Методика технико-экономической оценки вариантов построения организационно-технической системы класса «киберполигон»

А.В. Матвеев, М.Ю. Синещук, А.В. Шестаков, Б.В. Гавкалюк

Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург

Аннотация: Статья посвящена исследованию проблемных вопросов формирования организационно-технических систем класса "киберполигонов" с применением оригинального методического аппарата технико-экономического обоснования системотехнических решений по их построению. Рассматриваются особенности существующих подходов к обоснованию системотехнических решений по построению организационно-технических систем, информационно-технических и технических систем. Предложены направления по их развитию с учетом динамики поэтапного создания и модернизации организационно-технических систем, а также возможной адаптации или конвергенции с одновременно развивающимися инфраструктурными проектами и решениями. Формальные аспекты в методическом аппарате отражаются в изменении состава функциональных компонент в концептуальных и аналитических моделях, соответствующих формальных описаний их взаимосвязей и характеристик, а также в модификации процедур технико-экономической оценки вариантов построения киберполигона.

Ключевые слова: информационная безопасность, инфраструктура, киберполигон, технико-экономическая оценка, средство защиты.

Введение

Настоящий период характеризуется неуклонным ростом киберугроз в сфере информационно-коммуникационных ресурсов. Поэтому задача специально создаваемых подразделений в различных государственных и негосударственных организациях для противодействия киберпреступности является чрезвычайно актуальной. Сфера информационной безопасности и защиты информации является динамически развивающейся областью знаний, что приводит к новым требованиям к профильным специалистам, формированию эффективной системы подготовки кадров, которые специализируются на предотвращении, выявлении и реагировании на инциденты в киберпространстве.

Для реализации практико-ориентированного подхода в подготовке специалистов целесообразно использовать киберполигон [1], который являются мультифункциональной инфраструктурой, реализующей

компьютерно-моделирующую среду для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них. Т.е. для комплексных решений по обеспечению кибербезопасности, в том числе, могут быть использованы цифровые двойники защищаемых систем в виде киберполигонов для решения задач обнаружения кибератак и реагирования на них [2, 3].

Последние годы характеризуются новым витком развития технологий, появлением новых системотехнических решений, которые могут быть интегрированы между собой, реализуя единую концепцию создаваемого интегрированного киберполигона, активное развитие получают отечественные разработки в сфере информационной безопасности и защиты информации.

В ряде исследований, проводимых ранее, рассматривались теоретические и практические вопросы создания и развития инфраструктурных проектов типа "киберполигон". Так, в работе [4], рассматривались основные подходы к созданию инфраструктуры для проведения киберучений, а также аспекты моделирования технологических процессов промышленных объектов в рамках формирования такой инфраструктуры. Авторами из Краснодарского высшего военного училища им. генерала армии С.М. Штеменко была предложена методика экспериментальной оценки уровня защищенности информационных систем от компьютерных атак на базе киберполигона [5]. В статье [6] проведен анализ современного состояния методов и инструментальных средств защиты от инсайдерских угроз, а также предложена базовая методика защиты от инсайдерских угроз. Авторами Пермского военного института

войск национальной гвардии Российской Федерации разработан лабораторный комплекс киберполигона для обучения навыкам отражения компьютерных атак специалистами информационных технологий [7]. В работе [8] обоснованы возможности использования киберполигонов в качестве оценочных средств определения фактического уровня компетенций у обучающихся в области информационной безопасности.

При этом анализ известных публикаций показывает, что к настоящему моменту в целом еще не сформированы методические средства, позволяющие научно обосновывать многокритериальные решения по выбору оптимальных или рациональных вариантов инфраструктуры создаваемого киберполигона. Таким образом, настоящее исследование посвящено решению проблемы обоснования и выбора если не оптимального, то рационального варианта формирования инфраструктуры киберполигона в условиях существующих организационно-технических, финансовых и прочих условий и ограничений.

