Научная статья
УДК 004.519; DOI: 10.61260/2218-13X-2024-1-179-200

ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО СОЗДАНИЮ ВЕДОМСТВЕННЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ КЛАССА «КИБЕРПОЛИГОН» КАК СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕДОМСТВЕННОГО НАЗНАЧЕНИЯ

✉**Синещук Максим Юрьевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***smaxim@igps.ru***

Аннотация. Статья посвящена исследованию проблемных вопросов формирования ведомственных организационно-технических систем класса «киберполигон» как решение задачи управления в организационных системах на основе интегрирующей платформы в виде управляющего конфигуратора, который должен обеспечить необходимый уровень готовности киберполигона в условиях изменения в ведомственных системах обеспечения информационной безопасности применяемых технологий. Рассмотрен подход к обоснованию возможности обеспечения интегрирующей платформой необходимого (требуемого) уровня готовности организационно-технической системы класса «киберполигон» с учетом дефицита уровня готовности технологий функциональных модулей киберполигона. Приведены результаты сравнительной оценки уровня техники управляющего конфигуратора и решений, которые зарегистрированы в Российской Федерации как объекты промышленной и интеллектуальной собственности.

Ключевые слова: киберполигон, конфигуратор киберполигона, уровень готовности технологии, уровень готовности интеграции, уровень готовности системы

Для цитирования: Синещук М.Ю. Технические решения по созданию ведомственных организационно-технических систем класса «киберполигон» как средства обеспечения информационной безопасности ведомственного назначения // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 1. С. 179–200. DOI: 10.61260/2218-13X-2024-1-179-200.

Scientific article

TECHNICAL SOLUTIONS FOR THE CREATION OF DEPARTMENTAL ORGANIZATIONAL AND TECHNICAL SYSTEMS OF THE «CYBERPOLYGON» CLASS AS A MEANS OF ENSURING INFORMATION SECURITY FOR DEPARTMENTAL PURPOSES

✉**Sineshchuk Maxim Yu.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***smaxim@igps.ru***

Abstract. The article is devoted to the study of problematic issues of the formation of departmental organizational and technical systems of the «cyberpolygon» class as a solution to the problem of management in organizational systems based on an integrating platform in the form of a control configurator, which should ensure the necessary level of readiness of the cyberpolygon in the context of changes in the technologies used in departmental information security systems. An approach is considered to substantiate the possibility of providing the necessary (required) level of readiness of the organizational and technical system of the «cyberpolygon» class of the integrating platform, taking into account the shortage of the level of readiness of the technology of the functional modules of the cyberpolygon. The results of a comparative assessment

of the state of the art of the control configurator and solutions that are registered in the Russian Federation as objects of industrial and intellectual property are presented.

Keywords: cyberpolygon, cyberpolygon configurator, technology readiness level, integration readiness level, system readiness level

For citation: Sineshchuk M.Yu. Technical solutions for the creation of departmental organizational and technical systems of the «cyberpolygon» class as a means of ensuring information security for departmental purposes // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 1. P. 179–200. DOI: 10.61260/2218-13X-2024-1-179-200.

Введение

Актуальность исследований и результатов решения задачи повышения эффективности ведомственных систем обеспечения информационной безопасности (СОИБ) несомненна. Научно-практическая значимость затронутой проблематики в сфере информационной безопасности (ИБ) и защиты информации (ЗИ) обусловлена:

– доктринальными требованиями (например, Доктрина информационной безопасности Российской Федерации (2016) [1]; Стратегии национальной безопасности Российской Федерации до 2030 года) [2];

– отечественными нормами права (например, дополнительные меры по обеспечению информационной безопасности (2022) [3], меры технологической независимости и безопасности критической информационной инфраструктуры (2022) [4]);

– постоянно развивающимся законодательством государственного управления различного уровня (например, изменения в Федеральный закон « О безопасности критической информационной инфраструктуры» (2023) [5], О прекращении применения отдельных средств защиты информации (2023) [6], Требования к СУБД (2023) [7], Об организации процессов управления уязвимостями (2023) [8]), в том числе ведомственного (например, Об организации парольной защиты информационных ресурсов (2020) [9], Об определении угроз безопасности персональных данных в МЧС России (2022) [10]).

Доктринальными документами определен базовый терминологический аппарат, в частности:

– «информационная безопасность» – как «состояние защищенности субъекта от внутренних и внешних информационных угроз»;

– «обеспечение информационной безопасности» – как «осуществление различных мер применительно к информационным угрозам и последствиям их проявления»;

– «система обеспечения информационной безопасности» – как «совокупность сил (уполномоченных органов, подразделений и должностных лиц) и средств (правовые, организационные, технические и др.) решения задач по обеспечению ИБ».

Процессный подход описания управления, применительно к ведомственной СОИБ, регламентированный ФСТЭК России для задач управления уязвимостями в органе (организации), представлен данными табл. 1 распределения обязательных операций соответствующего процесса управления по должностным лицам (ДЛ), выполняющим профессиональную деятельность по вопросам устранения уязвимостей в различных структурных подразделениях и в виде схемы управления уязвимостями в организационной системе (рис. 1).

Таблица 1

Распределение обязательных операций процесса управления по устранению уязвимостей

Этапы, операции (задачи)	Функции ДЛ в подразделениях					
	ЗИ				ИТ	
	Р	А	С1	С2	Р	С3
1. Мониторинг уязвимостей и оценка их применимости						
1.1. Анализ информации об уязвимостях	О	И				
1.2. Оценка применимости уязвимости	О	И				
1.3. Принятие решений на получение дополнительной информации		О/И				

1.4. Постановка задачи на сканирование объектов	О/И					
1.5. Сканирование объектов	О		И			
1.6. Оценка защищенности	О		И			
2. Оценка уязвимостей						
2.1. Получение информации об объектах, подверженных уязвимости		О/И				
2.2. Определение уровня опасности		О/И				
2.3. Определение влияния на информационные системы		О/И				
2.4. Расчет критичности уязвимости	О	И				
3. Определение методов и приоритетов устранения уязвимостей						
3.1. Определение приоритетности устранения уязвимостей	О	И				
3.2. Определение методов устранения уязвимостей	О	И				
3.3. Принятие решения о срочной установке обновлений	О/И					
3.4. Создание заявки на срочную установку обновления	О/И					
3.5. Создание задания на установку обновлений		О/И				
3.6. Принятие решения о срочной реализации компенсирующих мер	О/И					
3.7. Создание задания на реализацию компенсирующих мер ЗИ		О/И				
4. Устранение уязвимостей						
4.1. Согласование установки с руководством подразделения ИТ	О/И				У	
4.2. Тестирование обновления					О	И
4.3. Установка обновления в тестовом сегменте					О	И
4.4. Принятие решения об установке обновления					О/И	
4.5. Установка обновления					О	И
4.6. Формирование плана установки обновлений					О/И	
4.7. Разработка и реализация компенсирующих мер ЗИ	О	И		И		У
5. Разработка и реализация компенсирующих мер ЗИ						
5.1. Определение мер ЗИ и ответственных за их реализацию	О/И	И				
5.2. Согласование привлечения работников	О/И				У	
5.3. Реализация организационных мер ЗИ	О/И				У	
5.4. Настройка средств ЗИ	О			И		У
5.5. Организация анализа событий безопасности	О			И		
5.6. Внесение изменений в ИТ-инфраструктуру		У			О	И
6. Контроль устранения уязвимостей						
6.1. Принятие решения о способе контроля	О/И					
6.2. Проверка объектов на наличие уязвимостей	О		И			
6.3. Оценка защищенности	О		И			
6.4. Выявление отклонений и неисполнений	О		И			
6.5. Предложения по улучшению управления уязвимостями	О	И			У	
7. Разработка предложений по улучшению процесса управления уязвимостями						
7.1. Определение причин отклонений и (или) неисполнений	О/И					
7.2. Корректировка механизмов мониторинга	О	И				
7.3. Добавление источника сведений об уязвимостях	О	И				
7.4. Корректировка механизмов оценки уязвимостей	О	И				
7.5. Согласование сроков устранения уязвимости	О/И				У	
7.6. Создание заявки на реализацию компенсирующих мер	О	И				

