МОДЕЛЬ СИСТЕМЫ АДАПТИВНОГО УПРАВЛЕНИЯ КИБЕРПОЛИГОНОМ МЧС РОССИИ НА ОСНОВЕ ОПЕРАТОРНОГО УРАВНЕНИЯ

Грызунов В. В.[1], Шестаков А. В.[2]

DOI: 10.21681/2311-3456-2024-6-140-149

Цель исследования: *формулировка условия существования киберполигона как организационно-технической системы, гарантированно решающей поставленные задачи.*

Методы исследования: *предложенная модель базируется на модели FIST, методах теории адаптивного управления.*

Полученные результаты: *1) показано, что киберполигон МЧС России имеет несколько треков согласно направлениям решаемых задач, является территориально распределённым, интегрируется с информационной инфраструктурой МЧС, оперирует пространственными данными, функционирует в среде всех возможных типов и проявляется в виде набора производительностей обеспечивающего уровня, уровня персонала, уровня аппаратного обеспечения и уровня программного обеспечения; 2) сформулированы ограничения, при которых возможен синтез киберполигона как системы адаптивного управления с изменяющейся архитектурой: на стабильность множества управляющих воздействий, на среднее время стабильного существования киберполигона; 3) формализовано операторное уравнение, описывающее киберполигон как организационно-техническую систему, обслуживаемую персоналом, и характеризующее условие гарантированного решения задач, стоящих перед киберполигоном; 4) обосновано введение новых элементов в структуру киберполигона: блока наблюдения и блока управления с учётом обратной связи.*

Научная новизна: *получена модель киберполигона, отличающаяся формализацией условия существования киберполигона как организационно-технической системы на всех уровнях (обеспечивающем, персонала, аппаратном, программном).*

Обсуждение: *конкретный вид формализованного в статье операторного уравнения может быть найден с помощью метода iSOFT.*

Ключевые слова: *модели управления информационной безопасностью, синтез организационно-технических систем, подготовка специалистов информационной безопасности, решения по обеспечению информационной безопасности.*

Введение

Существует тренд на повсеместное создание и применение киберполигонов, который обусловлен руководящими документами и объективной необходимостью подготовки специалистов информационной безопасности (ИБ), организации и проведения испытаний в сфере ИБ. Ориентировочная стоимость только одной аппаратно-программной части киберполигона составляет десятки миллионов рублей. При этом остаётся ряд нерешённых вопросов:

1) насколько эффективно киберполигон справляется с возложенными на него задачами;
2) какие временные, финансовые, организационные, человеческие ресурсы требуются для полноценного функционирования;
3) как киберполигон поведёт себя в условиях неопределённости и изменения объёма поставленных задач;
4) сможет ли он выдержать реальные внешние кибератаки и достигнуть поставленных целей;
5) где находятся пределы прочности киберполигона при увеличении нагрузки и другие аспекты.

Чтобы ответить на эти и другие вопросы, необходимо системно подойти к синтезу киберполигона как организационно-технической системы.

Анализ литературы

По большей части организационно-технические системы класса киберполигон строятся посредством рационального обобщения опыта противостояния киберугрозам и создания такой инфраструктуры, которая позволяет испытать и выбрать лучшие практики, а также реализовать их в нужном контексте.

В работе [1] на основе анализа более 200 источников международная группа исследователей представила статистические данные эволюции предметной области киберполигонов и их онтологий с учетом распределения сфер применения, участников, используемых методов проведения киберучений/кибертренировок и реализуемых сценариев

1 Грызунов Виталий Владимирович, доктор технических наук, доцент, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России. Санкт-Петербург, Россия. E-mail: viv1313r@mail.ru, ORCID https://orcid.org/0000-0003-4866-217X

2 Шестаков Александр Викторович, доктор технических наук, старший научный сотрудник, ведущий научный сотрудник университета Санкт-Петербургского университета ГПС МЧС России. Санкт-Петербург, Россия. E-mail: alexandr.shestakov01@yandex.ru, ORCID https://orcid.org/0000-0002-8462-6515

кибератак, архитектур построения, стеков протоколов и технологий виртуализации.

На Международном семинаре *ESORICS 2023 International Workshops* представлены материалы исследования [2] существующих зарубежных платформ для применения в качестве киберполигонов, адаптированных с учетом методов организации обучения и экспериментов, информационных инфраструктур и их топологий, а также возможного применения искусственного интеллекта для их конфигурирования под различные целевые задачи – как эволюционный путь развития платформ следующего поколения.

Подбор аналитического материала [3] по проблематике усовершенствований киберплощадок для прикладных задач киберфизических систем и информационных сетевых систем базируется на методологических рекомендациях поиска статей по определенным критериям и оценкам их качества (*PRISMA*) и анализе более чем 100 специализированных работ, на основании которых подтверждаются системные проблемы в архитектуре и инфраструктуре киберплощадок, что приводит к значительному росту нагрузки при администрировании и управлении предоставляемыми сервисами и формируемой требуемой конфигурацией.

Норвежскими специалистами в [4] рассмотрены различные аспекты разработки и оценки так называемых «неклассифицированных» киберполигонов (киберплощадок), которые в отличие от применяемых для обучения специалистов в области информационной безопасности, привития навыков и повышения знаний о новейших киберугрозах, защите от них или смягчения последствий, предназначены для непрофильной аудитории с целью повышения их киберграмотности и киберкультуры (кибергигиены), в том числе для проведения тестирования безопасности.

