гутеррешем, что киберпреступность злоумышленникам приносит дохода (затрагивая, в том числе и объекты критической информационной инфраструктуры) около 1,5 трлн долл. в год. Доходы злоумышленников продолжают расти, а значит защищённость и критической информационной инфраструктуры (КИИ) напрямую *зависит* от владения соответствующими органами (структурами) новых видов «оружия» и средств защиты информации (СЗИ), от методов (и степени) их использования и эффективности защиты информации.

[1]XXVII сессии Комиссии по предупреждению преступности и уголовному правосудию. URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/27th-crime-commission-lays-groundwork-for-further-integrating-prevention--criminal-justice-responses--says-unodc-executive-director.html (дата обращения: 15.12.2022).

Военные теоретики рассматривают информационное пространство наряду с наземным, морским, воздушным и космическим пространствами в качестве «пятого поля боя» [1]. Информационное противоборство в информационном пространстве накаляется. Модель информационного противоборства представлена авторами в статье [2, с. 153]. В документах стратегического планирования международных организаций и ведущих государств концептуализируются таким же образом глобальное информационное пространство и киберпространство [3].

По оценке экспертов [4], в настоящее время эффект целевого применения кибернетического «оружия» против информационных систем (ИС) сравним с эффектом применения оружия массового поражения [5]. В частности, например, в киберстратегии Пентагона (США) говорится «… Северная Корея и Иран также использовали злостную кибердеятельность, чтобы нанести ущерб гражданам США и поставить под угрозу интересы Соединённых Штатов… Растущая зависимость США от киберпространства… становится неприемлемым риском для нации». Или, например, «Критическая нехватка лекарств – угроза национальной безопасности, говорится в докладе Конгресса»: В США с полок исчезли многие жизненно важные препараты и антибиотики – как оказалось, отрасль сильно зависит от Китая, импортозамещения нет. Такая же проблема существует и в России. В настоящее время Китай сделал глобальный шаг вперед, укрепив свои межгосударственные связи, например, с Россией и Саудовской Аравией, которая присоединилась к возглавляемому Китаем блоку безопасности.

Рынок кибербезопасности Российской Федерации (РФ) по результатам 2021 г. оценён в 185,9 млрд руб. Совокупная доля услуг составила 27%, а поставки средств защиты информации, в том числе программных – 73% всего объёма рынка[2] (российские вендоры СЗИ занимали 61% рынка, тогда как зарубежные – 39%). Продолжающиеся зарубежной политикой наложения санкций (связанные с СВО) вынуждают иностранные компании на выполнение невыгодного им шага, уход с российского рынка.

Долевое распределение представленных на рынке в 2021 г. категорий услуг в области обеспечения информационной безопасности (ИБ) был распределён следующим образом[2]:

2% – расследование инцидентов;
3% – оценка защищённости;
17% – консалтинг;
19% – сопровождение;
29% – аутсорсинг (включая MSSP/MDR);
30% – внедрение (включая проектирование).

Для анализа подходов к оценке устойчивости технологических процессов в аспекте безопасности КИИ, как основной цели исследования и формулирования вывода, рассмотрим вначале основные терминологические понятия устойчивости технологического процесса.

1. Устойчивость технологического процесса

В целом *технологический процесс (ТП)* – установленная соответствующими технологическими документами последовательность действий, взаимосвязанных между собой и направленных на объект процесса с целью получения требуемого результата.

[2]Прогноз развития рынка кибербезопасности в Российской Федерации на 2022-2026 годы. Август 2022. Фонд «Центр стратегических разработок». URL: https://www.csr.ru/upload/iblock/13f/ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf (дата обращения: 15.02.2023).

Состоят технологические процессы из рабочих операций, которые могут быть связаны друг с другом с помощью технологических переходов[3].

Под нарушением устойчивости системы будем понимать любое изменение её состояния, приводящее к отсутствию соответствия целевому значению. При создании реальных сложных систем *устойчивость обеспечивается* в результате *оптимального сочетания* детерминированного и вероятностного подходов [6] к воздействию дестабилизирующих факторов. В различных сферах науки, применительно к конкретным сферам использования сложных систем, встречается большое количество определений устойчивости, что затрудняет определение данной категории сущности и содержанию для устойчивости производственных систем [6].

Под термином «устойчивость» будем понимать заимствование из теории управления физическими (техническими) системами, где он используется в качестве характеристики, определяющей способность системы автоматического управления сохранять в процессе работы своё установившееся состояние или восстанавливать его (а также переходить в новое состояние) после устранения действия дестабилизирующего фактора [6]. В табл. 1 приведены отличительные особенности производственной системы.

Таблица 1. Отличительные особенности производственной системы (фрагмент) [6]

Отличительные особенности производственной системы	**Требования к устойчивости производственной системы**
В системе протекают производственные процессы, основной и определяющей частью которых являются технологические процессы, благодаря которым происходит превращение отдельных элементов в полезную продукцию	С организационно-производственной точки зрения основным требованием, предъявляемым к производственной системе, является поддержание стабильного уровня выходных характеристик при наличии различного рода внешних и внутренних отклоняющих воздействий
В производственной системе протекают логистические процессы. Они охватывают движение материальных и информационных потоков с рынка закупок до рынка потребителей готовой продукции через всю необходимую совокупность производственных и др. процессов	Обеспечение функционирования производственного процесса в соответствии с поставленной целью и всей производственно-хозяйственной деятельности предприятия

Основные причины нарушения устойчивости ТП носят универсальный характер. На основании термина «устойчивость» в области информационной безопасности сформировался термин «киберустойчивость», который можно сформулировать следующим образом: киберустойчивость – это способность информационных систем осуществлять свое штатное (целевое) функционирование в условиях (на них) воздействия [6] компьютерных атак (КА) в киберпространстве (подход предполагает построение аналитических моделей реализации КА. Также может применяться, например, метод преобразования стохастических сетей) [7]. В отношении критических объектов в иностранной литературе применяется понятие «киберустойчивость» – способность системы противостоять кибератакам, восстанавливаться после них [8].

