DOI: 10.25728/mlsd.2022.1013

КЛАССИФИКАЦИЯ И ОЦЕНКА ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Абдулова Е.А., Калашников А.О.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва ул. Профсоюзная д.65
consoft@ipu.ru, aokalash@ipu.ru

Аннотация: оценка критичности критической инфраструктуры является важной задачей в комплексе задач по обеспечению защиты критической инфраструктуры. В статье представлена характеристика подхода к классификации объектов критической инфраструктуры (КИ) и критической информационной инфраструктуры (КИИ). Представлена процедура идентификации и категоризации объектов КИ и КИИ.

Ключевые слова: критическая инфраструктура, методы оценки критичности, кибербезопасность.

Введение

21 век — это эра технологий ради удобства, мощности и возможностей. Коммуникации, торговля, финансы и все формы управления и доступа к информации могут осуществляться практически из любого места. Благодаря широкому распространению Интернета и беспроводных сетей передачи данных именно взаимосвязь большого количества данных и множества устройств быстро стала основой современного общества. Современное общество – это общество, основанное на знаниях, которое в значительной степени полагается на технологии для выполнения или поддержки выполнения задач или функций. В результате современное общество гораздо более уязвимо даже по сравнению с началом века.

Масштабы уязвимости обусловлены тем, что очень много выполняемых операций в какой-то момент поддерживается вводом, хранением и поиском данных и информации во взаимосвязанной сети жестких дисков и серверов данных. Более того, в каждом из этих моментов существует возможность кражи информации, обхода защит, манипулирования или диверсии. При этом не учитывается риск, связанный с непреднамеренными инцидентами, связанными с человеческим фактором, системными сбоями, несовместимостью или другими неожиданными проблемами, а также «стихийными бедствиями».

Таким образом, безопасность этих компьютерных или «кибер»-систем является вопросом национальной безопасности. Эти угрозы настолько велики, что все больше и больше экспертов по безопасности заявляют, что защита киберсистем и данных является более серьезной проблемой, чем терроризм, учитывая масштаб угрозы (относительно натиска кибератак) и фактический ущерб, который наносится на ежегодной основе (а также возможные последствия в случае компрометации определенных систем и структур) [1-3].

Однако киберинфраструктура (критическая информационная инфраструктура) государства — лишь одна из многих важных систем и сетей. Государство и общество полностью зависят от функционирования различных инфраструктурных систем и компонентов. Потеря любого из этих различных критически важных элементов инфраструктуры может легко привести к потере возможности передвижения людей и вещей, нарушению торговли и коммерции, разрыву связи как на короткие, так и на большие расстояния, потере производства и передачи электроэнергии, и т.д.

Приоритетной целью государственной политики на сегодняшний день является обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ) Российской Федерации (КИИ РФ), так и КИИ в целом [4, 5]. Для успешной реализации мероприятий по обеспечению безопасности объектов КИИ РФ и КИИ РФ в целом необходимо решение целого ряда сложных научно-технических задач, из которых задача оценки текущего уровня безопасности объектов КИИ РФ и КИИ РФ в целом и прогнозирования его изменения является одной из ключевых [6].

Оценка критичности критической инфраструктуры, в том числе и КИИ, является важной задачей в комплексе задач по обеспечению защиты критической инфраструктуры.

1 Функции и категории кибербезопасности

В 2014 г в США была разработана национальная система кибербезопасности, а основу которой заложен подход базирующийся на оценке риска, который помогает при столкновении с угрозами кибербезопасности, систематически рассматривать, что они собой представляют (люди, информация, объекты и т. д.), и каковы возможные последствия этих угроз, что можно сделать для устранения этих угрозы, как отреагировать на угрозы, и что можно сделать, чтобы обеспечить быстрое восстановление

[1]. На рис. 1 представлены функции и категории в соответствии с этим подходом. На рис. 2 представлены потоки информации и решений в рамках этого подхода [7] на уровнях внутри организации:

- верхний уровень управления,
- уровень бизнес-процессов,
- уровень реализации/эксплуатации.