Исследователи Чешского Университета им. Масарика (Брно) [5] представили отчет о десятилетнем опыте использования интеллектуального анализа данных поведенческих процессов участников киберучений/кибертренировок, таких как *Capture the Flag* с применением технологий *Domain-Driven Design* для моделирования процесса подготовки специалистов на базе киберполигона с целью улучшить качество их подготовки. Вместе с тем, инфраструктурные аспекты киберполигона и проблематика организационной части остаются за рамками исследования.

В работе [6] обосновываются технические решения по созданию ведомственной организационно-технической системы класса «киберполигон» на основе анализа существующих практик создания подобных систем, зафиксированных в руководящих документах. Итоговое техническое решение выбирается экспертами с применением метода анализа иерархий. Такой подход обладает определенной долей субъективизма и предполагает некоторую статичность объекта управления с чётко заданными границами.

Исследование [7] посвящено выбору рационального варианта формирования инфраструктуры киберполигона как мультифункциональной инфраструктуры при существующих организационно-технических, финансовых и прочих ограничениях. Задача решается методом перебора всех возможных вариантов, каждый из которых характеризуется своим интегральным показателем эффективности. Предполагается: во-первых, линейность системы управления; во-вторых, фиксированные границы системы; в-третьих, относительная стабильность структуры и функций киберполигона во времени.

Вместе с тем, синтез организационно-технических систем в условиях неопределённости изучался рядом авторов достаточно давно. В некоторых работах[3] принято, что системы информационной безопасности в конкурирующих производственно-экономических структурах организационно включают в свой состав совокупность связанных единством цели элементов информационной безопасности (ИБ) на уровнях организационно-технических систем, технических систем и комплексов средств информационной безопасности. В работе упоминается, что синтез системы ИБ выполняется в условиях нечёткости и неопределённости исходных представлений о её задачах, составе, структуре и функционировании, при этом предполагаются фиксированные во времени границы системы и линейность системы управления, что является довольно сильным ограничением. По существу, сформулированная в исследовании задача решается методом последовательных приближений.

Более гибкое и менее формальное использование метода последовательных приближений для создания организационно-технических систем заложено в технологии Agile (гибкой разработки программного обеспечения), которая исследуется в работе [8], применительно к задачам формирования всестороннего организационного обеспечения вновь вводимых технологических систем компании. Авторы проинтервьюировали 52 респондента из Англии и Германии, выделили 4 модели компаний: бимодальная, полностью гибкая с межпродуктовой поддержкой, гибкая организация с проектной деятельностью, полностью гибкая организация без проектной деятельности; и 7 путей миграции компаний к полностью гибкой организации. Предлагаемый авторами подход учитывает неопределённость, с которой сталкивается

3 Мистров Л. Е. Модель синтеза систем информационной безопасности организационно-технических систем // Информационная безопасность регионов. – 2011. – №. 1. – С. 21–33

компания, и позволяет управлять изменениями компании во времени, но слабо формализован и, с точки зрения применимости к киберполигону, охватывает лишь часть киберполигона как объекта управления, в частности, только обеспечивающий уровень и уровень персонала согласно детализированной в [9] модели *FIST* (*Full Infrastructure of Sources Toolkit*), что является недостаточным для полного формирования системы.

Ещё одной группой вариантов синтеза системы управления организационно-техническими системами класса киберполигон или похожих на них путём последовательного приближения выступают технологии бизнес-моделирования: *IDEF0*, которая применена в [10] при формировании национальных систем наращивания потенциала в области кибербезопасности для стран с переходным этапом развития (*NCCBF, National Cybersecurity Capacity Building Framework*); *BPM* (*Business Process Management*), которая принята за основу в моделях жизненного цикла процессов [11] при персонализации киберучений; *UML* (*Unified Modeling Language*), применённая в [12] для представления инновационных платформенных решений обеспечения кибербезопасности на основе моделей с проверкой полученных навыков обучающихся в рабочей среде (*CYRA, CYber Range Assurance platform*) и другие.

Синтез начинается с формализации показателей эффективности результирующей системы, затем так или иначе фиксируется точка зрения на систему (специалист информационной безопасности, управленец, пользователь системы и т.д.), после чего путём достаточного количества итераций, включающих в себя опрос специалистов, синтезируются функции и, возможно, некоторые элементы системы.

Эти технологии, в целом, позволяют учесть неопределённости в объекте управления, гибко изменять алгоритмы управления, однако есть ряд существенных недостатков:

- ✓ во-первых, эффективность их применения существенно зависит от квалификации сотрудников, которые выполняют синтез;
- ✓ во-вторых, фиксированные точки зрения дают несколько, порой не вполне связных между собой моделей системы, что порождает отдельную сложную задачу интеграции этих моделей в целостную модель;
- ✓ в-третьих, переход от синтеза функций к синтезу структуры идёт интуитивно.

Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью, предложенная в [13], применяет декомпозицию на подграфы исходного графа организационного состава и структуры АСУ кибербезопасностью. При этом вопрос определения количества уровней в графе остаётся не решенным. В Методике принято, что структура и функции объекта управления и его элементов статичны.

В опубликованных работах не удалось обнаружить подходы, позволяющие найти и формализовать условие существования киберполигона как организационно-технической системы. Исключение составляет работа [14], где описывается метод *iSOFT*, позволяющий сформулировать условие[4] существование системы, заданное в виде операторного уравнения. Когда получается найти такое условие, возможно синтезировать систему, которая гарантированно решает поставленные задачи.