Примечание: Р – руководитель; А – аналитик угроз; С1 – специалист по проведению оценки защищенности; С2 – специалист по внедрению средств защиты информации; С3 – специалист; О – ответственный, должностное лицо, ответственное за завершение выполнения задачи; И – исполнитель, должностное лицо, непосредственно выполняющее задачу; У – участник, должностное лицо, участие которого требуется для выполнения задачи; ЗИ – защита информации; ИТ – информационная технология

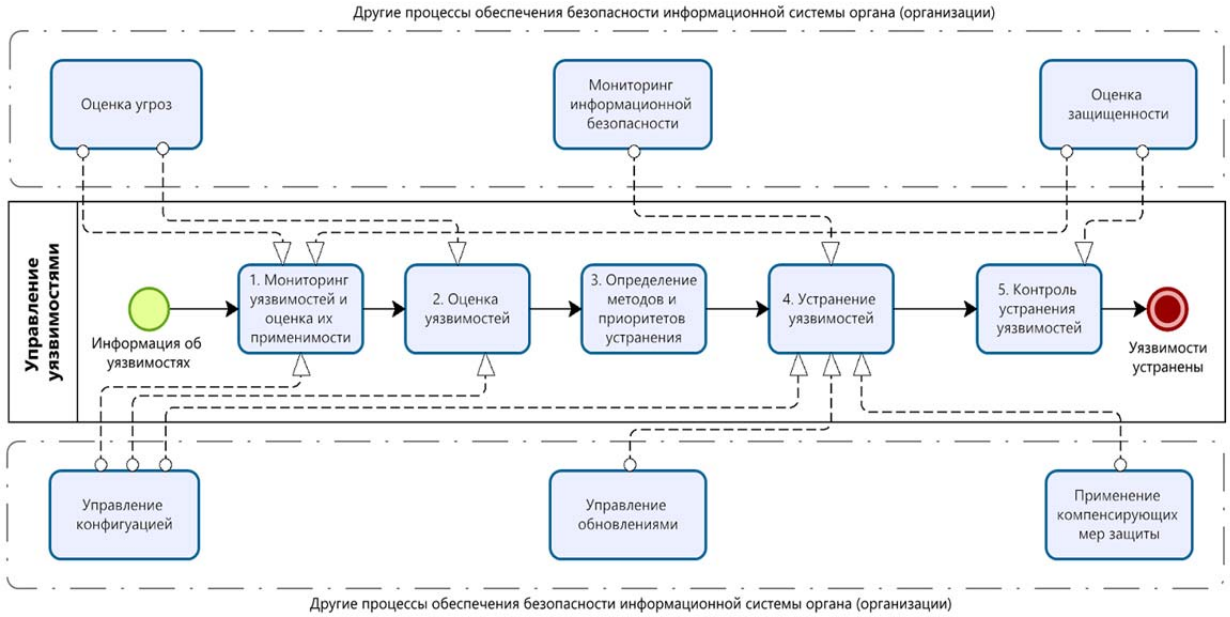

Рис. 1. **Схема управления уязвимостями информационной инфраструктуры (ИИ) в организационной системе**

Требования к временным характеристикам реализации процедур процессов управления существенно отличаются по типам регламентированной организации процессов, которые в качестве примера представлены схемами процессов этапа 4 «Устранения уязвимостей» и подпроцесса «Разработки и реализации компенсирующих мер защиты информации» этапа 4 «Устранения уязвимостей» – на рис. 2, 3 соответственно [11].

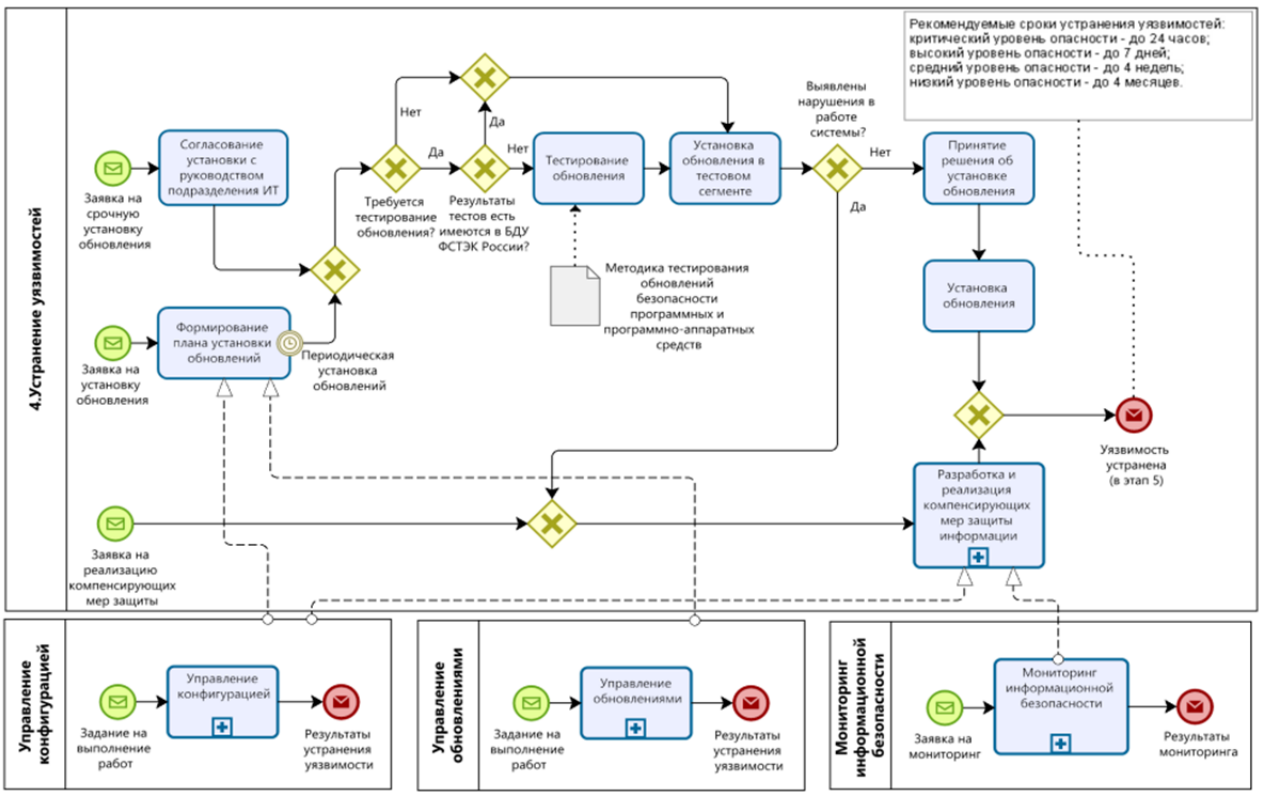

Рис. 2. **Схема операций этапа 4 «Устранения уязвимостей» ИИ в организационной системе**

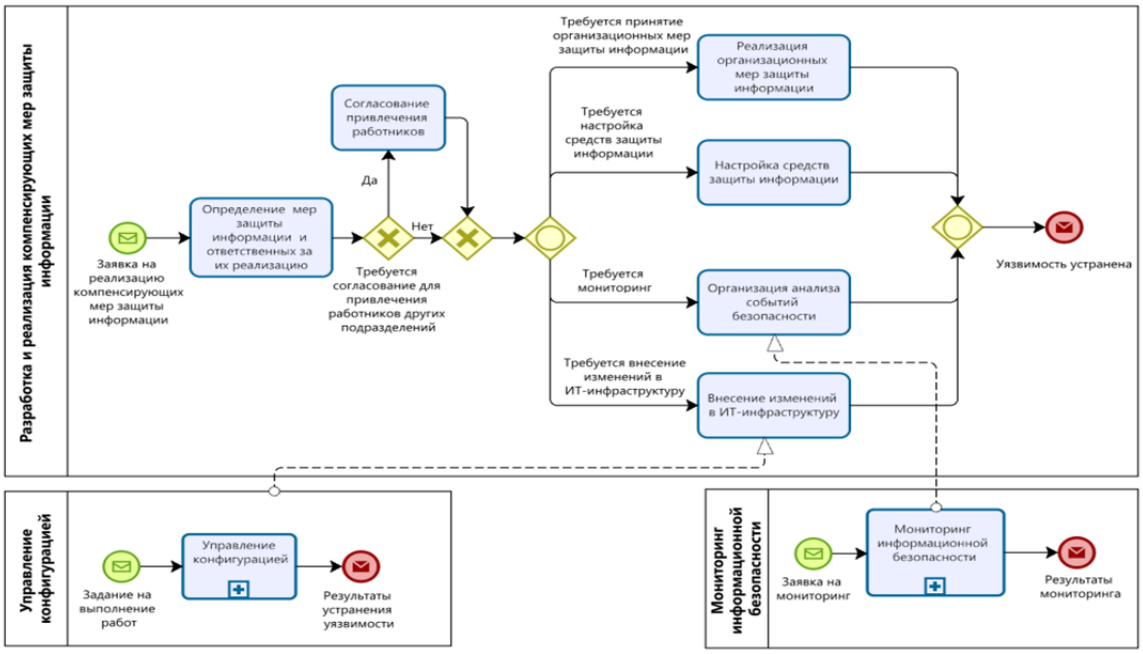

Рис. 3. **Схема подпроцесса «Разработка и реализация компенсирующих мер защиты информации» на этапе 4 «Устранения уязвимостей»**