Функция	Категория	Идентификатор
Идентификация риска	Управление активами	ID.AM
	Бизнес среда	ID.BE
	Управление безопасностью	ID.GV
	Оценка рисков	ID.RA
	Стратегия управления рисками	ID.RM
	Управление рисками цепочек поставок	ID.SC
Киберзащита	Управление идентификацией и контроль доступа	PR.AC
	Осведомленность и обучение	PR.AT
	Безопасность данных	PR.DS
	Процессы и процедуры киберзащиты	PR.IP
	Обслуживание	PR.MA
	Технология киберзащиты	PR.PT
Обнаружение инцидентов кибербезопасности	Аномалии и события кибербезопасности	DE.AE
	Непрерывный мониторинг кибербезопасности	DE.CM
	Процессы обнаружения инцидентов	DE.DP
Реагирование на инциденты кибербезопасности	Планирование реагирования	RS.RP
	Связи	RS.CO
	Анализ	RS.AN
	Минимизация последствий	RS.MI
	Улучшения	RS.IM
Восстановление	Планирование восстановления	RC.RP
	Улучшения	RC.IM
	Связи	RC.CO

Рис. 1. Функции и категории кибербезопасности

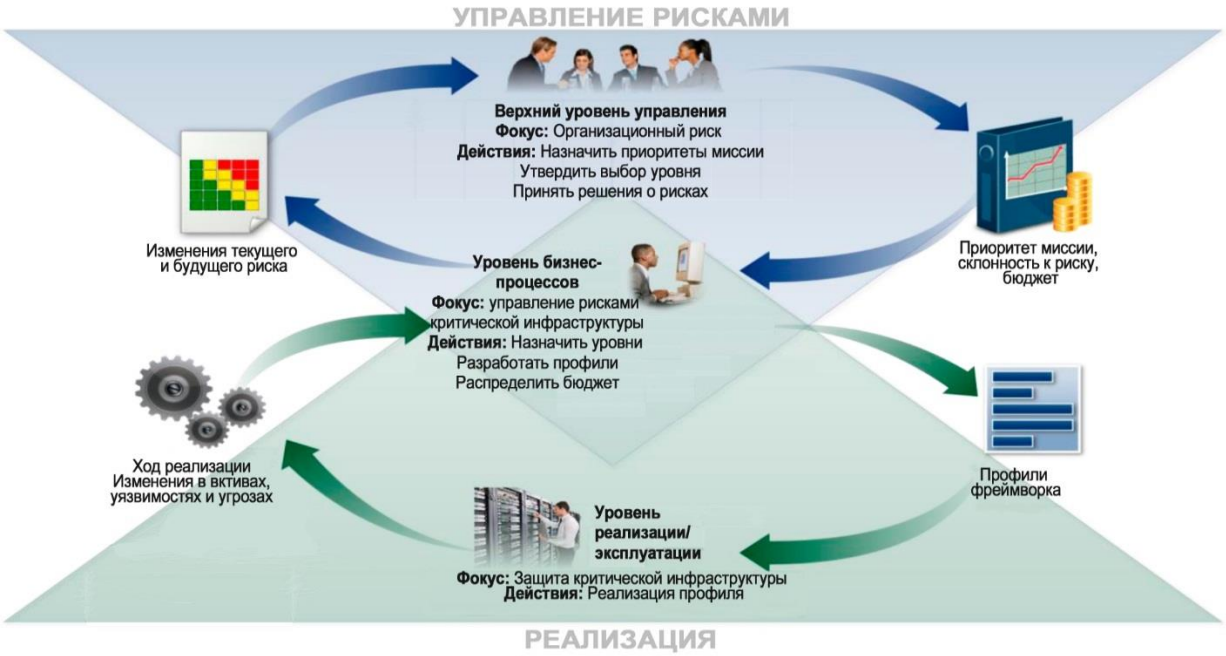

Рис. 2. Условные потоки информации и решений внутри организации

Верхний уровень управления сообщает о приоритетах миссии, доступных ресурсах и общей допустимости риска на уровне бизнес-процессов. Уровень бизнес-процессов использует эту информацию в качестве входных данных для процесса управления рисками, а затем взаимодействует с уровнем реализации/эксплуатации, для сообщения потребностей и создания профилей. Уровень реализации/эксплуатации сообщает о ходе реализации профиля на уровне бизнес-процесса. На уровне бизнес-процесса эта информация используется для оценки воздействия. Менеджмент на уровне бизнес-процесса сообщает о результатах этой оценки воздействия на верхний уровень управления, в

целях информирования о протекании общего процесса управления рисками организации, и на уровень реализации/эксплуатации для понимания влияния на происходящие процессы.

2 Категории кибер-целей

Кибер-цели в критической инфраструктуре можно оценивать и классифицировать по целевым характеристикам. Каждая цель имеет определенные характеристики, которые составляют основу для обнаружения, определения местоположения, идентификации и классификации цели для последующего наблюдения, анализа, нападения и оценки. Можно выделить четыре категории характеристик, на основе которых можно определить обычные цели: физические, функциональные, когнитивные, экологические [8].

Основными характеристиками цели являются физические особенности: форма, внешний вид, количество и природа элементов, отражательная способность, структурный состав, степень упрочнения, электромагнитное излучение, местоположение, размер и дисперсия. Примером характеристик окружающей среды являются особенности местности. К когнитивным функциям относятся, например, способ обработки информации целью, информация, которая требуется цели для функционирования, также сюда относятся процессы, которые выполняет цель, количество информации, которую может обрабатывать цель и как цель или система хранит информацию. Функциональные особенности — к ним относятся, например, какие материалы или ресурсы требуются цели для функционирования.