Целью настоящего исследования является формулировка условия существования киберполигона как организационно-технической системы.

Особенности киберполигона как объекта исследования

Под киберполигоном в настоящем исследовании понимается инфраструктура 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[5].

Следовательно, киберполигон должен за заданное время:

- ✓ во-первых, формировать навыки и умения у заданного количества специалистов ИБ;
- ✓ во-вторых, тестировать программное и аппаратное обеспечение в сфере ИБ.

Относительно ведомственного киберполигона, на примере МЧС России, конкретизация исходных данных формулируется следующим образом.

Свойства киберполигона МЧС России

Киберполигон с учетом специфики МЧС России, представляет собой не просто виртуальную среду, а единую организационно-техническую систему, состоящую из территориально-распределенных сегментов сил и средств, объединенных цифровой сетью связи, с централизованным управлением на базе образовательного учреждения МЧС России.

Ключевые особенности киберполигона для МЧС России:

4 Условие — Обстоятельство, от которого что-нибудь зависит (Ожегов С. И., Шведова Н. Ю. «Ожегов С. И. Толковый словарь русского языка: 72500 слов и 7500 фразеологических выражений» /С. И. Ожегов, Н. Ю. Шведова. – М. : Азъ, 1992. – 960 с.)

5 Постановление Правительства Российской Федерации «Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» от 12.10.2019 № 1320.

- ведомственная принадлежность: киберполигон предназначен для решения задач, связанных с обеспечением информационной безопасности МЧС России, с учетом специфики деятельности ведомства и задач единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС);
- многофункциональность: киберполигон объединяет несколько треков, каждый из которых направлен на решение определенных задач:
  - образовательный трек: предметно-ориентированное обучение и повышение квалификации специалистов по ИБ, интегрированное с электронной информационно-образовательной средой вузов МЧС России;
  - трек киберучений: организация киберучений, тренировок и соревнований для специалистов ИБ и руководителей (должностных лиц) МЧС России;
  - трек исследований и тестирования: апробация и тестирование новых технологий и средств защиты информации, исследование проблемных вопросов кибербезопасности, наполнение банка данных угроз ФСТЭК России;
- территориальная распределенность: киберполигон состоит из сегмента с функциями управления и территориальных сегментов, развернутых в различных подразделениях МЧС России;
- интеграция с информационной инфраструктурой МЧС России: киберполигон должен быть интегрирован с действующими системами (СЭД, КС АРМ ГС, ЕДДС АИУС РСЧС и т.д.), а также иметь возможность взаимодействия с внешними системами, например, ГосСОПКА;
- оперирование пространственными данными (данными о пространственных объектах и их наборах): расположение оборудования, объектов критической информационной инфраструктуры, геолокация пользователей и пр., следовательно, информационная система в основе киберполигона является геоинформационной системой[6];
- масштабируемость и развитие: киберполигон должен обеспечивать возможность поэтапного наращивания мощностей, добавления новых функций, модернизации и адаптации к новым задачам и угрозам.

Таким образом, в киберполигоне МЧС России присутствует несколько явно выраженных уровней, связанных с документальным сопровождением, работы персонала и аппаратно-программных средств, взаимодействие которых рассматривается в модели *FIST*.

Киберполигон согласно модели FIST

Киберполигон МЧС России представляет собой сложную организационно-техническую систему, включающую в себя не только программное и аппаратное обеспечение, но и персонал, пользователей, нормативно-правовые документы, финансовые потоки и другие взаимосвязанные элементы. Традиционные исследования информационной безопасности рассматривают эти элементы изолированно, упуская из виду их взаимосвязь и влияние друг на друга, что усложняет формализацию условия существования киберполигона, то есть условия, выполняя которое, киберполигон гарантированно достигает своей цели деятельности.

Модель *FIST* (*Full Infrastructure of Sources Toolkit*) [9] позволяет рассмотреть киберполигон как иерархическую систему с обеспечивающим уровнем, уровнем персонала, уровнями аппаратного и программного обеспечения (см. рис. 1).

6 ГОСТ Р 52155-2003 Географические информационные системы федеральные, региональные, муниципальные. Общие технические требования.