Постановка задачи и методы исследования

Техническая и организационная инфраструктура киберполигона в общем случае должна обеспечивать выполнение следующих задач (см. Национальная программа «Цифровая экономика Российской Федерации». Федеральный проект «Информационная безопасность». URL: digital.gov.ru/ru/activity/directions/858/):

– отработка практических навыков выявления компьютерных атак, расследования инцидентов информационной безопасности, взаимодействию между подразделениями информационных технологи и информационной безопасности, внедрению превентивных мер по предупреждению компьютерных атак;

– проведение киберучений, соревнований и практических тренировок по информационной безопасности для учащихся, специалистов, экспертов и

руководителей в сфере информационных технологи и информационной безопасности;

– тестирование программного обеспечения, оборудования, элементов автоматизированных систем на реализацию функций информационной безопасности, защищенность и отсутствие уязвимостей;

– тестирование средств защиты информации на реализацию их функциональных возможностей, защищенность и наличие уязвимостей.

Следовательно, с целью формального описания киберполигона можно сформировать множество функций $f \in \{1, F\}$, реализация которых обеспечивает решение представленных выше задач и его целевое предназначение в ходе создания (развертывания), функционирования и поэтапного развития.

Тогда можно утверждать, что существует множество средств – компонентов $i \in \{1, N\}$, которые могут потенциально использоваться при построении киберполигона. Компоненты входят в состав инфраструктуры киберполигона и характеризуются вектором параметров. В рамках решаемой задачи по выбору рационального варианта построения киберполигона такими параметрами являются:

– эффективность реализации i-ым компонентом (средством) каждой f-ой функции киберполигона – $P_{f,i}$; $(0 \leq P_{f,i} \leq 1)$, $i \in \{1, N\}$;

– стоимость i-го компонента (учитывается стоимость по всему циклу его эксплуатации) – C_i, $i \in \{1, N\}$.

С учетом многовариантности обеспечения целевого предназначения киберполигона и в условиях существующих организационно-технических, финансовых и пр. ограничений ставится задача обоснования рациональной инфраструктуры киберполигона с соответствующим составом включенных в нее функциональных компонент.

Для этого необходимо провести технико-экономическое оценивание каждого из множества альтернативных вариантов инфраструктуры киберполигона, что далее позволит принять обоснованное системотехническое решение о целесообразности того или иного варианта с учетом имеющихся критериев оценки [9].

Задача выбора рационального варианта инфраструктуры киберполигона $v \in \{1, V\}$ при лимитированном объеме выделяемых ресурсов на его реализацию (C_{max}) сводится к выбору рациональной совокупности компонентов r^v, $r^v \in \{1, R\}$, входящих состав киберполигона на основе критерия «эффективность/стоимость». Также в качестве ограничительных критериев формируются заданные требуемые уровни решения каждой *f*-ой функции киберполигона – P_f^{req}.

Каждый компонент, потенциально входящий в инфраструктуру киберполигона, обеспечивает определенную степень реализации его целевого предназначения P_i (эффективность компонента в целом для решения всей совокупности задач, стоящих перед киберполигоном).

Результаты исследования и их обсуждение

Как было отмечено выше, одним из ограничений при выборе варианта киберболигона является ограничение на финансовые ресурсы, что требует оценивания стоимости совокупности компонентов, входящих в состав *v*-го варианта. Общая стоимость при данном подходе может быть определена с помощью выражения:

$$C_v = \sum_{i=1}^{r_v} C_i \ , \qquad (1)$$

где r_v – суммарное количество функциональных компонент (средств), входящих в *v*-й вариант инфраструктуры киберполигона.

Следует учитывать, что стоимость компонент (средств) в инфраструктуре киберполигона, в целом определяется не только «разовыми затратами», т.е. расходами на приобретение и развертывание средств – $C_i^{разв}$, но и должна включать затраты на техническое обслуживания и поддержание его эксплуатационных характеристик в период функционирования – $C_i^{обс}$, на обучение должностных лиц службы эксплуатации и эксплуатационного персонала – $C_i^{об}$. Таким образом:

$$C_i = \sum_{i=1}^{r_v} C_i^{разв} + \sum_{i=1}^{r_v} C_i^{обс} + \sum_{i=1}^{r_v} C_i^{об} \ . \qquad (2)$$

Выражение (2) целесообразно использовать как модель затрат при технико-экономическом оценивании альтернативных вариантов инфраструктуры киберполигона.