Остановимся на объектах, отнесенных к КИИ. В соответствии с Федеральным законом РФ № 187-ФЗ[4] критическая информационная инфраструктура – это объекты КИИ, а также используемые для организации взаимодействия таких объектов сети электросвязи.

[3]Сайт Центр сертификации – Центр «ГОСТ Р». г. Санкт-Петербург. URL: https://gostus.com/about/ (дата обращения: 15.02.2023).

2. Устойчивость технологического процесса в аспекте ИБ КИИ

Киберпространство (согласно ISO/IEC 27032:2012) – это комплексная среда, возникшая в результате взаимодействия подключенных к сети «Интернет» людей, программного обеспечения (ПО) и услуг, которая не существует в материальной форме[5].

Кибербезопасность – это действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов. То есть, кибербезопасность – это состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз[6].

Киберустойчивость – это способность информационной инфраструктуры успешно предотвращать реализацию угроз или быстро восстанавливаться после их реализации.

Киберустойчивость является *интегральным показателем* и определяется такими показателями, как *киберживучесть*, *киберпомехоустойчивость* и *кибернадежность*, которые и отражают возможность выполнять свои задачи в системе управления КИИ в условиях деструктивных информационных воздействий [9]. Понятие «киберустойчивость» можно отнести к понятию «устойчивость функционирования в условиях угроз ИБ». По своей сути понятия очень схожи. Подходы, применяемые для оценки киберустойчивости, можно также использовать в том или ином виде и при оценке устойчивости функционирования объектов в условиях угроз информационной безопасности (УИБ). Вероятность нарушения функционирования объектов КИИ, обусловленная имеющейся возможностью возникновения нежелательных воздействий на их информационные элементы, заставляет рассматривать устойчивость объектов КИИ в условиях влияния на них УИБ. Оценка эффективности применяемых мер по обеспечению безопасности значимых объектов (ЗО) КИИ по своей сути определяется устойчивостью критических процессов (КП).

Подходы на основе показателей используют функции системы для оценки общей устойчивости системы или меры индивидуальных свойств компонентов [3], в то время как подходы на основе моделей используют моделирование конфигурации системы и анализ сценариев для прогнозирования динамики устойчивости системы (динамическая оценка) [3].

Изложенный в [10] анализ литературы, по организации обеспечения безопасности КИИ, надежности и устойчивого функционирования автоматизированной системы управления объектов КИИ показал, что в них не рассмотрены следующие вопросы, связанные с разработкой моделей, методов и методик [10]:

– оценка состояния объектов КИИ;

– формирование признакового пространства функционирования КИИ;

– создание и ведение единой распределенной базы данных с оперативной аналитической обработкой данных;

– адаптивное управление КИИ, учитывающих текущее и прогнозируемое состояние объектов КИИ в условиях деструктивных информационных воздействий.

---

[4]Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 05.02.2023).

[5]ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity // International Organization for Standardization. URL: http://www.iso.org/standard/44375.html (дата обращения: 05.12.2022).

[6]ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. URL: https://docs.cntd.ru/document/1200114169 (дата обращения: 05.12.2022).

Из [10] следует, что единственная реальная защита, которую могут предпринять специалисты по кибербезопасности, – укрепить системное множество потенциальных киберугроз и добиться исключения доступа киберсистем к интернету.

Оценку устойчивости можно применять на основе:

– показателей для стратегического управления устойчивостью (на этапе «планирования/подготовки», в том числе до начала эксплуатации объекта);

– структурно-функциональной модели во время и после реализации для определения изменений и оперативного управления объектом (этапы «поглощение», «восстановление» и «адаптация»).

В международной практике существуют различные методики оценки устойчивости, например, Cyber Resilience Review (CRR) – это пакет методологических документов, разработанный Министерством внутренней безопасности США. Данная оценка предназначена для измерения киберустойчивости организации, а также для анализа недостатков с целью улучшения на основе признанной передовой практики. CRR оценивает корпоративные программы и практики в следующих функциях управления [7], например:

– управление активами;
– управление средствами контроля;
– управление конфигурацией и изменениями;
– управление уязвимостями и т.д.

CRR, помимо самой методики оценки киберустойчивости, ещё содержит и руководства, которые помогут внедрить необходимые практики по каждой из вышеупомянутых функций управления [8].

Системы и сети реального мира состоят из взаимосвязанных физических элементов, устройств связи, людей и окружающей среды. Устойчивость системы во многом зависит от эффективности межобластного взаимодействия и координации на каждом этапе цикла управления событиями.

Остановимся на определениях.

Информационная область: информация и разработка информации о физической области.

Киберустойчивость (собственно, как и устойчивость в условиях угроз ИБ) следует рассматривать в контексте сложных систем, которые включают не только физические и информационные, но также когнитивные и социальные области [6].

Физическая область: физические ресурсы, возможности и структура этих ресурсов.