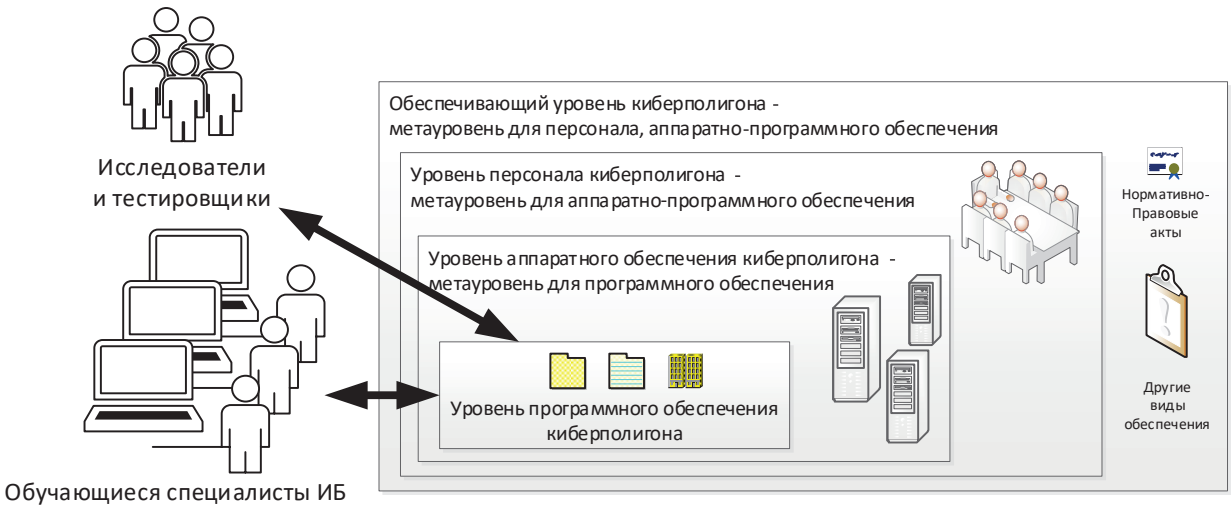

Рис. 1. Киберполигон согласно модели FIST

Метауровни задают требуемые пространственно-временные состояния вложенных уровней, например: руководящие документы формируют требования к персоналу, аппаратно-программному обеспечению; персонал настраивает и обеспечивает функционирование аппаратно-программного обеспечения; аппаратура предоставляет заданные ресурсы программному обеспечению.

От вложенных уровней в сторону метауровней идёт обратная связь, например: выбранное программное обеспечение не позволяет организовать многопользовательскую подготовку специалистов ИБ, распределённых в пространстве времени, что может потребовать применения распределённого в пространстве-времени аппаратного обеспечения, что в свою очередь изменяет требования к обслуживающему персоналу, что влечёт за собой изменения в руководящих документах или финансовом обеспечении.

Киберполигон существует на всех уровнях модели *FIST*:

- ✓ во-первых, на обеспечивающем уровне:
  - а) в виде нормативно-правового обеспечения – регламентов, политики, распоряжений и т.д.;
  - б) как система, оперирующая с финансовыми средствами;
  - в) содержит регламентированные профессиональные требования к специалистам ИБ, мотивационные и воспитательные составляющие;
- ✓ во-вторых, на уровне персонала в качестве преподавателей и вспомогательного персонала;
- ✓ в-третьих, на аппаратном уровне как оборудование, на котором развёрнуто программное обеспечение, необходимое для жизнедеятельности киберполигона;
- ✓ в-четвертых, на уровне программного обеспечения как набор специальных и общесистемных программ, с использованием которых:
  - а) осуществляется непосредственная подготовка специалистов ИБ;
  - б) выполняются действия, обеспечивающие работу киберполигона: бухгалтерия, кадры, резервное копирование и пр.

Уровни непрерывно взаимодействуют между собой и ориентированы на достижение цели деятельности всего киберполигона, и значит, система, синтезированная с использованием модели *FIST*, является целостной [14].

Множество пространственно-временных состояний киберполигона S состоит из множеств пространственно-временных состояний каждого уровня.

$$S = S^E \cup S^P \cup S^{Hard} \cup S^{Soft}, \quad (1)$$

где S^E – множество пространственно-временных состояний обеспечивающего уровня; S^P – множество пространственно-временных состояний уровня персонала; S^{Hard} – множество пространственно-временных состояний уровня аппаратного обеспечения; S^{Soft} – множество пространственно-временных состояний уровня программного обеспечения.

Пространственно-временное состояние системы – это сложившиеся отношения между элементами системы на момент времени.

Производительность киберполигона

Киберполигон предназначен для решения задач по подготовке специалистов ИБ (*e, education*) и для проведения испытаний в сфере ИБ (*test, testbeds*). Значит, можно сказать, что он обладает производительностью

$$\Omega_{CR} = \{\Omega_e, \Omega_{test}\}, \quad (2)$$

где Ω_e – производительность киберполигона по подготовке специалистов ИБ: количество специалистов в единицу времени; Ω_{test} – производительность киберполигона по проведению испытаний: количество испытаний в единицу времени.

Производительность (Ω) – количество задач $|K|$, решённое за время t:

$$\Omega = |K| / t, \quad (3)$$

где K – множество решаемых задач.

Множество задач K^*, которые должен решить киберполигон, определяется метасистемой-заказчиком, то есть задаётся извне.

Производительность всего киберполигона зависит от производительности каждого уровня киберполигона, от того, насколько элементы согласованы между собой:

$$\Omega_{CR} = F_\Omega(\Omega^E, \Omega^P, \Omega^{Hard}, \Omega^{Soft}, S, T), \quad (4)$$

где Ω^E – производительность обеспечивающего уровня: скорость разработки нормативно-правовых документов, срок действия документов, объём финансирования в единицу времени и т.д. Ω^P – производительность уровня персонала: количество задач, решаемых персоналом в единицу времени, «время жизни» персонала и т.д.; Ω^{Hard} – производительность уровня аппаратного обеспечения: *MIPS*, *FLOPS*, бод и т.д.; Ω^{Soft} – производительность уровня программного обеспечения: скорость сходимости реализованных алгоритмов, вычислительная сложность алгоритмов, ресурсоёмкость применяемых команд и т.д.; T – множество моментов времени, в которые функционирует киберполигон.