Результаты анализа основных процессов управления обеспечением ИБ, представленных на рис. 1 и данных табл. 1 о перечне работ и привлекаемых силах подразделений, указывают:

– на необходимость наличия высокого уровня осведомленности и компетентности в области ИБ и ЗИ должностных лиц как подразделений ЗИ, так и ИТ-подразделений организации;

– на востребованность в применении дополнительного ресурса сил и средств для выработки вариантов действий в условиях ограниченного времени на принятие решений в нештатных ситуациях или в качестве резервного (дублирующего) компонента сил и средств для задач обеспечения стабильного функционирования процессов управления ИБ организации, например, пункты 4.2–4.7 этапа 4 «Устранение уязвимостей», пункты 5.1–5.6 этапа 5 «Разработка и реализация компенсирующих мер защиты информации», пункты 6.1–6.5 этапа 6 «Контроль устранения уязвимостей», пункты 7.1, 7.4–7.6 этапа 7 «Разработка предложений по улучшению процесса управления уязвимостями».

Выявленные факторы и условия обусловливают потребность введения в контур СОИБ дополнительных сервисов организационно-технических систем (ОТС) нового класса [12].

Критические элементы технологий ОТС класса «киберполигон»

ОТС нового класса и их сервисы должны обеспечить:

– дополнительную поддержку принятия решений в ведомственных СОИБ;

– снижение дефицита профессиональных компетенций ДЛ в области ИБ и ЗИ.

Для решения подобного класса задач достаточно проработанной является концепция ОТС класса «киберполигон» [13].

Киберполигон представляет собой единую централизованную ОТС в составе территориально-распределенных сегментов сил и средств, с сегментом управления на базе образовательного учреждения, уполномоченного по вопросам создания, развития и функционирования киберполигона и его интегрированного применения в иерархической структуре ведомственной СОИБ, как изображено на рис. 4, перечень сервисов треков которой (кибертренировок (киберучений), ТК; образовательный, ТО; испытательный, ТИ) представлен в табл. 2.

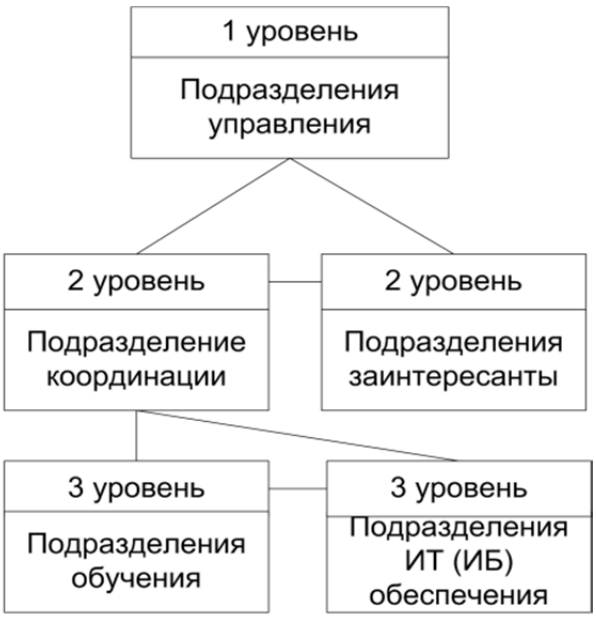

Рис. 4. **Организационная архитектура системы повышения уровня осведомленности персонала**

Таблица 2

Перечень сервисов треков киберполигона

Трек кибертренировок (киберучений), ТК	Трек образовательный, ТО	Трек испытательный, ТИ
1. Сервисы профориентированного образования по направлению ИБ и ЗИ с применением компьютерно-моделирующей среды прототипов и цифровых двойников реальных фрагментов корпоративной ИИ		1. Сервисы исследования проблемных аспектов кибербезопасности ведомственной инфраструктуры
2. Сервисы формирования групповых компентенций сил обеспечения ИБ	2. Сервисы формирования, апробации и внедрения новых дидактических методов с применением территориально-распределенных средств киберполигона и виртуальных сред	2. Сервисы формирования документов методического и организационного обеспечения ИБ ведомственной инфраструктуры
3. Сервисы формирования и регламентированного функционирования проактивной киберсреды информационной поддержки в корпоративной системе управления ИБ по проблемам текущей деятельности профильных подразделений и организаций, программно-целевого развития единого информационного пространства корпоративной проактивной киберсреды		3. Сервисы технической поддержки компонент ведомственной системы обеспечения ИБ
4. Сервисы сбора, обработки и предоставления сведений подразделениям о выявлении в треке киберполигона новых инцидентов по результатам мониторинга инцидентов в области ИТ и ИБ, реагирования на инциденты ИБ		
5. Сервисы выработки научно-обоснованных предложений для лиц, ответственных за реализацию политики ИБ, взаимосвязанных и согласованных мер киберзащиты организационного и технического характера		
–	6. Сервисы поддержки в актуальном состоянии информации об информационных ресурсах и ИИ корпоративных территориально-распределенных фрагментах киберполигона	

Создаваемые и отрабатываемые в киберполигоне шаблоны ИИ и СОИБ являются прообразами ведомственной ИИ и СОИБ, которые обеспечивают функционирование бизнес-процессов ведомства, его территориальных органов управления, подразделений и организаций.

Существующие прототипы киберполигонов имеют различную архитектуру, как показано на рис. 5, 6, которая зависит от его назначения и перечня предоставляемых сервисов реализованных трактов. Архитектуру прототипов киберполигона, реализующих основные принципы их проектирования [14], можно представить в виде обобщенной схемы (рис. 7). Однако, согласно результатам концептуальной проработки киберполигона, предлагается его архитектуру отобразить в виде базовой (рис. 8).

Рис. 5. **Архитектура киберполигона: подход Ростелеком (источник: https://www.tadviser.ru)**

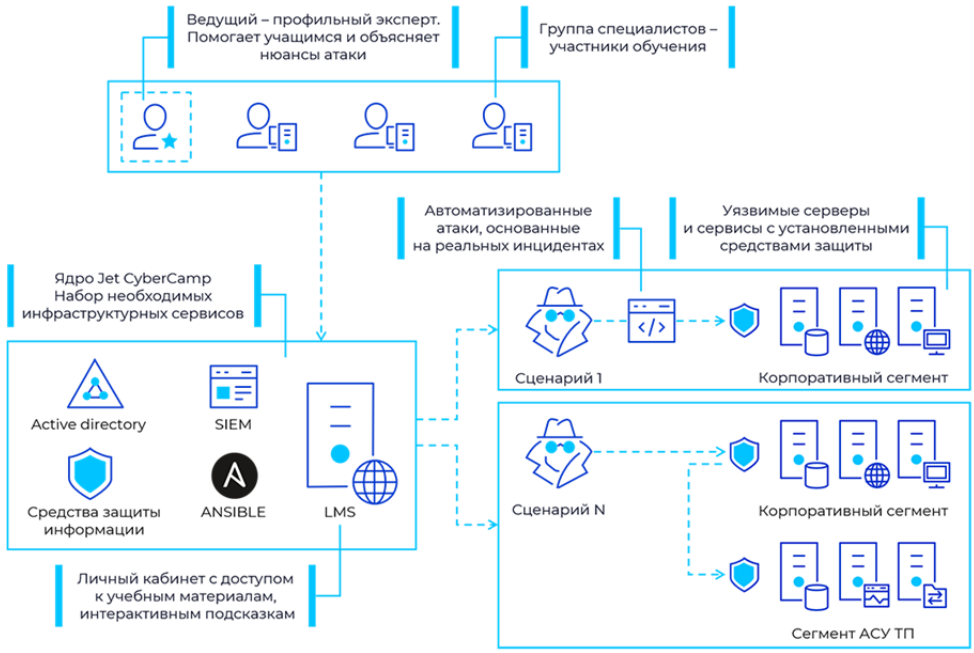

Рис. 6. **Архитектура Jet CyberCamp на платформе Jet (источник: https://www.anti-malware.ru/analytics/Market_Analysis/Cyber-Polygonsa) АСУТП – автоматизированная система управления технологическим процессом**