Когнитивная область: использование информации и физических областей для принятия решений.

Социальная область: организационная структура и коммуникации для принятия когнитивных решений.

Смоделировать функционирование сложной системы одновременно в четырех указанных областях является достаточно сложной задачей. Планируемая устойчивость требует для проведения измерений использования точных метрик [11].

Для формулирования конкретных мер устойчивости показателей киберустойчивости можно использовать матрицу устойчивости [11], представленную в табл. 2 (важно: выполнение циклов происходит по шкале времени).

Таблица 2. Матрица устойчивости, отображающая системные домены в рамках цикла [11]

Предыдущий цикл	**Планирование / Подготовка**	**Поглощение**	**Восстановление**	**Адаптация**
Физическая область	Состояние и возможности оборудования и персонала, структура сети	Распознавание событий и показателей работы системы для поддержания работоспособности	Изменение системы для восстановления предыдущей функциональности	Изменения для повышения устойчивости системы
Информа-ционная область	Подготовка, представление, анализ и хранение данных	Оценка функциональности в реальном времени, прогнозирование каскадных сбоев и происшествий	Использование данных для отслеживания прогресса восстановления и прогнозирования сценариев восстановления	Создание и улучшение протоколов хранения и использования данных
Когнитивная область	Решения по проектированию и эксплуатации системы с учетом возможности неблагоприятных событий	План действий в нештатных ситуациях и упреждающее (проактивное) управление событиями	Принятие решений по восстановлению и коммуникация	Разработка новых конфигураций системы, целей и критериев принятия решений
Социальная область	Социальная сеть, социальный капитал, институциональные и культурные нормы и обучение	Квалифицированные и доступные кадры и социальные учреждения для реагирования на события	Командная работа и обмен знаниями для улучшения восстановления системы	Добавление или изменение институтов, политик, программ обучения и культуры

3. Формулировка показателей для оценки устойчивости объектов КИИ

В соответствии со сформулированным определением, *устойчивость функционирования ЗО КИИ* – это свойство объекта выполнять свои основные функции (управление значимым процессом, обработку информации, необходимой для обеспечения значимого процесса), в условиях:

– попыток реализации угроз ИБ (этап подготовка, отражение);
– во время реализации угроз ИБ (этап поглощение, оперативное восстановление);
– после реализации угроз ИБ (восстановление и адаптация).

Данные функции должны осуществляться таким образом, чтобы исключить наступление значимых последствий. Любой объект КИИ можно разделить на *управляющую* и *управляемую части*.

В *информационных системах* (ИС) происходит управление процессом обработки информации.

В *информационно-телекоммуникационных сетях* (ИТКС) происходит управление процессом обмена информацией.

В *автоматизированных системах управления* (АСУ) может происходить управление как физическим, так и информационным процессом.

Управляющая часть объекта КИИ – совокупность элементов объекта, с помощью которых осуществляется управление значимым процессом (ЗП).

Управляющая часть системы безопасности – совокупность элементов объекта, с помощью которых осуществляется управление средствами обеспечения безопасности.

В случае если информационное воздействие затрагивает управляющую часть, канал управления или канал обратной связи, процесс управления может, наоборот, привести к нарушению ЗП, рис. 1.

3.1. Формулировка требований к показателям оценки

Управление указанными процессами происходит на основе распознавания отклонений четко определенных параметров: изменения температуры элементов, повышения загруженности канала передачи данных и т.п.

Если нарушение целостности или доступности информации возможно обнаружить, (хотя порой не совсем своевременно), то нарушение конфиденциальности информации без обнаружения самого воздействия определить, никак не получится [12].

Устойчивость выполнения ЗП зависит от устойчивости обеспечивающих его элементов [13]. Что в свою очередь зависит от их защищенности и устойчивости процесса управления их функционированием [14].

Защищённость элементов объекта увеличивает запас времени для реагирования на атаки и заставляет злоумышленников использовать различные средства и методы воздействия, что также повышает и вероятность их обнаружения, тем самым создавая запас устойчивости объекта.

Защищенность элементов можно оценивать в зависимости от соответствия применяемых к ним мер и средств [14], требованиям приказа 239, а также устойчивости функционирования самих СЗИ, которая в свою очередь зависит от защищённости СЗИ и устойчивости процесса управления их функционированием.

Обнаружение нарушений функционирования элементов системы (система управления ЗП) повышает вероятность обнаружения нарушений функционирования СЗИ (реализацию угроз в отношении СЗИ) и наоборот, т.е. для повышения устойчивости объекта КИИ необходимо осуществление взаимосвязанного управления и функционированием элементов системы и СЗИ, а также обеспечение максимального уровня защищенности элементов объекта и СЗИ. Такое взаимосвязанное управление возможно при наличии системы обеспечения устойчивости, которая должна быть отказоустойчивой и иметь возможность управления как системой управления ЗП, так и с системой управления безопасностью, и в то же самое время сама не должна [1] создавать угроз ИБ, представлена далее на рис. 2.

$x(t)$, $x'(t)$, $X(t)$, $X'(t)$, $X_{1,2,3}(t)$ – являются передаточными функциями обратной связи процесса управления системы обеспечения устойчивости объекта. Учитывая тот факт, что в состав отдельных элементов объекта входит персонал организации, а также принимая во внимание функционирование объекта в четырех областях (в том числе когнитивной и социальной), передаточная функция в отдельных случаях будет являться абстрактным понятием и представлять собой определенный порядок передачи информации, регламентированный в организации руководящими документами.