Среда функционирования киберполигона

Среда, воздействие которой обрабатывает киберполигон, имеет разную природу [15]:

- ✓ во-первых, детерминированная среда (Q_d), воздействие которой известно заранее и может быть

описано аналитически: техническое обслуживание, расписание подготовки специалистов ИБ, проведения испытаний и т.д.;

- ✓ во-вторых, стохастическая среда (Q_{st}), воздействие которой на систему выбирается из *известного множества альтернатив случайным образом при полностью известном вероятностном описании «механизма» этого выбора*: естественные сбои и отказы, поток задач, согласованных с метасистемой-заказчиком и т.д.;
- ✓ в-третьих, среда нестохастическая (Q_{nst}), то есть среда, которая не является средой Q_d и Q_{st}. Эта среда характеризуется тем, что: а) воздействие на киберполигон выбирается из известного множества альтернатив согласно некоторой цели либо отсутствуют некоторые элементы вероятностного описания «механизма» выбора; б) воздействие на киберполигон не описывается в рамках других сред: новые неучтённые ранее задачи, поставленные метасистемой-заказчиком, новая активность злоумышленников, изменения в ландшафте киберугроз и пр.

Назначение киберполигона – тренировать специалистов ИБ, которые и атакуют инфраструктуру, и защищают её. Специалисты ИБ должны иметь актуальные навыки в сфере ИБ, то есть деятельности, которая сильно и непредсказуемо изменчива.

Следовательно, киберполигон:

а) функционирует в условиях изменчивости цели управления: нужно готовить требуемое количество специалистов ИБ с актуальными знаниями, при этом требуемое количество специалистов и актуальность знаний изменчива;

б) поскольку киберполигон имеет ведомственную принадлежность с некоторой автономией на местах, то управление им будет сочетать в себе элементы и централизации, и самоорганизации;

в) архитектура киберполигона в виде совокупности структуры и протоколов взаимодействия элементов структуры между собой и со средой практически непрерывно изменяется в пространстве – времени;

г) имеет тенденцию саморазрушаться, что является штатным режимом функционирования и должно учитываться управляющей системой;

д) может подвергаться нестохастическим воздействиям внешних систем: кибератаки, резкое изменение требований к количеству и качеству подготавливаемых специалистов ИБ, появление новых угроз и т.д.

Таким образом, киберполигон представляет собой объект изменяющейся целью управления, с динамично изменяемой архитектурой, функционирующий в среде всех возможных типов, и значит, целесообразно его рассматривать как адаптивную систему управления[7].

Система управления – это сочетание управляющей системы и объекта управления[8].

Операторное уравнение, описывающее работу системы управления киберполигоном

Цель управления киберполигоном – решить множество поставленных задач K^* за заданное время t, несмотря на воздействия окружающей среды и саморазрушение киберполигона.

Следовательно, должна быть разработана система показателей, описывающая насколько киберполигон способен достичь своей цели деятельности.

Решить проблему управления – решить проблему выбора из множества альтернатив[9].

$$\{U_{\text{доп}}, S\} \longrightarrow U_{sat}, \qquad (5)$$

где $U_{\text{доп}}$ – множество допустимых управляющих воздействий; U_{sat} – множество управляющих воздействий, реализующих сатисфакционное управление киберполигоном и адаптирующих киберполигон к обработке входящих воздействий.

Киберполигон является децентрализованной системой, распределённой в пространстве-времени, следовательно, в произвольное время к киберполигону подключаются или отключаются от него сегменты с разными наборами управляющих воздействий.

Это означает, что множество допустимых управляющих воздействий $U_{\text{доп}}$ изменяется во времени.

Задача управления может быть упрощена, если потребовать неизменность $U_{\text{доп}}$. Физически неизменность реализуется разработкой соответствующих регламентов и созданием на устройствах специальной среды для решения задач киберполигона: виртуальная машина, контейнер или какой-то другой вариант виртуализации.

Ограничение 1. Множество $U_{\text{доп}}$ неизменно во все моменты времени из множества T.

В ходе адаптации необходимо определить объект управления. Это означает, что задача адаптивного управления распадается на две крупные части:

- идентификация объекта управления, то есть наблюдение;
- выбор управляющего воздействия.

Следовательно, модель киберполигона примет вид, приведенный на рис. 2.

7 Цыпкин, Я. З. Основы теории автоматических систем: учеб. пособие для вузов / Я. З. Цыпкин.– М. : Наука, 1977. – 560 с.

8 Растригин, Л. А. Адаптация сложных систем / Л. А. Растригин. – Рига: Зинатне, 1981. – 375 с.

9 Калинин, В. Н. Теоретические основы системных исследований: краткий авторский курс лекций для адъюнктов академии / В. Н. Калинин. – СПб.: ВКА им. А. Ф. Можайского, 2011. – 278 с.

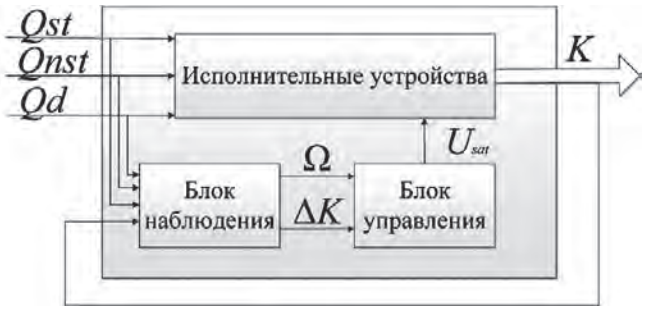

Рис. 2. Модель киберполигона с блоком наблюдения и управления

Согласно предложенной модели, наблюдение за киберполигоном и управление киберполигоном реализуются через производительности. Интегральная производительность формируется через оптимизацию структуры киберполигона и оптимизацию процессов выполнения задач.