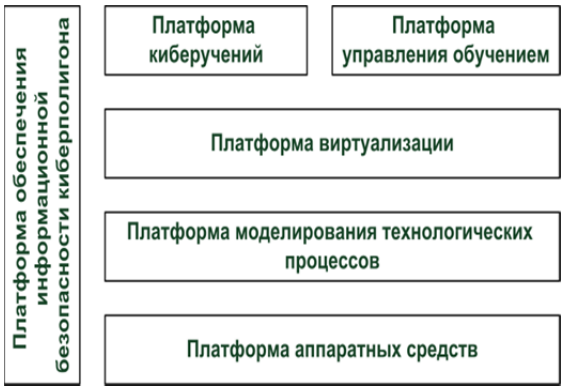

Рис. 7. **Обобщенная архитектура прототипов киберполигона**

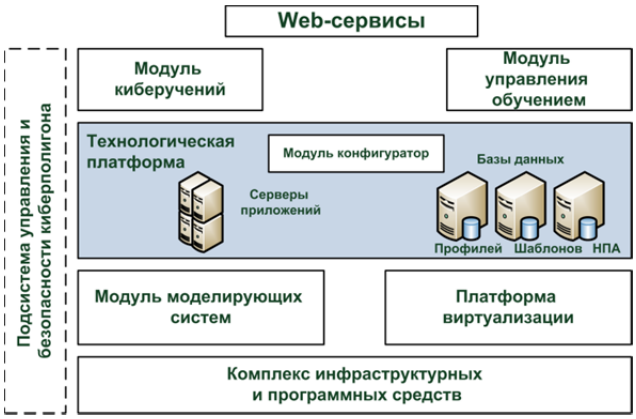

Рис. 8. **Базовая архитектура киберполигона**

Пространство технических решений, реализующих базовую архитектуру киберполигонов по отдельным ее функциональным программным модулям отечественных разработчиков, доведенных и реализованных в части технологий до уровня серийных изделий, достаточно представительно. Это послужило основой исследования и обоснования рационального варианта построения киберполигона на основе комплексирования готовых технических решений посредством различных альтернативных методов с соответствующей технико-экономической оценкой в Санкт-Петербургском университете ГПС МЧС России в 2023 г. Особенность технико-экономической оценки средств и оборудования киберполигона для ИТ (ИБ)-подразделений обеспечения заключается в определении, оценке и выборе варианта реализации, в частности, с привлечением специализированных компаний или собственных ресурсов [15]. По результатам технико-экономического анализа вариантов построения корпоративной системы типа «киберполигон» с применением метода анализа иерархий, выполненного коллективом ученых университета в научно-исследовательской работе (НИР) «Вариант», рекомендован вариант реализации на основе интегрирующего компонента интегратора. Таким компонентом в базовой архитектуре киберполигона является

функциональный программный модуль – технологическая платформа. Однако возможность практической реализации варианта построения киберполигона в значительной степени зависит от технологического уровня готовности критических компонент (критических элементов технологий, КЭТ) киберполигона, который при анализе в полной мере не учитывался, в частности, от уровня готовности технологии (УГТ) – технологической платформы как степени ее готовности к производству и эксплуатации, зависит уровень готовности системы (УГС) – киберполигона, которые можно оценить количественно [16].

Правовыми и нормативными документами Российской Федерации регламентирован не только терминологический ряд в части УГТ и УГС, а также методика (порядок, калькулятор) их определения (оценки), например, для результатов научно-исследовательских и опытно-конструкторских работ – приказ Минобрнауки России от 6 февраля 2023 г. № 107 «Об утверждении Порядка определения уровней готовности разрабатываемых или разработанных технологий, а также научных и (или) научно-технических результатов, соответствующих каждому уровню готовности технологий», ГОСТ Р 5979–2022; для программ Российского фонда развития информационных технологий – постановление Правительства Российской Федерации от 3 мая 2019 г. № 550; для проектов, поддерживаемых фондом «Сколково» – постановление Правительства Российской Федерации от 3 мая 2019 г. № 555; для экспериментальных разработок и поддержки производства – методика, утвержденная Минобрнауки России от 11 июля 2017 г. № ГТ-57/14вн, для сложных технических систем – ГОСТ Р 58048–2017 «Трансфер технологий. Методические указания по оценке уровня зрелости технологий». Для ОТС класса «киберполигон», которые базируются на ИТ и ИБ-технологиях, целесообразно использовать методические подходы, регламентированные для сложных технических систем. В этом случае, определение УГС киберполигона осуществляется на основе показателей УГТ, а также показателей «уровня готовности интеграции (УГИ)», под которым понимается степень совместимости технологий [16]. Характеристика шкал УГТ и УГИ представлена в табл. 3.

Таблица 3

Характеристика шкал УГТ и УГИ

Уровень	Технология		Интеграция	
	обозначение	характеристика	обозначение	характеристика
1	УГТ1	Основные принципы технологии изучены и опубликованы	УГИ1	Интерфейс между КЭТ определен с детализацией, достаточной для проектирования взаимодействия
2	УГТ2	Концепция технологии и/или ее применения сформулированы	УГИ2	Определена спецификация взаимодействия КЭТ через интерфейс
3	УГТ3	Критические функции и/или характеристики подтверждены аналитическим или экспериментальным путем	УГИ3	Достигнута совместимость технологий, позволяющая обеспечить их упорядоченную и эффективную интеграцию и взаимодействие
4	УГТ4	Компонент и/или макет испытаны в лабораторном окружении	УГИ4	Достигнуто качество взаимодействия и гарантируется интеграция между технологиями
5	УГТ5	Компонент и/или макет испытаны в окружении, близком к реальному	УГИ5	Достигнут достаточный уровень управления КЭТ по установке, поддержке, прекращению взаимодействия

Уровень	Технология		Интеграция	
	обозначение	характеристика	обозначение	характеристика
6	УГТ6	Модель системы/подсистемы или прототип продемонстрированы в окружении, близком к реальному	УГИ6	Интегрируемые КЭТ могут принять, преобразовать и структурировать информацию по назначению
7	УГТ7	Прототип системы продемонстрирован в условиях эксплуатации	УГИ7	Интеграция технологий была проверена и испытана с достаточной для использования степенью детализации
8	УГТ8	Реальная система завершена и квалифицирована в ходе испытаний и демонстрации	УГИ8	Реальная интеграция завершена и проверена испытаниями и демонстрацией в составе системы
9	УГТ9	Реальная система подтверждена путем успешной эксплуатации	УГИ9	Возможность интеграции проверена в применении

Оценка готовности технологии показывает зрелость КЭТ в системе, то есть элементов, от которых существенно зависят результативность и эффективность системы или с которыми соотносится главный технологический риск. Критическими элементами технологии относительно базовой архитектуры киберполигона являются функциональные программные модули (платформы): Web-сервисы (Веб); модуль управления обучением (МУО); модуль киберучений (МК), комплекс инфраструктурных и программных средств (КИПС), платформа визуализации (ПВ), модуль моделирующих систем (ММС), технологическая платформа (ТП).

Оценку i-й технологии проводят экспертным методом в соответствии с опросником (калькулятором), который регламентирован ГОСТ Р 58048–2017, учитывают по каждому уровню вид системы (оборудование (Hardware), программное обеспечение (Software) или комплексная система (Both), область анализа (технология (Technology), технология и организация производства (Manufacturing), проект разработки технологии (Project/Program), перечень вопросов для подтверждения соответствия состояния оцениваемой i-й технологии и пороговые значения ее оценки (100–75 % – «соответствует»; 85–50 % – «частично соответствует»; с рекомендованным 15 % разрывом между значениями).