При сравнении альтернативных вариантов инфраструктуры киберполигона вводится показатель их технико-экономической эффективности, который выражается отношением показателя степени реализации целевого предназначения (эффективности) варианта киберполигона к объему финансовых ресурсов, необходимых на его закупку, развертывание и поддержание в работоспособном состоянии:

$$E_v = \underline{P_v} / C_v \ , \qquad (3)$$

где $\underline{P_v}$ – интегральный показатель эффективности v-го варианта инфраструктуры киберполигона.

Допущением в процедурах сравнения интегральных возможностей альтернативных инфраструктур киберполигона при выборе рационального варианта состава средств киберполигона являются одинаковые условия их использования для решения идентичного перечня задач.

Предлагается использовать специально разработанную методику технико-экономической оценки альтернативных вариантов инфраструктуры

киберполигона, единая совокупность взаимосвязанных процедур которой представлена на рис.1 и включает в себя:

– процесс формирования варианта $v \in \{1, V\}$ инфраструктуры киберполигона, включающего в себя множество r^v компонентов (средств), входящих в данный вариант;

– определение значений весовых коэффициентов «важности» каждой из функций K_f, реализуемых в создаваемом киберполигоне, на основе метода анализа иерархий [10] с использованием результатов экспертных оценок лица, принимающего решения;