Преобразование физических и экологических характеристик в киберпространство может быть осуществлено путем преобразования их в виртуальные характеристики и функции информационной инфраструктуры. Физические характеристики будут преобразованы в виртуальные характеристики кибер-цели, такие как операционная система, необходимая эффективность процессора, необходимый объем памяти и форматы файлов или данных. Кибер-цель также может иметь интерфейс к физическому пространству, что позволяет злоумышленнику проникнуть в систему кибер-цели через физическое соединение. Характеристики среды будут учитывать характеристики сети, такие как сетевые протоколы, уровни, серверные операционные системы и базы данных, т.е., характеристики информационно инфраструктуры.

Функциональные характеристики учитывают, что выполняет кибер-цель. Например, такими характеристиками могут быть мобильность цели, способность ее защищаться и восстанавливаться. Эти характеристики у кибер- и обычной целей очень похожи. Когнитивные особенности кибер-цели — это, например, способы обработки информации, обработки ввода и вывода и способы хранения информации.

Общие физические и экологические характеристики должны быть преобразованы в виртуальные характеристики, а функциональные и когнитивные характеристики очень похожи в физическом и кибер- пространствах. Аналогия между физическими и кибер-характеристиками целей показана на рис. 3.

Кибер-цель может быть разделена на разные категории в зависимости от уровня цели. Высшим уровнем концепции кибер-цели будет система кибер-цели, которая формируется из подсистем и является основной целью атаки. Это может быть, например, SCADA или система управления объектом критической инфраструктуры. Кибер-целями будут отдельные функции и подсистемы, необходимые для функционирования всей системы.

Объект кибер-цели — это часть кибер-цели, которая может быть уничтожена по отдельности, но необходима для работы целевой системы. Объектом кибер-цели может быть один процесс, файл, датчик или одна функция. Объекты кибер-цели автономны, соединяются вместе и формируют услугу. Уровни кибер-цели представлены на рис. 4.

На уровне кибер-целей системы к целям можно отнести SCADA или другие информационные системы, сети и сетевые коммуникации или информационно-телекоммуникационная инфраструктура организаций, содержащая, например, хранилища данных, офисное программное обеспечение и системы обработки сертификатов безопасности. Сложная и распределенная структура этого уровня создает против нее несколько векторов атак.