Итоговый УГТj i технологии ($КЭТ_i$) киберполигона определяют по факту полной совокупности состояний j-го уровня со значением «соответствует». Результаты оценки УГТj по каждому КЭТ киберполигона заносят в матрицу УГТ киберполигона размерностью nx1 или представляют в табличной форме:

$$[УГТ]_{n\times 1} = \begin{bmatrix} УГТ_1 \\ \dots \\ УГТ_n \end{bmatrix},$$

где n – количество КЭТ киберполигона, принятых к оценке.

Следующей регламентированной процедурой определения УГС киберполигона является оценка УГИ киберполигона, для чего:

а) значение УГИ определяют по каждой оцениваемой паре КЭТ в диапазоне натуральных целых чисел от 1 до 9;

б) значения заносят в симметричную квадратную матрицу УГИ размерностью nxn, при условии, что:

– значение УГИij равно значению УГИji;

– значение УГИij равно 9, если i=j (любой КЭТ полностью интегрирован сам с собой);

– значение УГИij равно 0, если КЭТi и КЭТj не взаимодействуют друг с другом:

$$[\text{УГИ}]_{n\times n} = \begin{bmatrix} \text{УГИ}_{11} & \dots & \text{УГИ}_{1n} \\ \dots & \dots & \dots \\ \text{УГИ}_{n1} & \dots & \text{УГИ}_{nn} \end{bmatrix}.$$

На основе матриц $[\text{УГТ}]_{n\times 1}$ и $[\text{УГИ}]_{n\times n}$, элементы которых содержат значения в диапазоне натуральных целых чисел от 1 до 9, рассчитывают нормализованные матрицы $[\overline{\text{УГТ}}]_{n\times 1}$ и $[\overline{\text{УГИ}}]_{n\times n}$ со значениями в интервале [0, 1] путем операции деления на 9 каждого значения элемента матриц.

На основе $[\overline{\text{УГТ}}]_{n\times 1}$ и $[\overline{\text{УГИ}}]_{n\times n}$, рассчитывают значения элементов матрицы [УГС] размерностью nx1:

$$[\text{УГС}]_{n\times 1} = \begin{bmatrix} \text{УГС}_1 \\ \dots \\ \text{УГС}_n \end{bmatrix} = [\overline{\text{УГИ}}]_{n\times 1} \times [\overline{\text{УГТ}}]_{n\times 1}.$$

Итоговое значение УГС рассчитывается как:

$$\text{УГС} = \frac{\left(\frac{\text{УГС}_1}{m_1} + \frac{\text{УГС}_2}{m_2} + \dots + \frac{\text{УГС}_n}{m_n}\right)}{n},$$

где m_i – количество КЭТ, взаимодействующих с i оцениваемым (согласно данным матрицы УГИ).

Полученное нормализованное значение УГС киберполигона (индекс) сравнивают с данными шкалы УГС (табл. 4) и формулируют вывод об уровне готовности системы (киберполигона).

Таблица 4

Характеристика шкалы УГС киберполигона

Уровень	Обозначение	Характеристика	Индекс
1	УГС1	Уточнение концепции киберполигона	0,10–0,39
2	УГС2	Разработка технологии киберполигона	0,40–0,59
3	УГС3	Разработка и демонстрация киберполигона	0,60–0,79
4	УГС4	Производство киберполигона	0,70–0,89
5	УГС5	Применение и поддержка киберполигона	0,90–1,00

Сводные данные о результатах определения характеристик УГТ и нормированных значений показателей УГТ киберполигона по КЭТ, выделенным в НИР «Вариант» при проведении технико-экономической оценки варианта построения киберполигона, представлены в табл. 5.

Таблица 5

Сводные данные об УГТ функциональных программных модулей (платформ) киберполигона

№ п/п	КЭТ	УГТ	Значение УГТ	Нормированное значение УГТ
1	Веб	УГТ6	6	0,7
2	МУО	УГТ8	8	0,9
3	МК	УГТ7	7	0,8
4	КИПС	УГТ7	7	0,8
5	ПВ	УГТ6	6	0,7
6	ММС	УГТ7	7	0,8
7	ТП	УГТ8	8	0,9

Сводные данные о результатах определения характеристик УГИ киберполигона представлены в табл. 6.

Таблица 6

Сводные данные об УГИ функциональных программных модулей (платформ) киберполигона

Интеграция между модулями	Веб	МУО	МК	КИПС	ПВ	ММС	ТП
Веб	**9**	6	6	6	6	6	9
МУО	6	**9**	6	9	9	9	9
МК	6	6	**9**	9	9	9	9
КИПС	6	9	9	**9**	9	9	9
ПВ	6	9	9	9	**9**	9	9
ММС	6	9	9	9	9	**9**	9
ТП	9	9	9	9	9	9	**9**

Нормализация матрицы УГИ киберполигона представлена в виде:

$[\overline{УГИ}]_{7\times7}=$

	Веб	МУО	МК	КИПС	ПВ	ММС	ТП
Веб	1,0	0,7	0,7	0,7	0,7	0,7	1,0
МУО	0,7	1,0	0,7	1,0	1,0	1,0	1,0
МК	0,7	0,7	1,0	1,0	1,0	1,0	1,0
КИПС	0,7	1,0	1,0	1,0	1,0	1,0	1,0
ПВ	0,7	1,0	1,0	1,0	1,0	1,0	1,0
ММС	0,7	1,0	1,0	1,0	1,0	1,0	1,0
ТП	1,0	1,0	1,0	1,0	1,0	1,0	1,0

Результаты расчета матрицы УГС киберполигона представлены в следующем виде:

$[УГС]_{7\times1} =$

Модули	УГСкэт
Веб	4,0
МУО	5,7
МК	5,2
КИПС	5,4
ПВ	4,7
ММС	5,4
ТП	6,3

Относительно оценок УГТ и УГИ киберполигона в рассматриваемой конфигурации модулей Веб, МУО, МК, КИПС, ПВ, ММС, ТП рассчитан индекс УГС киберполигона, который составляет величину 0,75 и соответствует уровню 4 (Производство системы).

Традиционные методики технико-экономической оценки [17] используют процедуры, основанные на определении технического уровня системотехнического решения при ограничениях на учет оценок уровня интеграции базовых функций КЭТ системы, что обусловливает, как следствие, возможную значительную погрешность результатов технико-экономической оценки.

Подтверждением данного факта для рассматриваемой совокупности КЭТ киберполигона, являются результаты расчета УГС без учета УГИ КЭТ по данным УГТ киберполигона, как среднее значение, которое составляет 0,8. Погрешность результатов оценки уровня готовности системы, с учетом уровня готовности интеграции КЭТ киберполигона, составляет более 6 %, что должно отразиться на потенциальном недофинансировании доведения обоснованного и выбранного системотехнического решения киберполигона в части функциональности, которая зависит от интеграции его базовых компонент.

Интегрирующим компонентом киберполигона в соответствии с базовой архитектурой выступает технологическая платформа, в которой КЭТ является конфигуратором. От практической реализации конфигуратора технологической платформы зависят УГТ и УГИ киберполигона, и, как следствие, УГС киберполигона.

Конфигуратор киберполигона

Конфигуратор киберполигона – это программное средство технологической платформы организационно-технической системы для диспетчеризации настроечных (структурных, конфигурационных) и функциональных параметров, а также процессов основных функциональных программных модулей (платформ) при предоставлении сервисов треков киберполигона в соответствии с заявками пользователей или должностных лиц, выполняющих профессиональную деятельность в области управления, эксплуатации и ИБ киберполигона.

Конфигуратор киберполигона имеет существенное отличие в функциональности от сложившегося на практике понимания термина. Особенности определения «конфигуратор» в организационных, информационных и компьютерных системах представлены в табл. 7.