Переменная x показывает изменение состояния значимого процесса, а x' – изменение состояний критических элементов значимого процесса. Передаточные функции $x(t)$ и $x'(t)$ определяются еще на этапе проектирования объекта КИИ, а дублирование информации на управляющую часть системы обеспечения устойчивости (УЧ СОУ) целесообразно обеспечивать путем дублирования управляющей части объекта КИИ (УЧ ЗП). Кроме того, каналы обратной связи должны быть максимально разделены друг от друга.

Передаточные функции, определяющие переменные *x*1, *x*2, *x*3 и т.д., определяются на этапе проектирования системы безопасности объекта КИИ (СБ), при этом управляющая часть системы безопасности (УЧ СБ) и средства обеспечения безопасности [14] должны соответствовать требованиям нормативных документов ФСТЭК России (приказы 235 и 239).

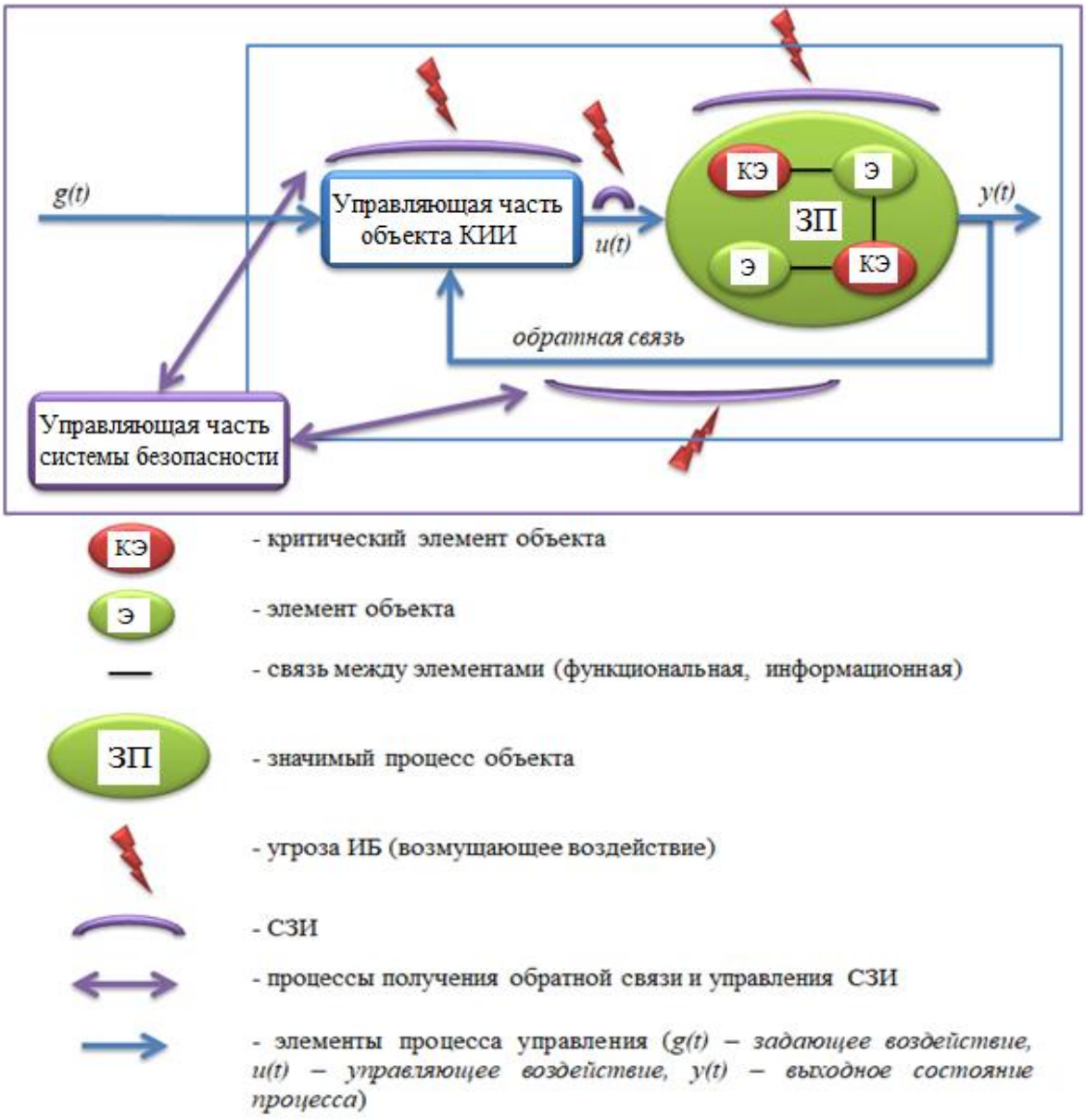

Рис.1. Основные процессы объектов КИИ
(значимый процесс, процесс управления значимым процессом)
Fig.1. The main processes of CII objects
(significant process, process of managing a significant process)

Передаточные функции, определяющие переменные *X*, *X'*, $X_{1,2,3}$ должны обеспечивать передачу информации о текущем состоянии процесса управления ЗП, процесса обеспечения безопасности, процесса функционирования смежных систем и сетей субъекта КИИ, а также информацию о текущем состоянии отдельных элементов, обеспечивающих указанные процессы (о случаях нарушения/прекращения их функционирования).