Таким образом, проблема адаптации киберполигона к обработке входящих воздействий формулируется так.

Дано:

T – множество моментов времени, когда функционирует киберполигон;

$Q = \{Q_d, Q_{st}, Q_{nst}\}$ – множество входных ситуаций;

$\Omega_{CR} = F_\Omega\ (\Omega^E, \Omega^P, \Omega^{Hard}, \Omega^{Soft}, S, T)$ – производительность киберполигона;

$K^* = \cup_{i=1}^{|K^*|} k_i,\ k_i = \langle \Omega^*_{CR,i}, t_i^* \rangle$ – множество поставленных задач;

t_i^* – требуемое время решения i-ой задачи;

$\Omega^*_{CR,i}$ – производительность киберполигона, которая требуется i-ой задаче;

$U_{\text{доп}}$ – множество управляющих воздействий.

Ограничение 2. $t_i \ll \tau,\ \forall i = \overline{(1,|K^*|)}$, τ – среднее время стабильного существования киберполигона.

Требуется:

При фиксированном $U_{\text{доп}}$ найти такое управляющее воздействие $U_{sat} \subset U_{\text{доп}}$, которое позволит решить все задачи, поставленные перед киберполигоном за заданное время, то есть найти оператор:

$$R_U\,(\Omega_{CR}, Q, U_{sat}, T) = K^*. \qquad (5)$$

Операторное уравнение (5) является моделью системы адаптивного управления киберполигоном и реализует условие адаптации киберполигона к обработке входящих воздействий, то есть условие гарантированного решения киберполигоном поставленных задач. При создании уравнения используются все возможные субстанциальные закономерности киберполигона, то есть закономерности, которые влияют на достижение системой цели её деятельности [14].

Решение операторного уравнения (5) представляет собой вариационную задачу, так одно уравнение содержит несколько переменных.

Из представленной модели следует, что множество задач K, которые решает киберполигон, может не совпадать со множеством задач K^*, поставленных метасистемой-заказчиком перед киберполигоном. Так происходит в следующих случаях:

1) киберполигон решает меньше задач, чем поставили, потому что не справляется с нагрузкой в силу резкого увеличения задач или своего разрушения из-за кибератак или в ходе эксплуатации;
2) киберполигон решает задачи злоумышленников.

Пример применения разработанной модели

Без нарушения общности предположим, что перед киберполигоном стоит задача повышать квалификацию 10 специалистам ИБ в месяц:

$\Omega_{CR} = \Omega_e$ = 10 специалистов в месяц на протяжении года.

Киберполигон функционирует T = 1 год = 12 месяцев.

k^* – подготовить 10 специалистов ИБ.

$|K^*|$ = 12, так как всего 12 задач (10 специалистов каждый месяц на протяжении года).

$K^* = \cup_{i=1}^{12} k_i,\ k_i = \langle \Omega^*_{CR,i} = 10,\ t_i^* = 1 \rangle$.

Q_{st} = равномерное появление 14±5 специалистов ИБ в месяц желающих повысить свою квалификации.

Q_{nst} = текущая ситуация в сфере ИБ, которая влияет на формирование перечня требований к специалисту ИБ. Может изменяться раз в неделю.

Исходя из условий примера, можно сказать, что:

1) киберполигон должен содержать какой-то элемент, который преобразует стохастическую величину на входе Q_{st} в детерминированную Ω_{CR} на выходе, например, за счёт управления количеством обучающихся в группе;
2) полностью формировать перечень требований к специалистам ИБ на уровне руководства МЧС нецелесообразно, потому что текущая ситуация в сфере ИБ Q_{nst}, влияющая на формирование требований, изменяется раз в неделю, что гораздо быстрее, чем формируются и утверждаются документы в МЧС (больше года, то есть 52 недели). Следовательно, частично требования к специалисту ИБ необходимо формировать в ходе самого обучения;
3) среднее время стабильного существования киберполигона должно быть много больше одного месяца.

Конкретный вид оператора (5) и его составляющих определяется на стадиях создания автоматизированных систем 4 «Эскизный проект» и 5 «Технический проект»[10] и реализуется методом *iSOFT* [14]. Этому посвящены последующие работы.

10 ГОСТ Р 59793-2021. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

Поскольку оператор строится с использованием всех субстанциальных закономерностей [14], то пригодность и адекватность модели обеспечивается полнотой учёта закономерностей.

Выводы

Фактически представленные материалы конкретизируют базовые мероприятия стадии 2 «Разработка концепции автоматизированной системы» при создании автоматизированной системы.

В статье сформулированы два ограничения, при которых должна решаться задача синтеза системы управления киберполигоном.

Предлагаемая в виде операторного уравнения модель киберполигона как организационно-технической системы в отличие от существующих моделей *формализует условие гарантированного решения поставленных киберполигоном задач*, связывает все уровни киберполигона, выдвигает требование ко времени стабильного существования киберполигона и позволяет выявить необходимость:

- ✓ во-первых, рассмотрения киберполигона как адаптивной системы управления с изменяющейся архитектурой на всех уровнях, учитывающей возможность изменения цели деятельности;
- ✓ во-вторых, присутствия блока наблюдения и формирования обратной связи;
- ✓ в-третьих, формирования множества допустимых управляющих воздействий, фиксированных на весь период существования киберполигона;
- ✓ в-четвертых, разработки иерархии показателей оценивания достижения киберполигоном цели деятельности;
- ✓ в-пятых, поиска конкретного вида операторного уравнения (5) и его сатисфакционного решения.