Таблица 7

Определения термина «конфигуратор»

Область применения	Определение	Источник
Организационные системы	Агрегат, состоящий из качественно различных языков описания системы, число языков минимально, но необходимо для заданной цели. Реализация: описания структуры подчиненности, функционирования и распределения информации	Лапыгин Ю.Н. Теория организаций: учеб. пособие. М.: ИНФРА-М, 2022. 324 с.
Информационные системы		
Сервисы Федеральной государственной информационной системы Росаккредитации	Конфигуратор заполнения электронного документа аккредитации продукции, процессов и услуг для подачи заявления	СМ № 02.1-3.0003. Инструкция по работе с конфигуратором
Система управления ресурсами предприятия с потребителем	Конфигуратор продукции под заказ клиента спецификациями для управления технологическими маршрутами	https://sapr.ru/article/14582?ysclid=lrwy34i71r881169665
Компьютерные системы		
ПЭВМ	Конфигуратор на программное обеспечение для типов ПЭВМ с расширенными функциональными возможностями	ГОСТ 27201–87 ЭВТ
Технологическое оборудование	Универсальный конфигуратор оборудования для встроенного программного обеспечения (микропрограмм)	Руководство оператора RU.05806720.00006-02 33 01 Промприбор

Конфигуратор киберполигона занимает особое место в классификации, которая представлена на рис. 9, применяемые в организационно-технических системах для процессного управления на основе полного стека применяемых технологий.

Рис. 9. **Классификация киберполигонов**

Разнообразие классификаторов, как показывают классификационные признаки, подтверждается объектами интеллектуальной собственности с названием «конфигуратор», зарегистрированными в Роспатенте. Количественная оценка зарегистрированных конфигураторов (объектов интеллектуальной собственности Российской Федерации) за последние 10 лет представлена в табл. 8, по типам (областям применения) – на рис. 10, а динамика – на рис. 11.

Таблица 8

Показатели регистрации в Российской Федерации технических решений по построению конфигураторов

Объекты интеллектуальной собственности	Количество зарегистрированных объектов интеллектуальной собственности, шт.										
	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
База данных	0	1	0	0	0	0	1	0	2	0	0
Программа для ЭВМ	19	15	18	24	16	18	43	39	53	36	33

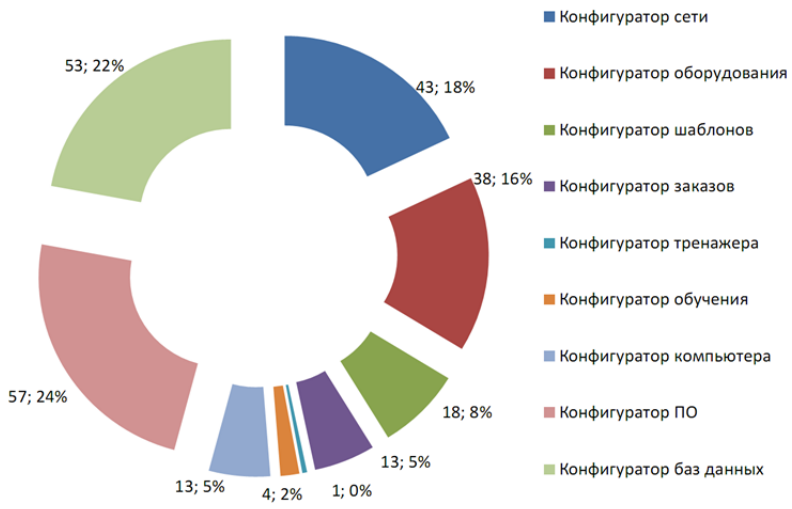

Рис. 10. **Распределение областей применения конфигураторов (результаты обработки базы данных Роспатента по состоянию на 1 января 2024 г.) (ПО – программное обеспечение)**

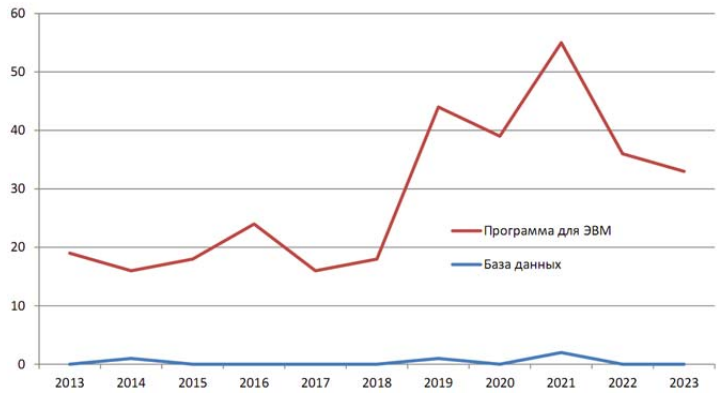

Рис. 11. **Активность регистрации объектов интеллектуальной собственности «конфигуратор» (по результатам обработки базы данных Роспатента по состоянию на 1 января 2024 г.)**

Основные характеристики прототипов конфигураторов киберполигона для серверов и баз данных (№ 2021660708, № 2021621501 (2021) [18, 19]), шаблонов оборудования (№ 2023665581 (2023) [20]), тренажеров (№ 2021668637 (2021) [21]), средств защиты (№ 2020616122 (2020) [22]), киберполигона (№ 2023616920 (2023) [23]) представлены в табл. 9.

Таблица 9

Характеристики прототипов конфигуратора киберполигона

Объекты конфигурирования	Характеристики зарегистрированных объектов интеллектуальной собственности				
	№ 2021660708 № 2021621501	№ 2023665581	№ 2021668637	№ 2020616122	№ 2023616920
1. Сервисы ТК					
1.1. Компетенций	Нет	Нет	Да	Нет	Да
1.2. Безопасности	Нет	Нет	Нет	Частично	Частично
2. Сервисы ТО					
2.1. Компетенций	Частично	Нет	Да	Нет	Да
2.2. Безопасности	Нет	Нет	Нет	Частично	Частично
3. Сервисы ТИ					
3.1. Безопасности	Нет	Нет	Нет	Нет	Нет
3.2. Регламентации	Нет	Нет	Нет	Нет	Нет
4. Оборудование					
4.1. АРМ	Да	Частично	Да	Нет	Частично
4.2. ЛВС	Нет	Частично	Нет	Нет	Частично
4.3. СО	Частично	Частично	Нет	Частично	Да
4.4. КО	Нет	Частично	Нет	Нет	Частично
5. СОИБ					
5.1. СППР	Нет	Нет	Нет	Нет	Нет
5.2. СПДн	Частично	Нет	Нет	Нет	Нет
5.3. СЗИ	Нет	Нет	Нет	Частично	Нет
6. Платформа					
6.1. Визуализатор	Частично	Нет	Нет	Нет	Частично
6.2. ОС	Нет	Да	Нет	Да	Частично
6.3. Библиотеки	Нет	Нет	Нет	Да	Частично
6.4. DevSecOps	Частично	Нет	Нет	Нет	Частично

Примечание: сервисы ТК – сервисы трека киберучений; сервисы ТО – сервисы образовательного трека, сервисы ТИ – сервисы исследовательского трека; АРМ – автоматизированное рабочее место; ЛВС – локальная вычислительная сеть; СО – система обеспечения; КО – коммуникационное оборудование; СОИБ – система обеспечения информационной безопасности; СППР – система поддержки принятия решений; СПДн – система персональных данных; СЗИ – средства защиты информации; ОС – операционная система

С целью практической отработки вариантов возможной реализации функциональных требований к конфигуратору технологической платформы киберполигона разработан макет программы для ЭВМ «Модуль-конфигуратор киберполигона» (Модуль). Модуль позволяет формировать схемы сервисов треков киберполигона на основе шаблонов, конфигурационных файлов для динамического развертывания виртуальной инфраструктуры и инфраструктуры образовательной среды, контуров управления доступом и мониторинга ИБ. Организовано:

– хранение и выдача данных для подбора инфраструктуры по параметрам следующего оборудования: антивирусные средства, средства доверенной загрузки, средства защиты от несанкционированного доступа, средства криптографической защиты, средства

контроля использования съемных носителей, системы мониторинга событий, сканеры уязвимостей, межсетевые экраны и т.д.;

– хранение параметров визуальных форм, элементов ввода информации;

– хранения данных о нормативных правовых актах и регламентах в области ИБ и ЗИ;

– доступ пользователей к данным об обозначении, исполнениях, версиях, характеристиках и другим сведениям о средствах (оборудовании) ИИ.

Экранные формы основных задач Модуля представлены на рис. 12–15.