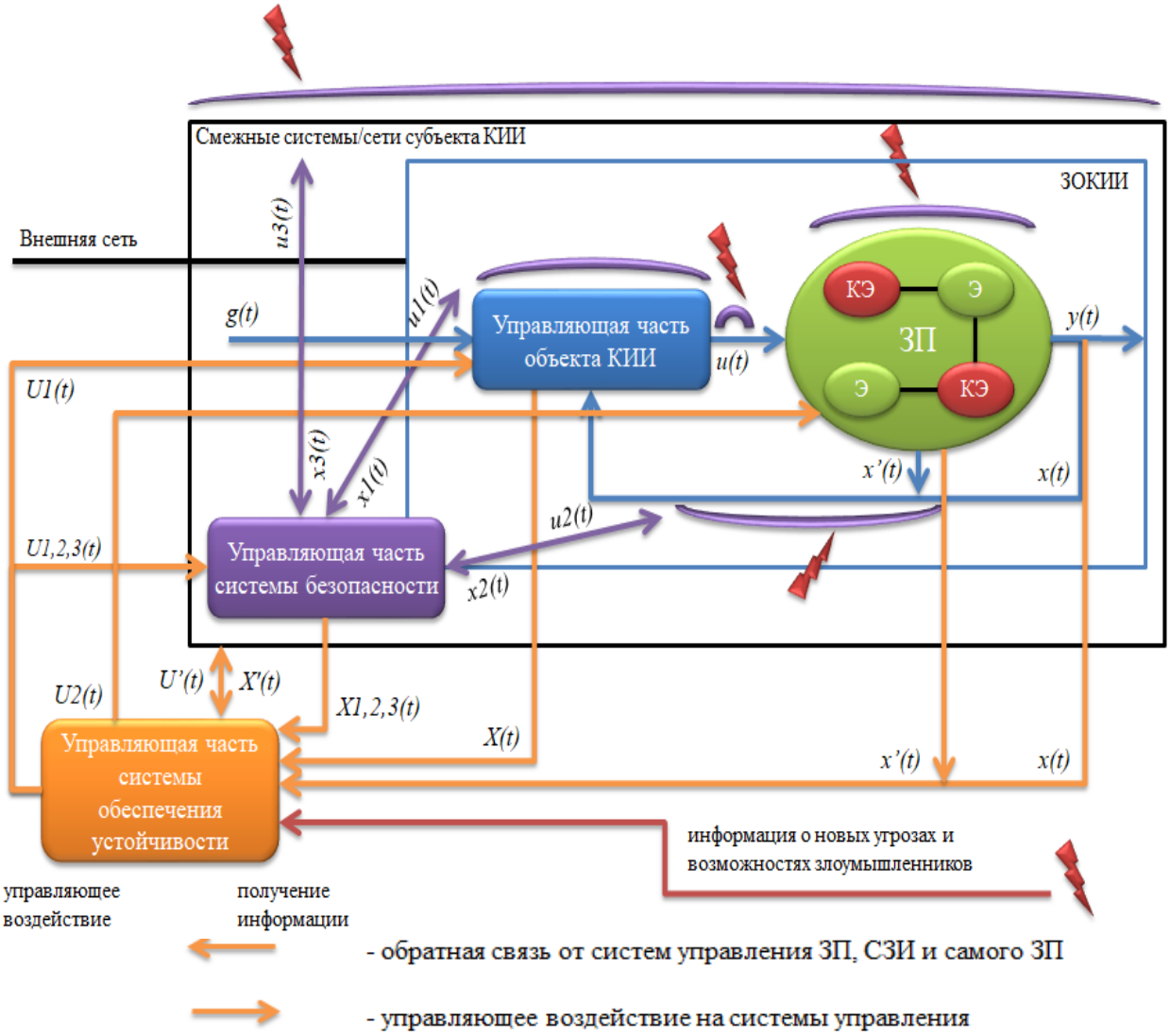

Рис. 2. Система обеспечения устойчивости объектов КИИ
Fig. 2. The system for ensuring the stability of CII objects

Сама система обеспечения устойчивости [15] должна иметь возможность перепроверки данных от различных служб и процессов для определения правильных результатов, т.е. должна быть защищена от «византийских сбоев» – когда узлы системы могут преднамеренно выдавать неправильные данные.

Необходимость взаимосвязи двух систем можно продемонстрировать на примере атаки на систему противоаварийной защиты (ПАЗ) нефтеперерабатывающего завода Petro Rabigh в Саудовской Аравии (2017) [16]. Так атака была обнаружена не сразу и первоначально была принята за обычный сбой контроллеров ПАЗ, его отключили. Служба безопасности не была вовремя проинформирована, и атака продолжилась до того момента пока количество атакованных контроллеров ПАЗ не увеличилось. Данные контроллеры ПАЗ работали в разных сегментах сети на различных установках производства, что могло в конечном итоге привести к выбросу ядовитых газов или даже их детонации. Однако одной взаимосвязью вышеуказанных систем проблему нехватки времени на реагирование не решить, этот вопрос всегда будет стоять очень остро, особенно в достаточно больших и сложных системах.

Для повышения эффективности управления система обеспечения устойчивости должна быть не только реактивной (отвечать на осуществляемое информационное воздействие), но также и проактивной – реагировать (усиливать устойчивость объекта на определенных направлениях) в соответствии с информацией о возможных угрозах, в том числе новых.

Устойчивое функционирование ЗО КИИ (управление объектом) должно соответствовать вышеуказанным требованиям, а саму устойчивость и ее оценку следует рассматривать в контексте сложных систем, включающих физическую (Ф), информационную (И), когнитивную (К) и социальную (С) области [6].