Разработанная модель может применяться на всех этапах жизненного цикла киберполигона: от разработки до утилизации.

Литература

1. *Ukwandu, E. et al. A review of cyber-ranges and test-beds: Current and future trends // Sensors. – 2020. – v. 20(24). – №. 24. – P. 7148. DOI:10.3390/s20247148.*
2. *Grimaldi, A. et al. Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms / In book: Computer Security. ESORICS 2023 International Workshops. Pp.271–290. DOI:10.1007/978-3-031-54129-2_16.*
3. *Stamatopoulos, D. et al. Exploring the Architectural Composition of Cyber Ranges: A Systematic Review // Future Internet, 16(7), June 2024. – P.16. DOI:10.3390/fi16070231.*
4. *Yamin, M., Katt, B., Gkioulos, V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture // Computers & Security. – October 2019. – v. 88. – P. 101636. DOI:10.1016/j.cose.2019.101636.*
5. *Macák, M., Oslejsek, R., Buhnova, B. Applying process discovery to cybersecurity training: an experience report // 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2022. – Pp. 394–402. DOI:10.1109/EuroSPW55150.2022.00047.*
6. *Синещук М. Ю. Технические решения по созданию ведомственных организационно-технических систем класса «киберполигон» как средства обеспечения информационной безопасности ведомственного назначения // Научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России». 2024. №.1. С. 179–200. DOI: https://doi.org/10.61260/2218-130X-2024-1-179-20.*
7. *Матвеев А. В., Синещук М. Ю., Шестаков А. В., Гавкалюк Б. В. Методика технико-экономической оценки вариантов построения организационно-технической системы класса «киберполигон» // Инженерный вестник Дона. – 2023. – №. 6 (102). – С. 187–200.*
8. *Gerster, D. et al. How Enterprises Adopt Agile Forms of Organizational Design: A Multiple-Case Study //ACM SIGMIS Database: the DATABASE for Advances in Information Systems. – 2020. – v. 51. – №. 1. – Pp. 84–103. DOI:10.1145/3380799.3380807.*
9. *Грызунов В. В. Модель геоинформационной системы FIST, использующей туманные вычисления в условиях дестабилизации // Вестник Дагестанского государственного технического университета. Технические науки. 2021. Т. 48. №. 1. С. 76–89. DOI: 10.21822/2073-6185-2021-48-1-76-89.*
10. *Naseir, M. A. B. National cybersecurity capacity building framework for counties in a transitional phase : Doctoral Thesis (Doctoral). – Bournemouth University. 2020.*
11. *Pfaller, T. et al. Towards Customized Cyber Exercises using a Process-based Lifecycle Model // EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference: Association for Computing Machinery (ACM), New York, pp. 37–45.*
12. *Smyrlis, M. et al. CYRA: A Model-Driven CYber Range Assurance Platform // Applied Sciences. – 2021. – v. 11. – №. 11. – P. 5165. DOI:10.3390/app11115165/.*
13. *Селифанов В. В., Мещеряков Р. В. Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – №. 1. – С. 39-40. DOI: 10.26102/2310-6018/2020.28.1.001.*
14. *Грызунов В. В. Формирование условия гарантированного достижения цели деятельности информационной системой на базе операторного уравнения // Информатизация и связь. – 2022. – № 4. – С. 67–74. – DOI 10.34219/2078-8320-2022-13-4-67-74.*
15. *Burlov, V. G., Gryzunov, V. V., Tatarnikova, T. M. Threats of information security in the application of GIS in the interests of the digital economy // Journal of Physics: Conference Series : 23 (St. Petersburg, 27–29.05.2020). – St. Petersburg : IOP Publishing Ltd, 2020. – P. 012023. – DOI: 10.1088/1742-6596/1703/1/012023.*
16. *Грызунов, В. В. Концептуальная модель адаптивного управления геоинформационной системой в условиях дестабилизации // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 1. – С. 102–108. – EDN GVCRHF.*

MODEL OF THE ADAPTIVE CONTROL SYSTEM OF THE CYBER RANGE OF THE RUSSIAN EMERGENCIES MINISTRY BASED ON THE OPERATOR EQUATION

Gryzunov V. V.[11], Shestakov A. V.[12]

The purpose of the research *is to formulate the conditions for the existence of a cyber range as an organizational and technical system that is guaranteed to solve the tasks.*

Research methods: *the proposed model is based on the FIST model, methods of the theory of adaptive control.*

Results: *1) it is shown that the cyber range of the Ministry of Emergency Situations of Russia has several tracks according to the areas of the tasks to be solved, is geographically distributed, integrates with the information infrastructure of the Ministry of Emergency Situations, operates with spatial data, functions in an environment of all possible types and manifests itself in the form of a set of performance levels of the supporting level, the level of personnel, the level of hardware and the level of software; 2) the limitations under which it is possible to synthesize a cyber range as an adaptive control system with a changing architecture are formulated: on the stability of a set of control actions, on the average time of stable existence of a cyber range; 3) the operator equation describing the cyber range as an organizational and technical system maintained by personnel and characterizing the condition for the guaranteed solution of the tasks facing the cyber range has been formalized; 4) the introduction of new elements into the structure of the cyber range is substantiated: an observation unit and a control unit taking into account feedback.*