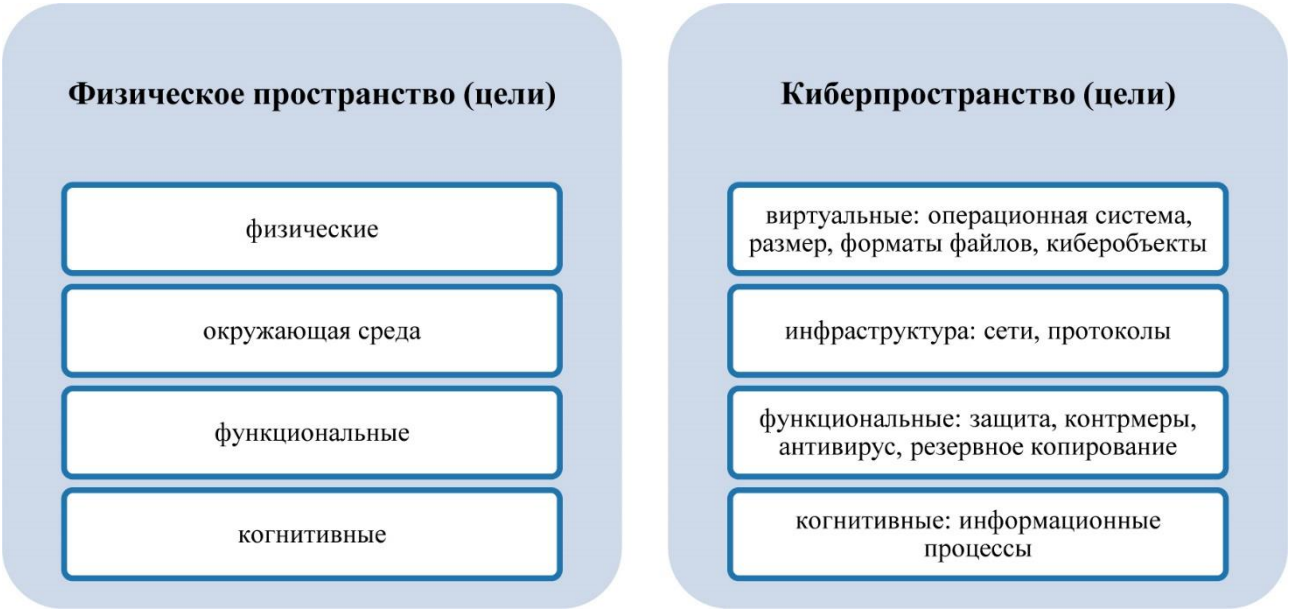

Рис. 3. Аналогия между характеристиками обычных и кибер- целей

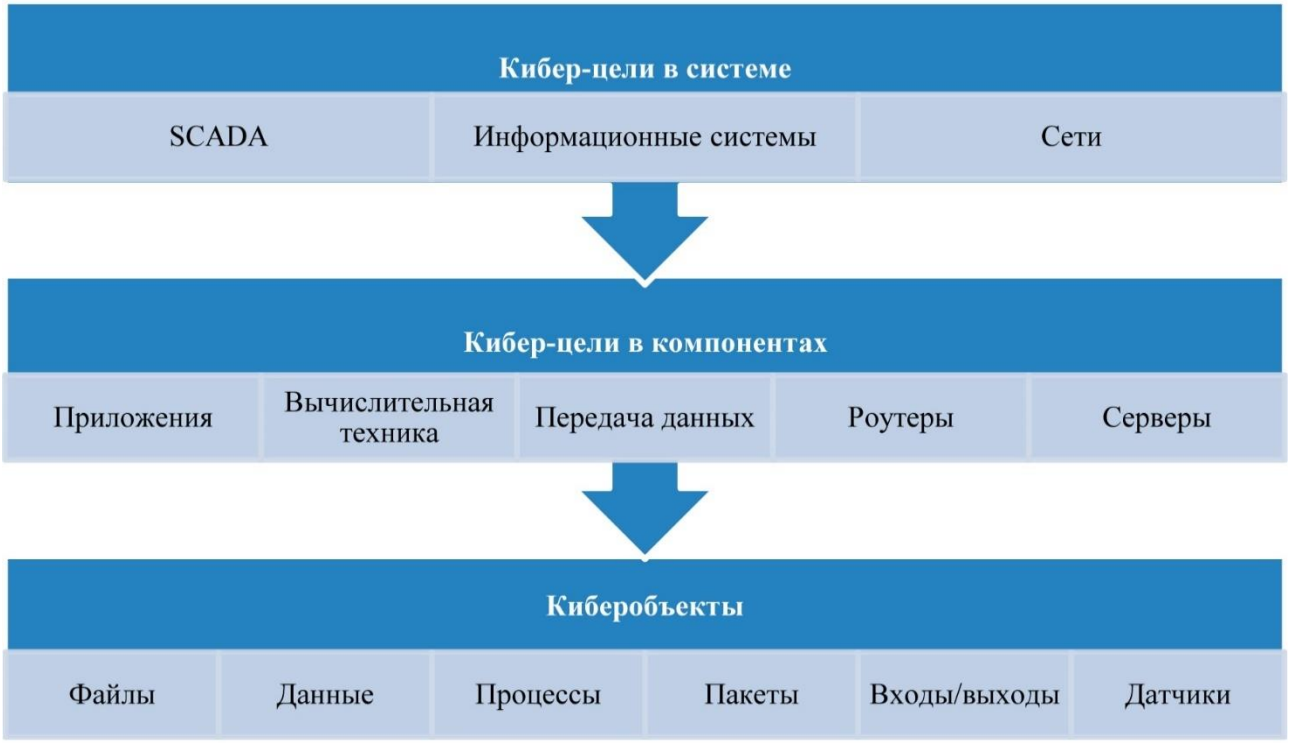

Рис. 4. Уровни кибер-целей

Кибер-цель в системе также может быть гибридной, существующей как в киберпространстве, так и в физическом пространстве. В такой системе можно оказывать влияние на конечного пользователя через систему, даже если пользователь не существует в киберпространстве или целью может быть физическое устройство.

3 Характеристика подхода к классификации объектов критической инфраструктуры

При оценке критичности критической инфраструктуры, включая КИИ, важно понимать разницу в методологических подходах к оценке критичности и риска (или рискового потенциала [9-12]). При оценке критичности объекта инфраструктуры в первую очередь учитывают оценку негативного воздействия инфраструктуры на население, общество, окружающую среду, экономику государства, национальную безопасность и т.д. То есть важно оценить ущерб, который был бы вызван, если бы объект перестал функционировать или был бы уничтожен. Вероятность инцидента считается равной единице. При анализе рисков сначала анализируют угрозу активам объекта и оценивают ущерб,

который будет нанесен самому объекту. В этом принципиальное различие между подходами к оценке критичности и оценке риска.

Основными критериями, возникающими при оценке критичности объекта критической инфраструктуры, являются: воздействие на общество; экономический эффект; воздействие на окружающую среду; политическое влияние; влияние на национальную безопасность; оценка взаимозависимости, т.е. влияния на функционирование другой критической инфраструктуры. При оценке также учитываются: масштаб воздействия (каскадные эффекты, географический масштаб и др.), временные характеристики - скорость проявления негативного воздействия, продолжительность воздействия, время восстановления безопасного состояния.

Можно выделить 5 категорий критичности:

- I категория критичности - критические объекты (объекты общегосударственного значения, имеющие разветвленные связи и значительное влияние на другую инфраструктуру).
- II категория критичности - жизненно важные объекты, выход из строя которых приведет к кризису регионального значения.
- III категория критичности - важные объекты.
- IV категория критичности - необходимые объекты.
- V категория критичности - некритичные объекты.