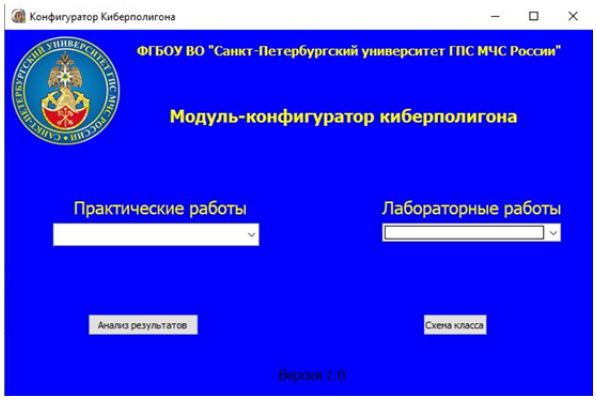

Рис. 12. **Интерфейс пользователя**

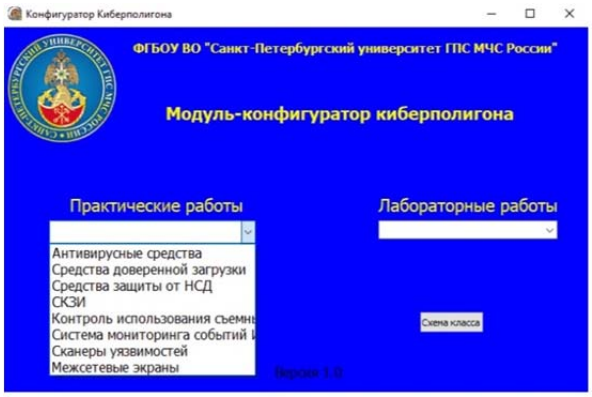

Рис. 13. **Интерфейс «Выбор вида занятий»**

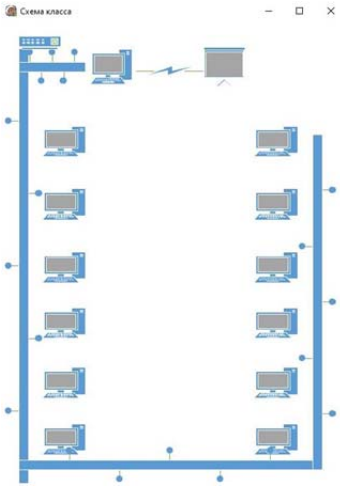

Рис. 14. **Интерфейс «Шаблон инфраструктуры»**

Рис. 15. **Интерфейс «Шаблон результатов»**

В учебном процессе университета в 2023–2024 учебном году успешно апробированы функции киберполигона по обеспечению инфраструктурой и информационными ресурсами плановых занятий в требуемой электронной информационной образовательной среде, оперативной корректировке конфигураций шаблонов для отработки учебных задач в ходе лабораторных и практических работ.

Результаты проведенной сравнительной оценки характеристик разработанного Модуля с характеристиками прототипированных решений конфигуратора (табл. 9) представлены на диаграмме рис. 16.

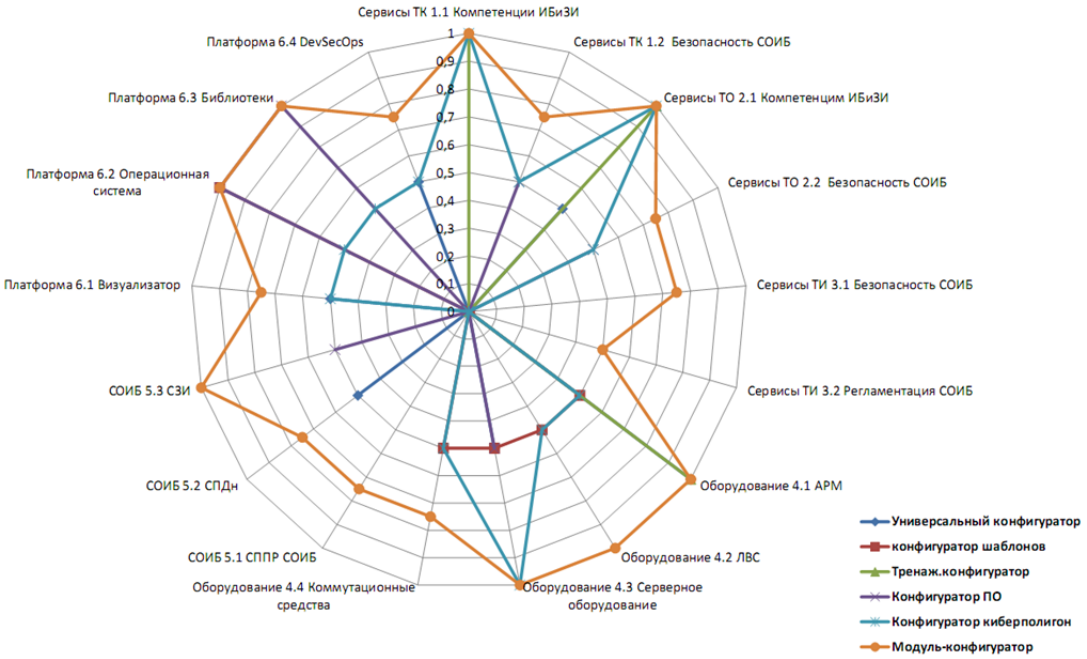

Рис. 16. **Диаграмма характеристик Модуля и прототипов конфигуратора**

Анализ данных диаграммы на рис. 16 показывает, что принятый подход к разработке Модуля, ориентированный на обеспечение ключевых свойств КЭТ кибеполигона, позволяет достигать высокого уровня показателей характеристик по группам основных требований к системам поддержки принятий решений по управлению СОИБ ведомственной ИИ и обеспечения мероприятий по повышению уровня осведомленности (уровня компетенций) должностных лиц в области ИБ и ЗИ.

Заключение

Требуемый уровень готовности организационно-технической системы класса «киберполигон» в условиях изменения в ведомственных системах обеспечения ИБ применяемых технологий поддерживают интегрирующие критические элементы технологий, которыми, в частности, являются технологическая платформа и конфигуратор киберполигона.

Повышение уровня интеграции функциональных программных модулей (платформ) киберполигона может быть обеспечено посредством опережающего развития и реализации функциональных характеристик конфигуратора киберполигона для управления сервисами, процессами и оборудованием ИИ и образовательной среды.

Статья подготовлена в рамках выполнения в 2024 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России по тематике «Киберсреда».

Список источников

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Рос. Федерации от 5 дек. 2016 г. № 646). Доступ из справ.-правовой системы «КонсультантПлюс».

2. О Стратегии национальной безопасности Российской Федерации: Указ Президента Рос. Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

3. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 1 мая 2022 г. № 250. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента Рос. Федерации от 30 марта 2022 г. № 166. Доступ из справ.-правовой системы «КонсультантПлюс». Доступ из справ.-правовой системы «КонсультантПлюс».

5. О внесении изменения в статью 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации: Федер. закон от 10 июля 2023 г. № 312-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. О прекращении применения отдельных средств защиты информации: Информационное сообщение ФСТЭК России от 30 авг. 2023 г. № 240/21/4233. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Требования по безопасности информации (утв. приказом ФСТЭК России от 14 апр. 2023 г. № 64). Доступ из справ.-правовой системы «КонсультантПлюс».

8. Руководство по организации процесса управления уязвимостями в органе (организации): методический документ (утв. ФСТЭК России 17 мая 2023 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об организации парольной защиты информации, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных ресурсах МЧС России: распоряжение МЧС России от 14 дек. 2002 г. № 949. Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных ПДн, эксплуатируемых при осуществлении МЧС России функций, определенных законодательством Российской Федерации: приказ МЧС России от 5 дек. 2022 г. № 1231. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Руководство по организации процесса управления уязвимостями в органе (организации): методический документ (утв. ФСТЭК России 17 мая 2023 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

12. 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 // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2022. № 3. С. 1–17. EDN OGPXZX.

13. Синещук М.Ю., Шестаков А.В., Гавкалюк Б.В. Инфологическая модель и критерии качества решений по построению ведомственных организационно-технических систем класса «киберполигон» // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 1. С. 121–137. EDN MYIAHH.

14. Основные принципы проектирования архитектуры современных систем защиты / М.В. Буйневич [и др.] // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58. EDN VPRMIB.

15. Методика технико-экономической оценки вариантов построения организационно-технической системы класса «киберполигон» / А.В. Матвеев [и др.] // Инженерный вестник Дона. 2023. № 6 (102). С. 187–200. EDN HSAZAO.

16. Шестаков А.В., Тукмачева М.А., Линник В.А. Безопасность жизнедеятельности: информационная безопасность. Схемы и QR-ссылки: учеб. пособие. СПб.: Типография Любавич, 2023. 108 с.