Scientific novelty: *the author provides a model of a cyber range, which is distinguished by the formalization of the conditions for the existence of a cyber range as an organizational and technical system at all levels (support, personnel, hardware, software).*

Discussion: *A specific kind of operator equation formalized in the paper can be found using the iSOFT method.*

Keywords: *information security management models, synthesis of organizational and technical systems, training of information security specialists, information security solutions.*

References

1. *Ukwandu, E. et al. A review of cyber-ranges and test-beds: Current and future trends // Sensors. – 2020. – v. 20(24). – №. 24. – P. 7148. DOI:10.3390/s20247148.*
2. *Grimaldi, A. et al. Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms / In book: Computer Security. ESORICS 2023 International Workshops. Pp.271–290. DOI:10.1007/978-3-031-54129-2_16.*
3. *Stamatopoulos, D. et al. Exploring the Architectural Composition of Cyber Ranges: A Systematic Review // Future Internet, 16(7), June 2024. – R.16. DOI:10.3390/fi16070231.*
4. *Yamin, M., Katt, B., Gkioulos, V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture // Computers & Security. – October 2019. – v. 88. – P. 101636. DOI:10.1016/j.cose.2019.101636.*
5. *Macák, M., Oslejsek, R., Buhnova, B. Applying process discovery to cybersecurity training: an experience report //2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2022. – Pp. 394–402. DOI:10.1109/EuroSPW55150.2022.00047.*
6. *Sineshhuk M. Ju. Tehnicheskie reshenija po sozdaniju vedomstvennyh organizacionno-tehnicheskih sistem klassa «kiberpoligon» kak sredstva obespechenija informacionnoj bezopasnosti vedomstvennogo naznachenija // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii». 2024. №.1. S. 179–200. DOI: https://doi.org/10.61260/2218-130X-2024-1-179-20.*
7. *Matveev A. V., Sineshhuk M. Ju., Shestakov A. V., Gavkaljuk B. V. Metodika tehniko-jekonomicheskoj ocenki variantov postroenija organizacionno-tehnicheskoj sistemy klassa «kiberpoligon» // Inzhenernyj vestnik Dona. – 2023. – №. 6 (102). – S. 187–200.*
8. *Gerster, D. et al. How Enterprises Adopt Agile Forms of Organizational Design: A Multiple-Case Study //ACM SIGMIS Database: the DATABASE for Advances in Information Systems. – 2020. – v. 51. – №. 1. – Pp. 84–103. DOI:10.1145/3380799.3380807.*
9. *Gryzunov V. V. Model' geoinformacionnoj sistemy FIST, ispol'zujushhej tumannye vychislenija v uslovijah destabilizacii // Vestnik Dagestanskogo gosudarstvennogo tehnicheskogo universiteta. Tehnicheskie nauki. 2021. T. 48. №. 1. S. 76–89. DOI: 10.21822/2073-6185-2021-48-1-76-89.*
10. *Naseir, M. A. B. National cybersecurity capacity building framework for counties in a transitional phase : Doctoral Thesis (Doctoral). – Bournemouth University. 2020.*

11 Vitaliy V. Gryzunov, Dr.Sc., Associate Professor, professor of department of applied mathematics and information technologies, St. Petersburg University of State Fire Service of EMERCOM of Russia, E-mail: viv1313r@mail.ru, ORCID https://orcid.org/0000-0003-4866-217X

12 Alexander V. Shestakov, Dr.Sc., senior researcher, leading researcher, St. Petersburg University of State Fire Service of EMERCOM of Russia. E-mail: alexandr.shestakov01@yandex.ru, ORCID https://orcid.org/0000-0002-8462-6515

11. Pfaller, T. et al. Towards Customized Cyber Exercises using a Process-based Lifecycle Model // EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference: Association for Computing Machinery (ACM), New York, pp. 37–45.
12. Smyrlis, M. et al. CYRA: A Model-Driven CYber Range Assurance Platform //Applied Sciences. – 2021. – v. 11. – №. 11. – P. 5165. DOI:10.3390/app11115165/.
13. Selifanov V. V., Meshherjakov R. V. Metodika formirovanija dopustimyh variantov organizacionnogo sostava i struktury avtomatizirovannoj sistemy upravlenija informacionnoj bezopasnost'ju //Modelirovanie, optimizacija i informacionnye tehnologii. – 2020. – T. 8. – №. 1. – S. 39-40. DOI: 10.26102/2310-6018/2020.28.1.001.
14. Gryzunov V. V. Formirovanie uslovija garantirovannogo dostizhenija celi dejatel'nosti informacionnoj sistemoj na baze operatornogo uravnenija // Informatizacija i svjaz'. – 2022. – № 4. – S. 67–74. – DOI 10.34219/2078-8320-2022-13-4-67-74.
15. Burlov, V. G., Gryzunov, V. V., Tatarnikova, T. M. Threats of information security in the application of GIS in the interests of the digital economy // Journal of Physics: Conference Series : 23 (St. Petersburg, 27–29.05.2020). – St. Petersburg : IOP Publishing Ltd, 2020. – P. 012023. – DOI: 10.1088/1742-6596/1703/1/012023.
16. Gryzunov, V. V. Konceptual'naja model' adaptivnogo upravlenija geoinformacionnoj sistemoj v uslovijah destabilizacii / V. V. Gryzunov // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. – 2021. – № 1. – S. 102–108. – EDN GVCRHF.