Оценка критичности объектов критической инфраструктуры (КИ) и объектов критической информационной инфраструктуры на основе следующих принципов и допущений:

- Идентификация объектов КИИ осуществляется в пределах секторов (подсекторов) критической инфраструктуры. При этом, следует учитывать идентификацию объектов критической инфраструктуры и соответствующих видов их услуг и функций.
- Объект критической инфраструктуры рассматривается как актив критической инфраструктуры (в частности, как организационно-техническая система).
- Идентификация и категоризация объектов КИ и КИИ осуществляется в рамках сектора (подсектора) критической инфраструктуры.
- Категорирование объектов критической инфраструктуры осуществляется по двум группам критериев. Первая группа – отраслевые критерии, вторая группа – межотраслевые критерии. Отраслевые критерии разрабатываются индивидуально для каждого сектора и применяются исключительно к объектам КИ этого сектора критической инфраструктуры. Межотраслевые критерии и применяются ко всем объектам КИ, независимо от их отраслевой значимости.
- Отнесение объекта КИ к определенной категории критичности осуществляется на основе полученных баллов объекта КИ по каждому критерию критичности. Определение категории критичности основано на анализе суммы полученных баллов и использовании универсальной шкалы Харрингтона.
- Оценка критичности объекта КИИ осуществляется на основе его влияния (информационные, телекоммуникационные системы, автоматизированные систем и т.д.) на функциональность и целостность объектов КИ, способность непрерывно и устойчиво работать, обеспечивать жизненно важные услуги и функции. В случае определения влияния объекта КИИ на функционирование объекта КИ категория критичности объекта КИИ приравнивается к критичности объекта КИ.

Критичность объекта инфраструктуры определяется на основе анализа возможного ущерба обществу, окружающей среде, экономике, национальной безопасности государства в результате нарушения или приостановления эксплуатации объекта инфраструктуры. Важность критической инфраструктуры оценивается с использованием следующих наборов критериев, аналогичных критериям для КИИ [5]:

- социальная значимость объекта инфраструктуры;
- политическая значимость объекта инфраструктуры;
- хозяйственное значение объекта инфраструктуры;
- взаимосвязь между объектами критической инфраструктуры (негативное влияние на непрерывное и устойчивое функционирование другого объекта инфраструктуры, предоставляющего такую же жизненно важную услугу (функцию); негативное влияние на непрерывное и устойчивое функционирование другого объекта инфраструктуры, обеспечивающего другие жизненно важные услуги (функции));
- значение для национальной безопасности.

Каждому критерию соответствуют показатели, соответствующие одной из четырех категорий критичности. Для категорирования формируется команда специалистов, которая оценивает объект по каждому критерию. Оценка проводится методом экспертного опроса и/или мозгового штурма. Каждый ответ оценивается в баллах:

I категория – 4 балла,

II категория – 3 балла,

III категория – 2 балла,

IV категория – 1 балл.

Также дается «некритичный» ответ – 0 баллов.

Обобщенная категория критичности определяется обобщенным индексом и универсальной шкалой Харрингтона. Пусть у нас есть m метрик, которые измеряют критичность объекта CI_i. Объект может получить максимальное количество баллов CI_{max}, если он оценивается как критический в первой категории по всем показателям. Тогда обобщенный показатель уровня критичности можно рассчитать по формуле:

$$CI_{OI} = \frac{\sum_{i=1}^{m} CI_i}{CI_{\max}}.$$

Предлагается принять решение об отнесении объекта критической инфраструктуры к одному из критических уровней на основе использования универсальной шкалы Харрингтона [13]. Таким образом, классификация критичности представляет собой правило:

- если $0.8 < CI_{OI} \leq 1$, то категория критичности I,
- если $0.63 < CI_{OI} \leq 0.8$, то категория критичности II,
- если $0.37 < CI_{OI} \leq 0.63$, то категория критичности III,
- если $0.2 < CI_{OI} \leq 0.37$, то категория критичности IV,
- если $CI_{OI} \leq 0.2$, то категория критичности V.