Показатели такой оценки удобнее всего формировать с помощью матрицы показателей устойчивости [17] или в духе системной инженерии [18].

3.2. Формулировка показателей оценки устойчивости

Оценка устойчивости будет включать в себя оценку динамической устойчивости (управление функционированием) составляющих частей элементов объекта КИИ и оценку запаса (защищенность) устойчивости.

Устойчивость рассчитывается для каждого элемента объекта в отдельности, однако для однотипных элементов (одинаковые ТС с одинаковыми программами и СЗИ), расположенных в одном сегменте сети, показатель устойчивости будет один и тот же. Например, можно использовать предложенную в [19] матрицу.

Для упрощения оценки устойчивости отдельным показателям в матрице сопоставлены меры обеспечения безопасности, указанные в приказе 239 ФСТЭК России.

Следует отметить, что многие меры ФСТЭК России выполняются сразу на нескольких этапах обеспечения устойчивости функционирования элемента, имеют различный масштаб и пересекаются между собой, поэтому сопоставление данных мер с матрицей устойчивости еще нуждается в доработке.

Для более детальной расстановки мер ФСТЭК по ячейкам матрицы устойчивости необходимо проведение работ по формулировке однозначных определений данных мер и описанию всех действий, выполняющихся при их реализации.

Устойчивость элемента объекта состоит из устойчивости его составляющих частей [6]: программно-аппаратных (железо + системное ПО) средств (ПАС), прикладного ПО (ППО), средств защиты информации (СЗИ) и персонала, эксплуатирующего элемент (трудовые ресурсы – ТР) [18]. Устойчивость функционирования составляющих частей элемента системы зависит от человеческого фактора (правильная установка и настройка, безопасная эксплуатация и т.д.) [12].

При расчете устойчивости определенной составляющей учитываются только те меры, которые можно реализовать в отношении нее, т.е. для разных составляющих (ПАС/ППО/СЗИ) будет свой перечень мер. Если отдельные меры безопасности не реализованы ввиду физического отсутствия соответствующих им угроз ИБ, то количество необходимых мер ($К_{НМ}$) уменьшается на количество указанных отсутствующих мер.

Критерии оценки еще нуждаются в уточнении, как и формулы, по которым происходит их преобразование в итоговый показатель устойчивости элементов.

Применение логико-вероятностного подхода [20], как и когнитивного [21] также может иметь место.

Помимо этого, для корректной расстановки коэффициентов $К_{1.1}$ необходимо использование информации о требованиях к уровням доверия 1–3, что выходит за рамки данной работы.

Устойчивость элементов системы можно представить в виде среднеарифметического,

минимального и другого значения составляющих его подэлементов (в зависимости от целей оценки).

Например, устойчивость АРМа может зависеть от устойчивости ППО, ПАС и СЗИ:

$$У_Э = \text{min/ср. арифм./др. } (К_{УСТ\ ПАС}; К_{УСТ\ ППО}; К_{УСТ\ СЗИ}) \times (1 - Р_{НП\ Э})$$

где $У_Э$ – устойчивость элемента объекта; $К_{УСТ\ ППО}$ – устойчивость прикладного программного обеспечения элемента; $К_{УСТ\ ПАС}$ – устойчивость программно-аппаратных средств элемента; $К_{УСТ\ СЗИ}$ – устойчивость СЗИ элемента; $Р_{НП\ Э}$ – вероятность наступления недопустимых последствий (последствий, которые могут привести к нарушению КП) в результате информационного воздействия на элемент (в случае, если $Р_{НП\ Э} = 1$, то вместо $(1 – Р_{НП\ Э})$ в формулу подставляется значение 0,01).

Приближенно $Р_{НП\ Э}$ можно рассчитать пропорцией, разделив количество состояний элемента, которые могут привести к нарушению КП, на количество всех возможных состояний элемента после реализации угроз ИБ.

Применительно к АРМу можно определить шесть возможных состояний элемента после информационного воздействия: утечка, модификация, разрушение защищаемой информации, нарушение функционирования, захват управления (полный контроль над элементом) или разрушение элемента. В нашем случае недопустимые последствия будут во всех 6 состояниях элемента и $(1 – Р_{НП\ Э}) = 0,01$.

$У_Э$ показывает относительную вероятность элемента сохранить неизменность своего состояния в условиях возможной реализации угроз ИБ (вероятность высчитывается относительно максимальной, которая получается при соблюдении всех возможных требований к устойчивости подэлементов).

Устойчивость системы к реализации случайных антропогенных и техногенных угроз, обусловленных ошибками персонала или сбоями оборудования, можно представить в виде среднеарифметического, минимального или другого значения произведений устойчивостей элементов на вероятность наступления критических ситуаций для данных элементов (в случае если реализация угрозы происходит только в отношении одного элемента и распространение дальше невозможно):

$$У_{ОКИИ} = \min (У_{Э1.}; У_{Э2.}; \dots У_{Эn.}) \text{ либо } У_{ОКИИ} = (У_{Э1.} + У_{Э2.} \dots + У_{Эn.}) / n$$

$$У_{ОКИИ} = \min (У_{Э1.}; У_{Э2.}; \dots У_{Эn.})$$

либо

$$У_{ОКИИ} = (У_{Э1.} + У_{Э2.} \dots + У_{Эn.}) / n$$

где $У_{ОКИИ}$ – устойчивость объекта к случайных антропогенным или техногенным угрозам ИБ; $У_Э$ – устойчивость элемента объекта.