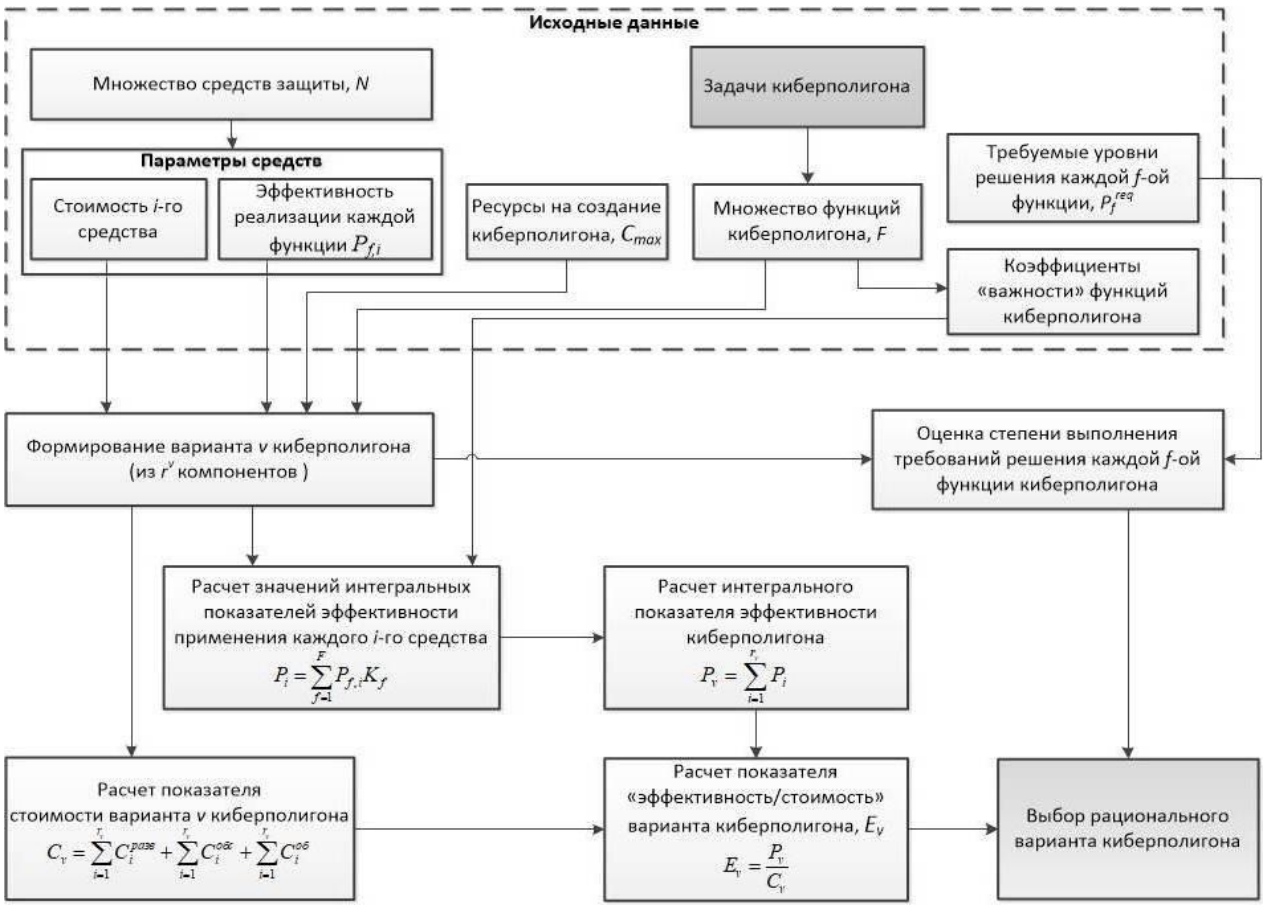

Рис. 1. – Процедуры методики технико-экономической оценки вариантов построения киберполигона

– оценка значений показателей эффективности реализации каждой *f*-ой функции каждым *i*-м средством – $P_{f,i}$;

– расчет значений интегральных показателей эффективности использования каждого *i*-го средства, входящего в состав киберполигона варианта *v*, на основе значений весовых коэффициентов «важности» каждой *f*-ой функции и значений показателей степени реализации функции данным средством $P_{f,i}$:

$$P_i = \sum_{f=1}^{F} P_{f,i} K_f \ ; \qquad (4)$$

– оценка степени выполнения требований решения каждой *f*-ой функции киберполигона;

– оценка значения интегрального показателя эффективности *v*-го варианта киберполигона P_v:

$$P_v = \sum_{i=1}^{r_v} P_i \ . \qquad (5)$$

– оценка стоимости *v*-го варианта киберполигона C_v на основе выражения (2);

– расчет показателя технико-экономической эффективности *v*-го варианта киберполигона E_v с использованием выражения (3);

– выбор рационального варианта киберполигона с учетом результатов технико-экономической оценки множества альтернативных вариантов и степени выполнения требований решения каждой функции P_f^{req}.

Таким образом, суть предложенной оригинальной методики состоит в том, что на начальном этапе определяется и выбирается конкретный тип используемого средства по каждой частной функциональной задаче, а затем формируется системотехническое решение в целом, в рамках которого определяется состав используемых средств в инфраструктуре киберполигона.

Возможны две альтернативные постановки задачи по выбору рационального варианта построения киберполигона:

1. Обеспечение максимальную возможного значения степени реализации целевого предназначения создаваемого киберполигона при имеющихся финансовых и организационно-технических ресурсах.

2. Обоснование необходимого объема финансовых средств на обеспечение требуемого уровня целевого предназначения создаваемого киберполигона.

Виды и количество используемых компонентов (средств) в создаваемой организационно-технической системе класса "киберполигон" будут определяться на основе перечня функциональных задач киберполигона, доступности (наличия на рынке услуг) средств защиты, реализующих требуемый функционал, а также размера финансовых ограничений.

Сущность предложенной оригинальной методики заключается в том, что в исходные данные процедур оценки, в качестве которых используются как стоимостные показатели средств защиты, входящих в инфраструктуру киберполигона, так и показатели степени решения каждым средством соответствующих функциональных задач, добавляются также весовые коэффициенты важности каждой из функций и требуемые уровни решения каждой функциональной задачи, что позволяет с учетом имеющихся ресурсных ограничений строить план развития с учетом динамики поэтапного создания и модернизации организационно-технических систем класса «киберполигон», а также возможной адаптации или конвергенции с одновременно развивающимися инфраструктурными проектами и решениями [11].