После определения критичности объекта инфраструктуры следует провести идентификацию и категоризацию объекта информационной инфраструктуры. Для этого оператор объекта критической инфраструктуры формирует полный перечень информационно-телекоммуникационных систем и сетей, используемых на объекте критической инфраструктуры, а затем оценивает влияние этих систем на непрерывность и устойчивость предоставления жизненно важных услуг (функций).

Заключение

В докладе рассмотрены функции и категории кибербезопасности, а также категории кибер-целей.

Рассмотрен подход к оценке критичности объектов информационной инфраструктуры, состоящий из этапов:

- Первый этап: определение и регулирование важнейших секторов инфраструктуры (и подсекторов) и типичных жизненно важных услуг, предоставляемых в соответствующем секторе;
- Второй шаг — оценка критичности инфраструктуры. Оценка проводится по нормативным критериям оценки критичности. Оценка производится методами неформального анализа - методами экспертного опроса, методами мозгового штурма и др.
- Третий этап: оценка критичности объектов информационной инфраструктуры. Критичность объектов информационной инфраструктуры оценивается на основе анализа потребности в информационно-телекоммуникационных системах для непрерывного функционирования и оценка влияния информационно-телекоммуникационных систем на непрерывность и устойчивость предоставления жизненно важных услуг и функций.

В докладе предлагается подход для оценки критичности КИ, в котором критерии критичности инфраструктуры определяются уровнем КИ по каждому критерию и уровнем критичности в баллах. Общий уровень критичности оценивается на основе анализа обобщенной нормативной оценки (сумма всех баллов) с последующей универсальной шкалой Харингтона. Это позволяет применить более гибкий подход к определению критических объектов разных категорий, оптимизировать затраты на обеспечение защиты объектов. В дальнейшем для получения более точных оценок можно использовать корректировку весов критериев.

Литература

1. *Bullock J.A., Haddow G.D., Coppola D.P.* Cybersecurity and critical infrastructure protection (in book Introduction to Homeland Security Principles of All-Hazards Risk Management – Elsevier. 2021. – P.425-497.
2. *Markopoulou D., Papakonstantinou V.* The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular // Computer Law & Security Review. Vol. 41. 2021, 105502.
3. *Maglaras L.A., Kim K.H., Janicke H., Ferrag M.A., Rallis S., Fragkou P., Maglaras A., Cruz T.J.* Cyber security of critical infrastructures. // ICT Express. Vol. 4. 2018, iss. 1. – P.42-45.
4. *Шеремет И.А.* Противодействие информационным и кибернетическим угрозам // Вестник академии военных наук. 2016. Т. 55, № 2. – С. 29-34.
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. *Калашников А.О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информация и безопасность. 2016. Т. 19, № 3. – С. 315-322.
7. *Barrett M.P.* Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 – NIST. 2018– 55p.
8. Air Force Doctrine Publication 3-60, Targeting, U.S. Air Force, 2021. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf
9. *Абдулова Е.А., Калашников А.О.* К вопросу управления рисками критической информационной инфраструктуры / Труды 14-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD-2021). – М.: ИПУ РАН, 2021. – С. 1275-1282.
10. *Сакрутина Е.А., Калашников А.О.* Анализ кибербезопасности значимого объекта критической информационной инфраструктуры / Труды 13-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2020). – М.: ИПУ РАН, 2020. – С. 1445-1452.
11. *Калашников А.О., Сакрутина Е.А*. Концепция оценки рискового потенциала энергетических объектов в системе SMS / Материалы 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2019). – М.: ИПУ РАН, 2019. – С. 850-852.
12. *Калашников А.О., Сакрутина Е.А.* Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры // Информация и безопасность. 2018. Т. 21, № 4. – С. 465-470.
13. *Harrington E.C.* The Desirability Function // Industrial Quality Control. Vol. 21. 1965, № 10. – P.494-498,