Анализируя вышеуказанную информацию можно заметить, что статическая оценка устойчивости показывает обобщенную характеристику объекта и актуальна при долгосрочном планировании и стратегическом управлении объектом, однако для оперативного управления необходимо использование другого подхода, например, основанного на моделировании объекта и его процессов [22]. Также помним, что защита КИИ – это ещё и безопасное окружение [23], а не только защита промышленных протоколов, контроль целостности и т.д.

Заключение

По результатам исследования установлено, что оценка устойчивости функционирования объектов может быть реализована на реальных объектах КИИ, коэффициенты устойчивости элементов могут быть детализированы более подробно.

В работе в результате проведенного исследования установлено:

– при оценке устойчивости функционирования критических информационных объектов необходимо одновременно использовать подходы на основе показателей и моделей, которые будут дополнять друг друга;

– устойчивость функционирования критических информационных объектов в условиях угроз ИБ следует рассматривать в контексте сложных систем, которые включают в себя не только физические и информационные области, но также социальные и когнитивные;

– на основе полученных результатов, был выработан подход и сформулированы общие требования к оценке устойчивости функционирования ЗО КИИ в условиях угроз ИБ;

– абсолютной устойчивости объекта КИИ добиться невозможно, можно лишь повысить устойчивость системы в условиях реализации угроз ИБ определенного масштаба, на примере рассмотренных целенаправленных информационных воздействий, или реализации случайных антропогенных и техногенных угроз ИБ (ошибки людей и отказы ТС, ПО);

– сформулированные основные требования к показателям для статической и динамической оценки устойчивости функционирования ЗО КИИ позволяют выполнить расчёт устойчивости объекта к различным угрозам ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Libicki M. Cyberspace in Peace and War. Naval Institute Press, 2016. – 478 p.
2. 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://elibrary.ru/item.asp?id=34939627 (дата обращения: 01.02.2023). – EDN: XNRISL.
3. Department of Defense Cyber Strategy 2018. Summary. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 01.10.2022).
4. 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.
5. Kott A. andLinkov I. To Improve Cyber Resilience, Measure It. in Computer. Feb. 2021, vol. 54, no. 2, p. 80–85. DOI: http://dx.doi.org/10.1109/MC.2020.3038411.
6. Шотыло Д.М. Сущность и содержание устойчивости производственной системы. ЭКОНОМИНФО. 2006, № 6. URL: https://cyberleninka.ru/article/n/suschnost-i-soderzhanie-ustoychivosti-proizvodstvennoy-sistemy/viewer (дата обращения: 21.12.2022).
7. Чупров С.В. Мониторинг устойчивости производственных систем. Иркутск: Изд-во БГУЭП, 2005. – 231 с. URL: https://search.rsl.ru/ru/record/01002813504 (дата обращения: 01.10.2022).
8. Котенко И.В., Саенко И.Б., Коцыняк М.А., Лаута О.С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей. Тр. СПИИРАН, 55 (2017), с. 160–184. URL: https://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=trspy&paperid=981&option_lang=rus (дата обращения: 21.11.2022).
9. Бачевского С.В. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция. СПб.: СПбГУТ, 2017. – 580 с. URL: https://elibrary.ru/item.asp?id=29890038 (дата обращения: 15.12.2022). – EDN: WQROHP.
10. Руслан Рахметов, Security Vision. Кибербезопасность, киберустойчивость, киберучения – что это? URL: https://www.securityvision.ru/blog/razbor-terminologii-kiberbezopasnost-kiberustoychivost-kiberucheniya-chto-eto/ (дата обращения: 15.12.2022).
11. Linkov I., Kott A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. DOI: http://dx.doi.org/10.1007/978-3-319-77492-3_1.
12. Linkov I., Eisenberg D., Bates M., Chang D., Convertino M., Allen J., Flynn S., Seager T, Measurable Resilience for Actionable Policy. Environ. Sci. Technol. 2013, 47, p. 10108−10110. DOI: dx.doi.org/10.1021/es403443n.
13. 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.

14. 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. DOI: http://dx.doi.org/10.26583/bit.2022.4.05. – EDN: OKPDVN.
15. Кубарев А.В. Вопросы реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Кибербезопасность цифрового предприятия. Онлайн-конференция, 4 декабря 2020. URL: https://ict.moscow/presentation/voprosy-realizatsii-federalnogo-zakona-o-bezopasnosti-kriticheskoi-informatsionnoi-infrastruktury-rossiiskoi-federatsii/ (дата обращения: 06.10.2022).
16. 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/cybersecurity (дата обращения: 11.10.2022).
17. Прошин А. Аварийная ситуация: как противостоять атакующему системы ПАЗ вредоносу Trisis. Публикация от 19 октября 2021 г. URL: https://www.securitylab.ru/analytics/523661.php (дата обращения: 11.10.2022).
18. 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.
19. Bodeau, D.J., Graubart, R.D. (2019). Systems Engineering Approaches. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-77492-3_9.
20. 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). DOI: https://doi.org/10.21681/2311-3456-2019-6-37-48.
21. Вечеркин В.Б., Галанкин А.В., Прохоров М.А. Методика оценивания устойчивости функционирования автоматизированной системы управления критической информационной инфраструктурой в условиях информационного воздействия. Известия ТулГУ. Технические науки. 2018, вып. 6: с. 160–169. URL: https://cyberleninka.ru/article/n/metodika-otsenivaniya-ustoychivosti-funktsionirovaniya-avtomatizirovannoy-sistemy-upravleniya-kriticheskoy-informatsionnoy (дата обращения 01.05.2022).
22. 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).
23. 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 г. URL: https://www.itsec.ru/adapt/conference16.07 (дата обращения 10.10.2022).