Заключение

Рост угроз объектам критической инфраструктуры, проявляющихся в виде кибератак, оказывает существенное влияние на национальную

безопасность [12 – 14]. Подготовка высококвалифицированных кадров с использованием практико-ориентированного подхода играет чрезвычайно важную роль в развитии защитного потенциала от угроз в киберпространстве. С помощью специально создаваемых киберполигонов оказывается возможным изучать проявления подобных угроз без ущерба реальным объектам за счет моделирования и тестирования средств защиты в управляемых виртуальных средах. Таким образом, использование киберполигонов может способствовать повышению гибкости в принятии решений и скорости реагирования на угрозы в информационном пространстве [15]. Их можно разрабатывать и использовать как на государственном, так и негосударственном уровне. При этом в настоящее время рынок средств защиты информации достаточно широк и существует задача обоснования и выбора рационального варианта формирования инфраструктуры киберполигона в условиях существующих организационно-технических, финансовых и прочих условий и ограничений.

Предложенная в данном исследовании методика технико-экономического оценки вариантов построения киберполигона позволяет ранжировать альтернативные варианты инфраструктур создаваемого киберполигона по величине показателя их технико-экономической эффективности и осуществить выбор рационального из них.

Дальнейшими направлениями исследований являются:

– совершенствование методического аппарата обоснования организационных и системотехнических решений по построению киберполигонов на основе детализации моделей обоснования подсистемы управления и информационной безопасности киберполигона, сформированной на базе образовательных ресурсов развивающихся ведомственных систем и инфраструктур, за счет ввода в эксплуатацию новых

средств защиты информации, в динамических оперативных условиях и воздействующих экономических факторов;

– развитие методологии оценки рациональности вариантов построения корпоративных информационных систем типа "киберполигон";

– технико-экономический анализ предложений на рынке киберполигонов;

– актуальные концептуальные основы создания, функционирования и развития корпоративных киберполигонов в современных условиях.

Статья подготовлена в рамках выполнения в 2023 году прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР № 123030100017-2 и № 123030100009-7 от 01.03.2023.

Литература

1. Буйневич М.В., Матвеев А.В., Смирнов А.С. Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". 2022. № 3. С. 1-17.

2. Miloslavskaya N., Tolstoy A. Cyber polygon site project in the framework of the MEPhI network security intelligence center // Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. Springer International Publishing, 2021. Pp. 295-308.

3. Ciuperca E., Stanciu A., Cîrnu C. Postmodern education and technological development. Cyber range as a tool for developing cyber security skills // INTED2021 Proceedings. IATED, 2021. Pp. 8241-8246.

4. Архангельский О.Д., Сютов Д.В., Кузнецов А.В. Практические подходы к созданию инфраструктуры индустриального киберполигона // Автоматизация в промышленности. 2020. № 11. С. 52-57. DOI: 10.25728/avtprom.2020.11.08. Сизоненко А.Б., Рудь И.С., Титарев А.О. Методика экспериментальной оценки уровня защищенности информационных систем от компьютерных атак на базе киберполигона // Электронный сетевой политематический журнал "Научные труды КубГТУ". 2022. № 6. С. 52-66.

5. Полянчико М.А. Базовая методика выявления инсайдерских угроз информационной безопасности // Национальная безопасность и стратегическое планирование. 2018. № 3(23). С. 74-77. Горячев С.Н., Михалев В.В., Кобяков Н.С., Русских В.Н. Опыт создания макета критической инфраструктуры организации // Вестник Пермского университета. Математика. Механика. Информатика. 2023. № 1(60). С. 63-69. DOI: 10.17072/1993-0550-2023-1-63-69.

6. Монахов М.Ю. Тельный А.В., Мишин Д.В. О возможностях использования киберполигонов в качестве оценочных средств определения уровня сформированности компетенций // Информационное противодействие угрозам терроризма. 2015. Т. 1, № 25. С. 269-277.