17. Методические рекомендации по оценке целесообразности создания и развития государственных информационных систем на единой цифровой платформе Российской Федерации «ГОСТЕХ» // Минцифры России. М., 2023. 54с.

18. Серверный модуль универсального конфигуратора баз данных crm db 2.0.: Свидетельство о регистрации программы для ЭВМ № 2021660708. Патентообладатель: Булычев Е.С., Бураков А.А. Заявл. № 2021619041 от 03.06.2021. Опубл. 01.07.2021.

19. База данных crm db 2.0.:Свидетельство о регистрации базы данных № 2021621501. Патентообладатель: Булычев Е.С., Бураков А.А. Заявл. № 2021621299 от 18.06.2021. Опубл. 12.07.2021.

20. Конфигуратор шаблонов унифицированной структуры единого пространства имен: Свидетельство о регистрации программы для ЭВМ № 2023665581. Патентовладелец: ООО «Автоматика сервис». Заявл. № 2023664882 от 17.07.2023. Опуб. 18.07.2023.

21. НЕО ТРЕНАЖ. КОНФИГУРАТОР: Свидетельство о регистрации программы для ЭВМ № 2021668637. Патентовладелец: АО «Инжиниринговая компания «НЕОТЕК МАРИН». Заявл. № 2021667558 от 08.11.2021. Опубл. 18.11.2021.

22. Универсальный конфигуратор ПО для пакета программ защиты Web-сервера: Свидетельство о регистрации программы для ЭВМ № 2020616122. Патентообладатель: ФГБУ «Институт теоретической и экспериментальной физики имени А.И. Алиханова Национального исследовательского центра «Курчатовский институт». Заявл. № 2020615340 от 03.06.2020. Опубл. 10.06.2020.

23. Модуль «Конфигуратор» платформы «Иннокиберполигон»: Свидетельство о регистрации программы для ЭВМ № 2023616920. Патентовладелец: АНКО ВО «Университет Иннополис». Заявл. № 2023615701 от 29.03.2023. Опубл. 03.04.2023.

References

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utv. Ukazom Prezidenta Ros. Federacii ot 5 dek. 2016 g. № 646). Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

2. O Strategii nacional'noj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 2 iyulya 2021 g. № 400. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

3. O dopolnitel'nyh merah po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 1 maya 2022 g. № 250. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

4. O merah po obespecheniyu tekhnologicheskoj nezavisimosti i bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 30 marta 2022 g. № 166. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus». Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

5. O vnesenii izmeneniya v stat'yu 2 Federal'nogo zakona «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: Feder. zakon ot 10 iyulya 2023 g. № 312-FZ. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

6. O prekrashchenii primeneniya otdel'nyh sredstv zashchity informacii: Informacionnoe soobshchenie FSTEK Rossii ot 30 avg. 2023 g. № 240/21/4233. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

7. Trebovaniya po bezopasnosti informacii (utv. prikazom FSTEK Rossii ot 14 apr. 2023 g. № 64). Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

8. Rukovodstvo po organizacii processa upravleniya uyazvimostyami v organe (organizacii): metodicheskij dokument (utv. FSTEK Rossii 17 maya 2023 g.). Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

9. Ob organizacii parol'noj zashchity informacii, ne soderzhashchej svedeniya, sostavlyayushchie gosudarstvennuyu tajnu, obrabatyvaemoj v informacionnyh resursah MCHS Rossii: rasporyazhenie MCHS Rossii ot 14 dek. 2002 g. № 949. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

10. Ob opredelenii ugroz bezopasnosti personal'nyh dannyh, aktual'nyh pri obrabotke personal'nyh dannyh v informacionnyh PDn, ekspluatiruemyh pri osushchestvlenii MCHS Rossii funkcij, opredelennyh zakonodatel'stvom Rossijskoj Federacii: prikaz MCHS Rossii ot 5 dek. 2022 g. № 1231. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

11. Rukovodstvo po organizacii processa upravleniya uyazvimostyami v organe (organizacii): metodicheskij dokument (utv. FSTEK Rossii 17 maya 2023 g.). Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

12. Bujnevich M.V., Matveev A.V., Smirnov A.S. Aktual'nye problemy podgotovki specialistov v oblasti informacionnoj bezopasnosti MCHS Rossii i konstruktivnye podhody k ih resheniyu // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2022. № 3. S. 1–17. EDN OGPXZX.

13. Sineshchuk M.Yu., Shestakov A.V., Gavkalyuk B.V. Infologicheskaya model' i kriterii kachestva reshenij po postroeniyu vedomstvennyh organizacionno-tekhnicheskih sistem klassa «kiberpoligon» // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2023. № 1. S. 121–137. EDN MYIAHH.

14. Osnovnye principy proektirovaniya arhitektury sovremennyh sistem zashchity / M.V. Bujnevich [i dr.] // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2020. № 3 (31). S. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58. EDN VPRMIB.

15. Metodika tekhniko-ekonomicheskoj ocenki variantov postroeniya organizacionno-tekhnicheskoj sistemy klassa «kiberpoligon» / A.V. Matveev [i dr.] // Inzhenernyj vestnik Dona. 2023. № 6 (102). S. 187–200. EDN HSAZAO.

16. Shestakov A.V., Tukmacheva M.A., Linnik V.A. Bezopasnost' zhiznedeyatel'nosti: informacionnaya bezopasnost'. Skhemy i QR-ssylki: ucheb. posobie. SPb.: Tipografiya Lyubavich, 2023. 108 s.

17. Metodicheskie rekomendacii po ocenke celesoobraznosti sozdaniya i razvitiya gosudarstvennyh informacionnyh sistem na edinoj cifrovoj platforme Rossijskoj Federacii «GOSTEKH» // Mincifry Rossii. M., 2023. 54s.

18. Servernyj modul' universal'nogo konfiguratora baz dannyh crm db 2.0.: Svidetel'stvo o registracii programmy dlya EVM № 2021660708. Patentoobladatel': Bulychev E.S., Burakov A.A. Zayavl. № 2021619041 ot 03.06.2021. Opubl. 01.07.2021.

19. Baza dannyh crm db 2.0.:Svidetel'stvo o registracii bazy dannyh № 2021621501. Patentoobladatel': Bulychev E.S., Burakov A.A. Zayavl. № 2021621299 ot 18.06.2021. Opubl. 12.07.2021.

20. Konfigurator shablonov unificirovannoj struktury edinogo prostranstva imen: Svidetel'stvo o registracii programmy dlya EVM № 2023665581. Patentovladelec: OOO «Avtomatika servis». Zayavl. № 2023664882 ot 17.07.2023. Opub. 18.07.2023.

21. NEO TRENAZH. KONFIGURATOR: Svidetel'stvo o registracii programmy dlya EVM № 2021668637. Patentovladelec: AO «Inzhiniringovaya kompaniya «NEOTEK MARIN». Zayavl. № 2021667558 ot 08.11.2021. Opubl. 18.11.2021.

22. Universal'nyj konfigurator PO dlya paketa programm zashchity Web-servera: Svidetel'stvo o registracii programmy dlya EVM № 2020616122. Patentoobladatel': FGBU «Institut teoreticheskoj i eksperimental'noj fiziki imeni A.I. Alihanova Nacional'nogo issledovatel'skogo centra «Kurchatovskij institut». Zayavl. № 2020615340 ot 03.06.2020. Opubl. 10.06.2020.

23. Modul' «Konfigurator» platformy «Innokiberpoligon»: Svidetel'stvo o registracii programmy dlya EVM № 2023616920. Patentovladelec: ANKO VO «Universitet Innopolis». Zayavl. № 2023615701 ot 29.03.2023. Opubl. 03.04.2023.

Информация о статье:
Статья поступила в редакцию: 18.02.2024; одобрена после рецензирования: 11.03.2024;
принята к публикации: 12.03.2024

The information about article:
The article was submitted to the editorial office: 18.02.2024; approved after review: 11.03.2024;
accepted for publication: 12.03.2024

Информация об авторах:
Синещук Максим Юрьевич, заместитель начальника центра информационных и коммуникационных технологий – начальник отдела связи и сетевых технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), e-mail: smaxim@igps.ru

Information about authors:
Sineshchuk Maxim Yu., deputy head of the center for information and communication technologies – head of the department of communications and network technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), e-mail: smaxim@igps.ru