REFERENCES:

[1] Libicki M. Cyberspace in Peace and War. Naval Institute Press, 2016. – 478 p.
[2] 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, t. 10, № 2, s. 52–61. URL: https://elibrary.ru/item.asp?id=34939627 (дата обращения: 01.02.2023) (in Russian). – EDN: XNRISL.
[3] Department of Defense Cyber Strategy 2018. Summary. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed: 01.10.2022).
[4] Minaev V.A., Korolev I.D., Zelencova E.V., Zaharchenko R.I. Critical information infrastructure: sustainability assessment. Technologies and production radio industry (russia). 2018, vol. 28, no. 4. URL: https://elibrary.ru/item.asp?id=36511234 (дата обращения: 01.10.2022) (in Russian). – EDN YPERPV.
[5] Kott A. andLinkov I. To Improve Cyber Resilience, Measure It. in Computer. Feb. 2021, vol. 54, no. 2, p. 80–85. DOI: http://dx.doi.org/10.1109/MC.2020.3038411.
[6] SHotylo D.M. Sushchnost' i soderzhanie ustojchivosti proizvodstvennoj sistemy. EKONOMINFO. 2006, № 6. URL: https://cyberleninka.ru/article/n/suschnost-i-soderzhanie-ustoychivosti-proizvodstvennoy-sistemy/viewer (accessed: 21.12.2022) (in Russian).
[7] CHuprov S.V. Monitoring ustojchivosti proizvodstvennyh system. Irkutsk: Izd-vo BGUEP, 2005. – 232 s. URL: https://search.rsl.ru/ru/record/01002813504 (accessed: 01.10.2022) (in Russian).

[8] Kotenko I.V., Saenko I.B., Kocynyak M.A., Lauta O.S. Ocenka kiberustojchivosti komp'yuternyh setej na osnove modelirovaniya kiberatak metodom preobrazovaniya stohasticheskih setej. Trudy SPIIRAN. 55 (2017), s. 160–184. URL: https://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=trspy&paperid=981&option_lang=rus (accessed: 21.11.2022) (in Russian).

[9] Bachevskogo S.V. Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii. VI Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya. SPb.: SPbGUT, 2017. – 580 s. URL: https://elibrary.ru/item.asp?id=29890038 (accessed: 15.12.2022) (in Russian). – EDN: WQROHP.

[10] Ruslan Rahmetov, Security Vision. Kiberbezopasnost', kiberustojchivost', kiberucheniya – chto eto? URL: https://www.securityvision.ru/blog/razbor-terminologii-kiberbezopasnost-kiberustoychivost-kiberucheniya-chto-eto/ (accessed: 15.12.2022).

[11] Linkov I., Kott A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. DOI: http://dx.doi.org/10.1007/978-3-319-77492-3_1.

[12] Linkov I., Eisenberg D., Bates M., Chang D., Convertino M., Allen J., Flynn S., Seager T, Measurable Resilience for Actionable Policy. Environ. Sci. Technol. 2013, 47, p. 10108−10110. DOI: dx.doi.org/10.1021/es403443n.

[13] Antonov S.G., Antsiferov I.I., Klimov S.M. Method of instrumental estimation of critical information infrastructure under information technology interference. Dependability. 2020; 20(4): 35–41. DOI: https://doi.org/10.21683/1729-2646-2020-20-4-35-41 (in Russian).

[14] 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. DOI: http://dx.doi.org/10.26583/bit.2022.4.05 (in Russian). – EDN: OKPDVN.

[15] 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://ict.moscow/presentation/voprosy-realizatsii-federalnogo-zakona-o-bezopasnosti-kriticheskoi-informatsionnoi-infrastruktury-rossiiskoi-federatsii/ (accessed: 06.10.2022) (in Russian).

[16] 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).

[17] Proshin A. Avarijnaya situaciya: kak protivostoyat' atakuyushchemu sistemy PAZ vredonosu Trisis. Publikaciya ot 19 oktyabry 2021. URL: https://www.securitylab.ru/analytics/523661.php (accessed: 11.10.2022) (in Russian).

[18] 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.

[19] Bodeau, D.J., Graubart, R.D. (2019). Systems Engineering Approaches. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-77492-3_9.

[20] 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). DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-37-48 (in Russian).

[21] Vecherkin V.B., Galankin A.V., Prohorov M.A. Metodika ocenivaniya ustojchivosti funkcionirovaniya avtomatizirovannoj sistemy upravleniya kriticheskoj informacionnoj infrastrukturoj v usloviyah informacionnogo vozdejstviya. Izvestiya TulGU. Tekhnicheskie nauki. 2018, vyp. 6: s. 160–169. URL: https://cyberleninka.ru/article/n/metodika-otsenivaniya-ustoychivosti-funktsionirovaniya-avtomatizirovannoy-sistemy-upravleniya-kriticheskoy-informatsionnoy (accessed: 01.05.2022) (in Russian).

[22] 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).

[23] 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).

Поступила в редакцию – 06 декабря 2022 г. Окончательный вариант – 12 апреля 2023 г.
Received – December 06, 2022.The final version – April 12, 2023.