7. Матвеев А.В., Попивчак И.И. Методика технико-экономической оценки альтернативных вариантов комплексной системы безопасности потенциально опасного объекта // Фундаментальные и прикладные исследования в современном мире. 2016. № 15-1. С. 86-92.

8. Саати Т. Принятие решений Методом анализа иерархий. М.: Радио и связь, 1993. 320 с.

9. Синещук М.Ю., Шестаков А.В., Гавкалюк Б.В. Инфологическая модель и критерии качества решений по построению ведомственных организационно-технических систем класса «киберполигон» // Научно-

аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". 2023. № 1. С. 121-137.

10. Кобец П.Н. Кибертерроризм - как важнейшая угроза национальной безопасности // Национальная безопасность и стратегическое планирование. 2022. № 1(37). С. 23-28. DOI: 10.37468/2307-1400-2022-1-23-28.

11. Лапшина И.В., Першонкова Е.А. Рефлексивно управляемые кибервойны современности с позиции когнитивного моделирования // Инженерный вестник Дона. 2021. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2021/7187/.

12. Lapshina I.V., Kravets A.V. Modern cybersecurity from the perspective of cognitive modeling // Инженерный вестник Дона. 2023. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8120/.

13. Метельков А.Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. 2022. №. 1. С. 51-60.

References

1. Bujnevich M.V., Matveev A.V., Smirnov A.S. Nauchno-analiticheskij zhurnal "Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii". 2022. No. 3. pp. 1-17.

2. Miloslavskaya N., Tolstoy A. Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. Springer International Publishing, 2021. pp. 295-308.

3. Ciuperca E., Stanciu A., Cîrnu C. INTED2021 Proceedings. IATED, 2021. pp. 8241-8246.

4. Arhangel'skij O.D., Syutov D.V., Kuznecov A.V. Avtomatizaciya v promyshlennosti. 2020. No. 11. pp. 52-57. DOI: 10.25728/avtprom.2020.11.08.

5. Sizonenko A.B., Rud' I.S., Titarev A.O. Elektronnyj setevoj politematicheskij zhurnal "Nauchnye trudy KubGTU". 2022. No. 6. pp. 52-66.

6. Polyanchiko M.A Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2018. No. 3(23). pp. 74-77.

7. Goryachev S.N., Mihalev V.V., Kobyakov N.S., Russkih V.N. Vestnik Permskogo universiteta. Matematika. Mekhanika. Informatika. 2023. No. 1(60). pp. 63-69. DOI: 10.17072/1993-0550-2023-1-63-69.

8. Monahov M.YU. Tel'nyj A.V., Mishin D.V. Informacionnoe protivodejstvie ugrozam terrorizma. 2015. V. 1, No. 25. pp. 269-277.

9. Matveev A.V., Popivchak I.I. Fundamental'nye i prikladnye issledovaniya v sovremennom mire. 2016. No. 15-1. pp. 86-92.

10. Saati T. Prinyatie reshenij Metodom analiza ierarhij [Decision making by the method of analysis of hierarchies]. M.: Radio i svyaz', 1993. 320 p.

11. Sineshchuk M.YU., SHestakov A.V., Gavkalyuk B.V. Nauchno-analiticheskij zhurnal "Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii". 2023. No. 1. pp. 121-137.

12. Kobec P.N. Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2022. No. 1(37) pp. 23-28. DOI: 10.37468/2307-1400-2022-1-23-28.

13. Lapshina I.V., Pershonkova E.A. Inzhenernyj vestnik Dona. 2021. No. 9. URL: ivdon.ru/ru/magazine/archive/n9y2021/7187/.

14. Lapshina I.V., Kravets A.V. Inzhenernyj vestnik Dona. 2023. No. 1. URL: ivdon.ru/ru/magazine/archive/n1y2023/8120/.

15. Metel'kov A.N. Pravovaya informatika. 2022. No. 1. pp. 51-60.